

# How to Work with a Technology Consultant

*Toby Brown*

May 2006

The best tool to have when dealing with an IT professional is knowledge. Just as legal clients can benefit from having an understanding of how a legal process works and what elements and terms are involved, a lawyer will benefit from knowing some IT basics when hiring an IT professional.

Attached is an article from a Legal Technology Consultant on Do-It-Yourself technology. David Moon was selected as the Legal Technology Consultant of the Year for 2005 by TechnoLawyer and is very knowledgeable about legal specific technology in addition to more general technology subjects.

This article is intended to give you knowledge about the issues you will face when hiring a technology consultant. The basics focus on: 1) computer networks and their elements, 2) general and legal software applications, 3) integration and security issues, and 4) mobile device factors. The article was utilized as part of a TechShow presentation made in partnership with Mr. Moon.

After gaining an understanding of the basics of legal technology, the next step in hiring an IT professional is due diligence. Again the analogy of a client hiring a lawyer applies. Just like your clients, you are placing a lot of trust in an IT professional. They will have access to yours and your clients' information and should be treated accordingly. As I like to say these days: Data is Money. So you will want to put extra effort into checking references and checking in with colleagues who may be aware of a particular consultant and their business.

There are a growing number of legal specific technology consultants coming into the market. So as the choices are increasing, make sure you end up with a technology consultant who you can trust to get your job done.

# Networking: Can I Still Do It Myself?

## A Basic Guide to a Do It Yourself Technology Implementation

By David R. Moon

Americans have a long-standing tradition of “do-it-yourself” (DIY) thinking. This attitude can span everything from the simplest home improvements to the most complex financial decisions a person can make. When it comes to a network, careful planning and implementation are key components to a successful DIY network. Massive improvements in technology have made computers much easier to use. This, coupled with DIY confidence, can lead a person to believe they can setup and maintain their own computer network for their office. As many of us enjoyed the antics of Tim, “The Toolman”, on the Home Improvement sitcom, we know a do-it-yourself project can blow up and end up costing far more than it should. So at any time, if you ever feel uncomfortable with a do-it-yourself technology implementation, go with your intuition and hire a professional. While it is unlikely anything you could do may cause bodily harm, a mistake could mean a malpractice lawsuit against your firm. We will focus on getting you up to speed with some basics to start a do-it-yourself technology implementation. Because there is such a wide variety of technology available, an in-depth coverage of everything is far beyond the scope of this article.

### Network Types

The first decision a do-it-yourselfer has to make is deciding upon what type of network to install. There are two types of networks: **peer to peer** and **dedicated server**.

#### *Peer to Peer Networks*

A Peer to Peer takes two or more computers and allows them to share hard drives and printers. This is often the least expensive to get up and running, but over time this can actually be the more costly solution. To connect two or more computer in a peer to peer network, all is needed is a network card for each computer and a switch. The network cards and switch can be wireless or cable but for extra speed and reliability, a cabled solution is better.

The most common problems with a Peer to Peer network are:

- Lack of central location of data
- Use of applications requiring a common drive letter
- Unexpected shut down of a critical computer

A user may be connected to one or more computers for drive sharing and thus able to save data to more than one workstation in the group. As the number of workstations grows, so does the problem. Locating data at a later time will stress the calmest person. Not to mention, backing up data in this type of environment is a challenge in itself. Applications designed to be on a network often require every workstation to use the same drive mapping. On a Peer to Peer network, the workstation which holds the data is often

configured to see the local drive as “C” while the remote workstations see the same drive as drive letter “F”. If an application will not work properly in an environment of mixed drive mappings, then care must be taken to setup a consistent drive mapping across all workstations.

The most common problem in a Peer to Peer network is the unexpected shutdown of a computer hosting data for others. It is more common mainly because the hosting computer is being used as a workstation and server. An unexpected shutdown or crash not only wastes time (and money) for everyone; it could also cause data corruption or even lost data. The cost of recovery of this data can add up quickly through lost billable time, re-entering data from the last backup, and the out of pocket expense of hiring an expert to recover data. A successful peer to peer network is usually the result of effective training of the users and constant maintenance and vigilance of the do-it-yourselfer.

### *Dedicated Servers*

A dedicated server is a more robust and more stable network environment than a peer to peer. The upfront cost is more but may actually save money over time. The cost saving over time is largely due to stability and centralized management. The first Microsoft servers were much simpler to setup and install. Do-it-yourselfers discovered they could set one up using the default settings. Today’s Microsoft servers are much more complicated than this and require more customization of the server setup in order to get full and proper use of the server. For example, today’s server-based networks rely heavily on Internal Domain Naming Server (DNS). This is a method in which the workstation will request a server resource by IP address of the server. If the DNS is not setup properly, the result can be poor network performance and improperly working applications.

A more specific example of getting full use of your server is the Microsoft Small Business Server (SBS). It is designed to make it easy for someone with the most basic networking knowledge to install. While a typical do-it-yourselfer should be able to get SBS up and running, they probably will need the help of an experienced IT Consultant to make the server more user friendly. For instance, some of Microsoft SBS’s best features are the ability for new computers to be quickly configured for the network and install network applications automatically from the server. The web portal can be configured to allow users access to their office computer very easily from home. These extra features are not something a typical “do it yourself” installer will know how to install or even be aware of. Regardless of the type of network, it is important to know what programs will be installed or run from the server and setup the network accordingly. Many applications have certain tweaks which is required for stability. For example, Opportunist Locking is a network setting turned on by default. This adds tremendous performance to the network but at the same time is often the cause of data corruption on most databases. For more information on Opportunist Locking, Google Opportunistic Locking. Some legal applications have great tech notes available on this subject.

<http://support.tabs3.com/main/R10200.htm>).

## **Backups**

Once the network is up and running, the backup system is a vital part of the system. If the information on the network is essential to your law firm, then it is only logical that the information be protected to the fullest. Proper design, setup and maintenance of your backup system are critical to have something that is dependable and reliable. Improper setup of the backup or failure to maintain the backup system can lead to a complete system loss.

There are many backup software programs available on the market. But just buying the standard package may not be enough to protect your files. For example, how often do users leave their computers on with documents and programs open every night? Those open documents and programs are probably the most critical to the company, but most backup programs need additional add-on modules to backup open files. Depending on the needs of your network, you may need additional add-on modules or even a different backup software program that can handle your needs more fully. Researching the various available packages is a key aspect to your backup solution. It is more important to get the best backup system for your network than getting the cheapest backup system. It may save a few dollars to buy the cheapest, but in the long run this could be a disastrous decision for your firm.

A backup system should show easy-to-read reports that detail if the backups were successful or not, and deliver those reports to the person in charge. One of the most common mistakes made in the backup system is failure to ensure that backups are being made on a regular basis. Most backup software packages offer a variety of delivery methods that are fairly easy to setup. A popular backup software is Backup Exec and was recently purchased by Symantec([www.symantec.com](http://www.symantec.com)). Another backup is Arcserve by computer associates ([www.ca.com](http://www.ca.com)). When purchasing, if you have Windows Small Business Server, purchase the backup software made specifically for it.

## **Remote Access**

There are two type of remote access, both of which have advantages and disadvantages. The first is Remote Node and the other is Remote Control. VPN is not a remote access solution but a security solution and may be used in conjunction with either of the two methods.

### *Remote Control*

Remote Control is the method of controlling a host computer (or host virtual computer). In this environment, all programs and data stay on the host side (the office). The remote computer is more of a 'dumb terminal' and is only responsible for input from the mouse and keyboard and output from the host video. In most situations, this is a secure environment as the only data traveling the keyboard data as travels the internet.

Commonly used examples of Remote Control include:

- PCAnywhere
- Windows XP Professional Remote Desktop

- Terminal/Citrix Server

The advantages are:

- Speed
- Data and programs reside on the Host side (Office)
- Access can be made available from virtually any computer (excluding PCAnywhere)
- Security even without VPN
- Looks exactly the same as being at the office

The disadvantages are:

- Number of computers (This does not include Terminal/Citrix Server)
- The cost (varies depending on the type of solution)

### *Remote Node*

Remote Node takes a remote computer (Home PC) and connects it to the network as if it was physically located at the office. The remote computer would have the same drive mappings. For this to work, in many cases, the applications need to be installed locally. Also, all data must travel through the connection which will be much slower. About the only application usable will be a Word Processor application. Any database application will be much too slow (SQL being the exception). In this situation, a VPN tunnel is required for security reasons. The overhead from the VPN encryption will have a small negative impact on speed. Even with a VPN, there is one security issue created in a Remote Node which is not present in Remote Control. If the remote computer is infected with a network aware virus, this could lead to the firm's network being infected. Home computers tend to be much more vulnerable because they do not have the protection of a good firewall, or have security patches installed on a regular basis.

The home computer with a VPN back to the network becomes a point of vulnerability for the network.

Commonly used setups include:

- Remote Access Server (Microsoft Servers)
- VPN tunnel on a firewall

The advantages are:

- No host computer required
- Cost

The disadvantages are:

- Very limited speed performance
- Difficult to access from different computers while traveling
- Data and programs leave the network
- Ability to transmit viruses from remote to host

## **Firewalls**

Firewalls restrict the number of points of access. The best way to understand this is to visualize a network as an office with warehouse space in the back. Each door allows people to access a different part of the office space for different needs.

The front door is open to the public. But once inside the front door, other doors restrict a person from just wandering around. In the computer world, this is called a DMZ in the firewall. A Web server might be placed in the DMZ. The public can view the Web Server but does not have access to other servers with critical information.

In the same office space, another door in the back may be used for pickup and deliveries. Generally, the public is not permitted in this area, only delivery personnel. In the computer world, this might be a client portal restricting access to those with an account. A firewall must be configured to allow certain ports (doors) to be open. Each IP address (think of this as the physical address of the office space) has thousands of ports. Each port has a special meaning. Below are some common ports and what they are used for.

Port Name Used for:

- 25 SMTP Inbound Email to an Email Server
- 80 HTTP Web traffic for Web Servers
- 110 POP3 Outbound Email pick up. Downloading Email
- 443 SSL Secure Socket Layer for Secure Web Services
- 3389 RDP Remote Control to a workstation/Server

## **Integration**

Today, every application and every device shares information. Email goes to a traditional email client such as Microsoft Outlook, but also may be redirected to one or more applications such as a document management system, practice management software or even a PDA phone. Email is not the only type of information that may be integrated with multiple software programs or devices. A practice management system may send the calendar information to the PDA phone and billing system to be billed. The billing system may send client information to the practice management system. The maze of dataflow keeps the best IT people on their toes or ripping out their hair.

To setup this level of integration, one must have a detailed, in-depth knowledge of most, if not all, of the systems. In some cases, integration is analogous to fitting a square peg in a round hole. Each system has differences in integration. While two practice management software packages may integrate with the same document management system, the method in which they do so can be very different. In some situations, a firm may find it very difficult to implement integration on their own and may require the help of an IT consultant who has specialized knowledge of the software packages.

## **Do-it-Yourself: Good or Bad Idea?**

*Should* you do it yourself? It depends. Is your time more valuable than the cost of a professional? In other words, do you bill at a higher rate than the professional would cost you, and would they get it done faster? If it is more cost effective to hire someone else to handle the network so that you can concentrate on billing, then it only makes sense to hire a Legal Technology/IT specialist. If, however, you don't think it would be cost effective or you have the time to spend away from your practice, this could be a good opportunity to "do-it-yourself" and learn more about networks and computers.

Just a word of warning: it is much more difficult and costly to correct a mistake or bad installation than to do it correctly the first time. But if you are going to do-it-yourself, here are some tips for a successful installation:

1. Do not be the first to try out a new hardware or software.
2. Do not skimp on hardware.
3. Get updates to the software or drivers to the hardware.
4. Setup a test system.
5. Read the documentation before, during and after the installation.
6. Plan to redo an installation a few times before putting it into place.

The first to implement something new must endure all the painful pitfalls. Take advantage of online discussion forums to learn about other people's experiences (good and bad). Learn from other people's mistakes and do not repeat them. Your time is valuable, so the less you spend on implementing any technology, the more time you have to bill your clients.

With computer technology, the less you pay upfront, the more it will cost you over the life of the technology. Cheap hardware may mean more compatibility issues and more time spent on finding a workaround solution (see the first guideline). Hardware which is shipped with drivers or software on CD's will most likely have been packaged months ago. It is already outdated before you purchased it. The first thing to do before and after installation is to check for updates online with the manufacturer. Check for updates before installation as known issues may be fixed. Check after the installation because things can change that quickly and new enhancements may be available. If this is your first time installing a new server or workstation, setup a test system. A test system is not a test system if the data stored within it cannot be lost or useable for several days. This might seem extreme, but the worst case scenario of any new installation is data loss.

A test system will allow an opportunity to experiment and learn without affecting the day to day operations. Just as a litigation attorney may have a mock trial to prep for a case, anyone implementing technology, both the professional and novice, should setup a test system. The test environment should be as identical as possible to the final environment. One subtle variation could cause the technology being implemented to fail. Before beginning, read the documentation - all of it. Many mistakes can be avoided just by reading the manual. Read the step by step how-to documentation again as the installation occurs to make sure you don't accidentally skip a step. Afterwards, go back and reread the documentation to verify all procedures were followed and that you understand how to maintain and protect the integrity of the system.

As practice makes perfect, repeat the installation in a test environment a few times. Between each installation, utilize the system with some extra data. After each installation and testing, one may see a better and more efficient way to implement the technology. This is especially true in legal applications and network design. This can also help to uncover any bugs in the system such as slowness, rights issues, hardware incompatibilities, etc. The more complex the system or the more it integrates with, the

more care should be taken. A PDA phone which will have primarily redundant data is not as critical. One might be able to test in a live environment with little consequences. But a practice management system takes some forethought as they are often customized to each firm. And all the features may take months to setup. Some of the features are built on top of the others. One can paint themselves into a corner with bad implementation/design. It is also important to keep an eye on the future of your law firm and where you plan to go with it. As your law firm grows or shifts, the network has to change accordingly with it. The more time that is spent on the design of your network now can save much pain and frustration later.

### **Finding (and Hiring) a Legal Technologist**

If you have decided that part or all of a technology project is best left to a consultant, finding the right Legal Technologist can be an exhausting job in itself. And there are many things to be considered, more than what can be discussed here in proper detail. So consider this to be a general overview.

Legal Technology is a very specialized field. Just because a network integrator has installed a server in one or more law firms does not make them a Legal Technologist. One should not pick up the yellow pages and call a random phone number thinking they are all the same. Nor should one just hire the neighbor or relative who can do this on the side and happens to know more than you. Going the cheapest route isn't necessarily the best route. The old adage, "you get what you pay for" is very true.

A Legal Technologist should have a working knowledge of most, if not all, of the systems in use. If you cannot find a single source who can handle all of your various systems, it might be necessary to find a group of consultants who can work together. It is important to make sure the group can communicate with each other and work well together.

Asking other attorneys for a referral can be another source. Keep in mind, however, that while the referral may have been the right choice for them, it may not be the right choice for you. Every firm has different needs and different systems. If you are looking for assistance with a particular legal application only and not the entire network, start with the application manufacturer's website. Persons certified are often listed there. Another resource is the State Bar which may have a list of Technology Consultants. Some state bars have staff to assist you for a small fee. Whether you decide to do-it-yourself or hire a professional for assistance, success will come to those who make informative decisions.

David R. Moon - Mr. Moon founded Lan-Tech, Inc. in 1993 and was voted *Legal Technology Consultant of the Year* in 2005 by the Techno Lawyer user community consisting of over 11,000 subscribers, including many law firms and legal organizations that have benefited from Lan-Tech's legal expertise and networking experience. In addition to being a graduate from Georgia Tech with a Masters in Electrical Engineering,

Mr. Moon is also a Citrix Certified Engineer Administrator, Microsoft Network Designer, certified trainer for Concordance, Summation and Worldox applications, an STI President Circle member, and a Time Matters/Billing Matters Certified Independent Consultant. Recently, he has developed methodologies and implemented software and hardware for law firms migrating to paperless office environments. He has designed and implemented over 200 networks ranging from small office to medium size firms. David Moon can be reached by email ([david.moon@lan-tech.com](mailto:david.moon@lan-tech.com)) or by phone at 770-514-0400 x12.

# Getting Rid of Paper ... Ethically

*Toby Brown*

May 2006

The service benefits and costs savings of going paperless are now well defined, especially outside the legal industry. Since lawyers deal almost exclusively in information, shifts away from paper towards electronic information make a lot of sense. This paper will explore the various reasons lawyers should head in this direction, then some of the steps in order to get there and finally, some of the issues and concerns that will pop up along the way.

Before you start down a paperless path, we should explore the reasons for taking such a path. The two overriding reason will be cost savings and client service abilities. Moving into an environment with less paper saves money from the perspective of scanning paper and from utilizing processes that avoid paper.

Next we will explore steps for moving away from paper, including scanning issues and dealing with electronic information. From there we will talk about the new issues you will have to address, including the ethical pitfalls and implications.

This exploration will have a practical emphasis, giving tips on how to effectively and ethically deal with each step of going paperless.

## **Good Reasons**

There are a multitude of cost savings lawyers can enjoy from going paperless. Fortunately the higher end of the litigation market has already demonstrated and proven out that electronic methods save money. First off, at the most basic level, it is cheaper to scan a document once than to copy it many times. The machine costs of scanning once compared to the copier, toner costs of making multiple copies are lower. Further levels of savings come since 1) the labor costs are lower for doing it once, 2) the floor space needs for storing paper go down, saving on rent expense, 3) the management time going into dealing with labor and copier hardware support goes down, and 4) the cost of properly destroying discarded paper (shredding, etc.) is reduced.

If cost savings are not enough, consider the enhanced productivity and client service aspects of less paper. Although paper is portable, carrying it everywhere is burdensome. Whereas remotely accessing your office (via VPN), being able to search massive mounts of information and then retrieving it, perhaps with just your PDA phone, is an option with electronic information. The point here is that access to your documents is greatly expanded with electronic information. This access brings about a number of values for your practice. The first one is for you. You can access client information and resolve problems from most any location. (Of course there are downsides to this aspect, and you should maintain balance in your life.) This type of tool can allow you to be

places other than your office when needed or desired. The next outcome of this accessibility is implied: that you can better serve your clients' needs. So both you and the client win in this scenario. From a productivity perspective, if you have multiple office locations, all staff and lawyers can access the same information. Or you can allow telecommuting for appropriate staff, helping a firm retain valuable staff and get the most out of them.

This last point indirectly brings up another; cost savings. Lawyers and firms spend a measurable amount of time looking for lost paper files. Electronic files are much harder to lose and much easier to find, given search technologies. So unproductive (and un-billable) lawyer and staff time spent looking for lost paper is reduced.

Another value point from the improved accessibility of e-info, is that this access can be shared with clients. Newer document management systems and other online services, allow for online sharing and collaboration of electronic information. This has the potential to improve client service, improving your chances of getting and keeping good clients.

Perhaps the biggest drawback of paper comes on disaster recovery. No one really attempts creating a back-up of a paper file room, because the cost would be immense. Therefore disasters that damage or destroy paper are difficult to impossible to plan for. In contrast the ability to back up electronic information, especially to offsite locations, is simple and cost effective.

Finally, with the advent and growth of e-filing in various courts, a lawyer being able to operate in a non-paper world is making more sense every day.

In summary, moving away from paper makes all kinds of sense. It reduces operational costs for lawyers and improves their ability to practice law and serve their clients. The real questions are less about why you should make the move, than about how you will.

### **Take the First Steps**

There are two aspects in terms of functionalities that need to be addressed in the move towards less paper. The first is the scanning of paper documents to create electronic versions. The second is implementing software and other tools to avoid going to paper whenever possible. Many technologies (and many old habits) point down the path of printing documents. So new tools and approaches need to be implemented to avoid this traditional path.

#### *The World of Scanning*

Once you decide to move to scanning, you will have hardware, software and even policy issues to deal with. Hardware will focus on the obvious: scanners. What type of scanner or scanners should you purchase? Software encompasses two aspects: software

for capturing the scans, then OCR<sup>1</sup> software that converts images of text into actual editable text.

When considering scanners there are obviously different levels of quality and features to consider. Basic flatbed scanners just provide moderate quality scans, one page at a time. If you are looking to take your practice in this paperless direction, you will likely want a higher quality scanner, with a paper feeder. HP scanners in this category run \$100 to \$500. Another approach is to replace your copier with a digital version that scans in addition to producing copies. This type of hardware is much more expensive, but allows for multifunction use and if you are in the market to replace a copier anyway, makes sense.

When scanning, if you plan on running OCR software to extract editable text, you will want quality scans of at least 300 DPI (dots per inch). This will give you better results from OCR. If you occasionally scan color documents, such as photos, a high quality color flatbed scanner makes sense. Although you won't be running OCR on these documents, you may need to produce them as exhibits and demonstrative evidence and will want high quality scans for high quality prints.

At the time of scan you will capture basic information about the document. This will help you index the document for later search and retrieval. The litigation support world has tackled this problem and has some lessons-learned. Although scanning seems a simple task, consider that letters have attachments and you will want to know that the page you are viewing is page 3 of an attachment to a 2 page letter dated January 10, 2006. This information needs to be acquired at the time of scan.

After you capture index information as noted above, you need somewhere to input that data so that the images are easy to find and retrieve. Typically this is done with document management software. Most current document management software programs allow for indexing of non-word processing files types, such as .pdf.<sup>2</sup> More sophisticated programs even allow for sound and video files. Some practice management and case management software programs that have document management functionality will also allow for indexing of .pdf and other scanned image file types.

One other consideration at the time of scan is which file format you should use. The litigation world generally uses a basic, standards-based file format called .tif or .tiff. The other format option is .pdf, which is the format Adobe uses for Acrobat. Although .tiff is widely used in litigation, you will probably want to use .pdf, since there are more tools available for managing and manipulating the .pdf format. Newer versions of Acrobat even have OCR functions for extracting text from image based .pdf's.

In summary, you will want quality scans of at least 300 DPI. You will want a scanner with a sheet feeder, so you don't waste staff time scanning one page at a time. You will want tools to help you capture document indexing information at the time of

---

<sup>1</sup> OCR stands for Optical Character Recognition.

<sup>2</sup> .pdf stands for Portal Document Format.

scan. You will want to scan into the .pdf format. And finally, you will need good software tools to help you OCR the scanned images.

### **Paperless “Issues”**

To cover ideas on how you can avoid going to paper, we will cross over into the subject of “issues” you may face when moving away from paper. Many of these issues have ethical aspects and we will cover those as well.

Perhaps the simplest aspect of avoiding going to paper is that you will (and probably already have) e-mail electronic documents instead of printing and mailing paper ones. The first ethical issue this raises has to do with metadata. Metadata is literally: information about information. Practically for a lawyer, this information is about Word and other electronic files. The problem comes about since much of this data is hidden from the average user’s view. A quick look at the document “Properties” in a Word document will show the highest level of metadata. This information tells you when the document was created, who created it and some other basic information about the creator, such as e-mail address and even phone numbers. Additionally, depending on the Word configuration you have, there may be past edits and comments hidden there too.

Ethical issues arise when this metadata may reveal client confidences. If a document was created by doing a “save as” from another client’s document, old information may now be contained in the new document. Or it may be that a lawyer is just e-mailing the document to an opposing counsel. Ethics opinions and dialogues on this issue vary. The basic questions are: should a lawyer have a duty to remove metadata before sending documents? And, should lawyers be prohibited from looking at metadata in the documents they receive? You will want to consult with your local ethics and discipline counsel to find out how your jurisdiction handles this issue. Regardless of the answer, it is still a good idea to remove metadata from documents before sending them. You probably do not want to be the ethics and malpractice test case for your jurisdiction on this issue. So take some steps and set in place policies for your practice about removing metadata before sending out electronic documents.

There are a few ways to remove metadata from documents. The first and simplest is saving documents into other formats, such as .pdf and .rtf. Most lawyers are moving to the .pdf option, as this also limits the ability of the recipient to alter the data in the document. Next easiest is Microsoft, with a metadata removal tool available for free online. It should be noted that most file types carry some level of metadata, even WordPerfect. Finally, there are commercial products available for removing metadata, such as Payne Consulting’s Metadata Assistant. This sells for \$80 and removes metadata from all Microsoft file types.

In addition to stripping metadata, there are also redacting issues. There are tools for redacting text from .pdf files, but this action needs to be done properly so as not to expose the redacted text. An online resource for doing this (from a Federal Magistrate no less) is available here: <http://utd-cmecf.blogspot.com/2006/05/redaction-warnings.html>.

A very common ethics question that comes up in paperless office discussions is: Can I discard/destroy paper documents once I have scanned them? The answer, so far, is yes provided you communicate this with the client. In 2005 Virginia released an ethics opinion (LEOC #1818) that states that lawyers can scan and toss paper documents provided the client is informed and it doesn't harm the client otherwise. Feedback from other states on this opinion has been positive. However, no other states, to my knowledge, have yet released similar opinions.

A final note on ethics and being paperless focuses on security. Paper file rooms are generally secured. There are in secure office buildings in locked rooms (hopefully). Once you have scanned electronic versions, these same files can exist on any number of devices, even your PDA phones. Steps should be taken to make sure this information is secured wherever it is stored. The primary step will be good policy. There are numerous technical solutions for securing data, but the driving factor should be good policy.

First and foremost, all information should be secured with strong passwords. Any mobile devices should be password protected and even desktop computers should be equally secured. There are many online resources available for examples of strong passwords for computers. And there are software add-ons available to improve passwords on PDA's and other mobile devices. Another emerging tool to consider is file encryption software programs. These programs enable strong encryption of files on hard drives and other devices. If a laptop is stolen, even with strong passwords, the extensive access to the device renders it vulnerable. Properly encrypted data will be secure even in this scenario. One example of encryption tools to review is PGP ([www.pgp.com](http://www.pgp.com)). This toolset has both e-mail and file encryption available.

All of the security and ethics discussions point to the need for good information policy management. Lawyers and their clients should have good policies and practices in place for how they create, acquire, maintain and ultimately destroy information. This is especially so since most information lawyers hold belongs to their clients. A great resource for best practices and ideas on information management is the American Records Management Association ([www.arma.org](http://www.arma.org)).

## **Conclusions**

There are many and significant reasons to move away from the paper world into a fully electronic one. Cost savings alone make this a good decision. On top of that value is the increased competitiveness a lawyer will have by being able to better serve clients and share information with them. A core aspect of this process is establishing good systems and processes for scanning paper into electronic forms. This needs to be done in a cost effective and useful method so that the resulting electronic information is of high quality and able to be effectively OCR'd into text for other uses. Once you have scanned documents, you will need to have in place tools for storing and easily retrieving documents. Finally, you need in place good policies and security for maintaining the integrity of your clients' information.