Integrating Technology Into Your Trial Practice

Contributors: Jacob Jesin, Taro Inoue, David Whelan, and Phil Brown
Paper Compiled by: Simon Borys

Presented at the Criminal Lawyers Association 2011 Fall Conference
December 8-9, 2011

Introduction

Technology has the ability to augment and improve any law practice. It need not completely replace any traditional way of doing things, but the potential benefits it offers cannot be ignored.

The thing to remember with integrating technology into your trial practice is that the technology ought to serve you; you should not be serving it. In other words, if it doesn't work for you, don't use it. We are not promoting the idea that using technology is an inherently better way of doing things (which means that you do not necessarily need the latest and best technology, or the most complex); we are simply promoting some of the ways that technology *may* assist you. In this paper we discuss some of those ways specifically. Not all of these ways will be appropriate for everybody, nor are they the only ways of doing things, but regardless of whether you are a sole practitioner or work in a large firm, or whether your practice is restricted to criminal law or you practice in multiple areas, we feel that integrating technology into your practice has the potential to improve it.

Tips on:

The Paperless Office (Jacob Jesin and Taro Inoue)

The paperless office, in law or other industries, is not a particularly new topic, but for those who are still wedded to a completely paper based system it can offer a number of benefits. Those benefits include: saving tress (which helps the environment), reducing office clutter and offsite storage costs, making all files (including closed and archived ones) available on demand and from multiple locations, preventing losses that can arise from destruction, loss, or theft of physical files, and, perhaps above all, organization.

Having a paperless office means more than just typing things up on your computer rather than writing them out. It means making an effort to receive things from others electronically, rather than in paper form (such as transcripts, disclosure, or pleadings), and scanning everything you can't get electronically. It also means making a switch conceptually to a way of doing things that doesn't involve paper as an intermediary. For example, documents do not need to be printed to be faxed anymore. If you need to fax something (as opposed to emailing it, which is preferable), you can use a service like Hello Fax (https://www.hellofax.com/), which allows you to send any electronic document straight from your computer to a physical fax machine. It also allows you to sign documents electronically (using either a pen and tablet or your mouse), so you don't need to print just to sign. Hello Fax even allows you to receive faxes on your computer if they are sent to your digital fax number.

That being said, the world is clearly not paperless yet, so you will still receive things in paper format. For the paperless office to be successful, those things need to be scanned, named and stored appropriately either locally or in a remote location. (This is described in more detail in the sections below.) But scanning takes work and everyone tends to procrastinate work, meaning you should not create any disincentives to scan. Slow or error-prone scanning is a big disincentive, so you should get the best sheet-feed scanner you can afford. A designated scanner (as opposed to an all-in-one machine), such as the Fujitsu ScanSnap S1500 (http://www.fujitsu.ca/products/scansnap/s1500/), is a good choice for a small office.

In order to be effective, your scanning policy needs to be explicitly spelled out and everyone in your office needs to be on board with it. Once documents are scanned, they need to be named and stored appropriately in order to be easily accessible. This is what is known as a Document Management System (DMS). There are lots of legal programs that offer built in document management systems to the sole and small firm, such as PCLaw, Amicus Attorney, etc. However, the best DMS is one that you design yourself that closely mimics the physical filing system that you have already grown accustomed to in your office. As with scanning, your naming and storing policy needs to be clear and everybody needs comply with it.

Here is an example of a paperless office scheme, which is being used by Jacob Jesin in his office:

For Non-Client Specific Files:

1) All non-client specific files are stored in a "top-level" folder entitled "Law Office". We view this file folder as the equivalent to the physical filing cabinet that our office also has.

2) Under the top-level folder are all of the other practice management folders that might be found in a typical office filing cabinet. For example:

    Accounting
    Bookkeeping
    Client Invoices
    Facilities
    Insurance Policies
    Office Correspondence
    Policies and Procedures
    Precedents
    Templates

3) Each subfolder is then further divided into yearly or other specific subfolders as needed.

For Client Specific Files:

1) Everything going out of, or coming into the office is scanned immediately and saved electronically in the DMS according to the DMS rules below. The original document is then physically stamped with a special "star-stamp" in the upper right corner of the document to indicate that it has been entered into the DMS. The physical document is then placed in the physical file while the file is active, and then destroyed once the matter is complete.

2) Word documents created in the office are saved to the appropriate folder with the proper filename according to the DMS rules. The Word file is then converted to PDF and sent out by email or faxed or mailed. The PDF file is kept alongside the original Word file with the same name, but with the PDF extension. A sent fax is scanned immediately, with the fax confirmation sheet, and then saved alongside the original file.

3) Papers that come into the office electronically (e.g. faxes) are never printed and stored in the physical file – they are only stored electronically.

4) Client matters are stored in one of two main sub-folders, under a "top level" folder called "Client Work and Materials". Those two sub-folders are: (a) Active Matters and (b) Closed Matters.

5) Within the Active/Closed folders are the individual matter sub-folders. Each matter sub-folder is titled in such a way as to show the client's name, the year of the charge, the courthouse where the charge is located, and a brief explanation of the charge. This way, multiple matters for the same client appear sorted chronologically and are easily distinguished from each other.

   E.g. Smith, John {} 2011, OCH Domestic Assault

   (Where "{}" indicates that this is an electronic file and "OCH" stands for Old City Hall courthouse.)

6) Under each matter folder are additional sub-folders. The defaults are:

Accounts and Retainer
Bail, Designation and Other Docs
Correspondence – Client and Other
Correspondence – Crown
Disclosure
Memos and Notes

(You can create a "blank folder template" with each of these blank subfolder names inside of it that can be replicated each time you open a new matter.)

7) Other Folders are added, as needed, as the case progresses, for example:

JPT Material
Sentencing Material
Application – 11(b)

8) Within each subfolder are the individual documents. The name of each document always begins with the creation date (not the scanned date or received date). The date is displayed in numeric YYYYMMDD format. This allows the entire folder to be displayed chronologically when the files are sorted by name.

9) Following the date, each filename starts with some standard descriptive words to identify what kind of document is contained in the file. It then includes a few words that describe the actual document. The description is then followed by a hyphen and the client's full name for identification (in case of accidental misfiling). 3 examples are:

20110804 Letter to Crown – Additional Disclosure Request for 911 Audio tape – John Smith.doc
20110905 Fax Letter from Crown – Response to Additional Disclosure Request – John Smith.pdf
20110906 Memo – Notes of Call with Crown to discuss outstanding 911 tape – John Smith.doc

With respect to file naming, one thing to keep in mind, when formulating your risk management strategy, is whether you are comfortable with including the client's name in the

title of the document, which may be visible to unauthorized eyes (an increased risk if your files are stored or backed up using the internet), even if the file itself is locked.

10) When a letter is faxed, a full copy of the letter including the cover page, and fax confirmation printout is then scanned back into the system and named the same as the original work document. A qualifier is then appended to the end of the file name to identify as the actual faxed copy. Example:

    20110804 Letter to Crown – Additional Disclosure Request for 911 Audio tape – John Smith {} FAXED.doc

    (Where "{} FAXED" is the qualifier.)

11) Other Qualifiers can be appended as needed. For example: "{}SCANNED COPY", "{} SENT", "{} SIGNED", or "{} FILED".

File Synchronization (David Whelan)

The practice of law relies heavily on files and, if you are running a paperless office, you may want to access or update those files while out of the office. This can dramatically improve the efficiency of your practice.

One of the easiest ways to do this is to use a file synchronization service. Synchronization creates mirror copies of files across multiple computers, including tablets and mobile devices, through the internet. Synchronization services usually include an access point via a website on the internet, which means you do not even need one of your regular devices to access the files – any computer with an internet connection will do.

Synchronization is distinguished from simple uploading and storing files on the internet, in that, where files are synchronized, changes are reflected across all locations where the file is stored, whereas if the files are only uploaded (and not synchronized), they need to be downloaded to be

worked on, then the new copy needs to be uploaded to the internet to replace the old file and then that file needs to be downloaded manually to replace each individual local copy of the file. This is obviously more time consuming and can lead to problems with different versions.

The one caveat to transmitting or storing files online (which applies whether you are synchronizing or just uploading) is security. While there is no doubt that files transmitted or stored on the internet are not completely secure, neither are paper copies. The amount of risk you are willing to accept with respect to the your use of the internet must be calculated the same as for your paper files, which are often placed in the hands of third parties, such as off-site storage companies. When performing your own risk assessment, keep in mind that the standard that is required of you is not perfection, but only reasonableness.

There are two primary elements regarding the security of your files. The first is to ensure you are using a "strong" password that cannot easily be guessed or cracked. The following are a couple points that you should consider with respect to passwords:

- Use a long password, using upper case and special characters
- Follow the do's and don't's discussed here: http://blog.zonealarm.com/2011/01/securing-yourself-from-a-world-of-hackers.html?view=infographic
- Write it down and store it with your other valuable information (credit cards, etc.)

The second aspect of security focuses on encryption, which creates a protective shell around your files. If your files are not encrypted and they are intercepted or accessed on the internet, the interceptor can read, use, and possibly change the information you are transmitting. File synchronization or uploading sites should encrypt your content both as it is transmitted and when it is stored. When you select your service, be aware of whether it encrypts at both points. While nearly all will encrypt files while they are being transmitted, your service provider may not encrypt stored files. (Encryption is described in more detail in its own section below.)

Some of the common basic file synchronization services are Dropbox (http://www.dropbox.com), Sugarsync (www.sugarsync.com), and Box.net (www.box.net).

Each has slightly different features, including the amount of storage space and the encryption protection they offer. These services also provide premium accounts where you can purchase better security and more space, as well as other features. You may need to purchase the premium account in order to get the complete set of features you need to properly store confidential client files online.

Google Docs (https://docs.google.com/) is a more robust file synchronization service. It addition to synchronizing files it also serves as an online productivity suite where you can edit documents, spreadsheets, and presentations in Google formats, Microsoft Office formats, and a variety of others. Google Docs editing is not as powerful as Microsoft Office, though (it does not have all the same features or functionality), so it is better considered a backup alternative than a replacement.

However, Google Docs, in and of itself, is just an upload and storage service, not a full synchronization service, meaning that if you have not uploaded a specific document to Google Docs, you will not have access to it. Google Cloud Connect (http://tools.google.com/dlpage/cloudconnect) solves this problem. When Cloud Connect is installed on the computer where your files are stored it synchronizes all of your Microsoft Office files with your Google Docs account. Even if you never need to access Google Docs, you can rest assured that the content will be available to you if you are out of the office and need emergency access.

An alternative to Google Docs, which is equally robust but keeps you entirely in the Microsoft universe, is Windows Live Mesh (http://explore.live.com/windows-live-mesh). Live Mesh can store 25 GB of files on Microsoft's Skydrive site and it comes with a set of free Microsoft Office Web apps (which are essentially web based versions of Word, PowerPoint, etc., with more power than the online apps Google offers, but still less than the full versions).

An additional benefit of using Live Mesh is that, through the web apps, you get access a free, albeit stripped down, version of Microsoft OneNote. One Note is a great organization tool for trial preparation, enabling easy organization of testimony and evidence for fast recall. You can

read a fulsome explanation of how here: http://office.microsoft.com/en-us/onenote-help/the-trial-lawyer-s-electronic-notebook-HA010385354.aspx.

If you use any kind of synchronization service, remember that you should consider locking files down with passwords and/or encrypting them to add an extra layer of protection. If you are still uncomfortable putting your files on the internet, you can leave them on your primary office computer and still remotely access them through a Virtual Private Network (VPN), as described in the section below.

Remote Access (Phil Brown)

From a security perspective, accessing your files through the internet on a WiFi connection can be a crapshoot. Your computer and your data is vulnerable to intrusion and interception and the internet connection you think you are making may have been constructed solely for the purpose of stealing your information.

The alternative is to set up your own Virtual Private Network (VPN) to remotely access data stored on your office computer or server. This can be accomplished using either applications built into your operating system, third party software you install on your computer, or subscription service like LogMeIn (https://secure.logmein.com/), GoToMyPC (http://www.gotomypc.com/), BackToMyMAC (a feature in MAC OS X 10.5 Leopard and later), or Tonido (http://www.tonido.com/).

These programs create connections that allow you to access and control your office computer or server from another computer in a remote location, or even from a mobile device. The programs allow you to decide which other computers or devices should have access to your computer and then authorize them. Most of these services also allow for collaboration and you can assign control of your computer to others so they can add to documents or draw on a white board for collaboration, but since this is all done within a Virtual Private Network, the only people or

devices that have access are those that you have authorized and everything is still on your office computer or server.

This is also a great solution for those who want to carry a "clean" laptop when travelling. In the event that it is lost, stolen, or seized, there is nothing on it to be compromised.

Backing Up Your Files (David Whelan)

Your practice's continuity and business viability depends on having your information available when you need it and whether you are running a totally paperless office or not, chances are you have some, or likely a great deal, of important information stored on your computer. If this computer fails, it can mean lost business, missed deadlines, or worse – lawsuits and professional sanctions.

One of the easiest steps to take to avoid this problem is to use an online backup service. Depending on how you practice, it may be sufficient to use one of the file storage or synchronization services described in the section above, however, those services will generally not be used for file types other than documents, nor can they back up your applications or software. If you use specialized software that is installed on your primary computer, you should consider a backup site like Mozy (www.mozy.com) or Carbonite (www.carbonite.com). Both offer inexpensive off-site, online backup for your practice. These are just two examples. For a full list, check out Backup Review's November 2011 look at the top 100 online backup services (http://www.backupreview.info/category/top25/).

One thing to keep in mind with online backups is that your Internet Service Provider (ISP) may have a cap on the amount of data you are allowed to transmit with a fee per GB if you go over that amount. The costs for data overage are usually fairly significant and can add up quickly if you are backing up your entire hard drive. Remember that the cap usually includes the total amount of uploaded *and* downloaded data.

By using an online backup, you immediately address two fundamentals of a good backup regimen: automation (since people tend to forget to regularly do manual backups) and keeping backups off site. With this, if your computer fails, even if your entire office is destroyed, you can still recover quickly by downloading the appropriate software from your provider and activating the stored backup on a new computer.

In addition to (or in lieu of) using an online backup service, you should also consider making local backups yourself. This allows you to access your backups in the event that you need them and you cannot access the internet for some reason. In the past, local backups meant tapes or removable disks or CDs, but now you can simply use an external hard drive (which usually connects through USB), make a mirror image of your entire system and store it wherever you want.

There are a number of programs that will enable you to create your own local backups on an external drive. Windows and Mac both have applications built into the operating system (Windows Backup and Time Machine, respectively) to do this and there are a number of third party applications that can do it as well, such as Acronis (www.Acronis.com) or Norton Ghost (http://us.norton.com/ghost/).

All of these programs allow you to designate which files and folders you want to back up or you can simply backup the entire computer. While backups of the entire drive take up more space and are more time consuming to perform, they allow you to get back up and running faster, in the event you need to use the backup, because you do not have to reinstall and reconfigure every program you had on your computer.

With respect to backing up your bookmarks, internet passwords, web history, and browser plug-ins, most browsers can create a cloud based backup of these items, which can be synced across computers and can be used as a recovery tool if need be.

All backups (cloud based or local), should be routinely testing to make sure they are viable and will be there when you need them. Consider the following recommended procedures:

1. Test your backup to make sure that it contains the latest information. Be aware that sometimes a change in your network settings can disable a backup service without your knowledge.
2. Confirm that any applications that have the ability to back themselves up (such as web browsers) are doing so.
3. Be aware of the health of your portable hard drive. You should periodically test it to make sure the drive doesn't report any errors. A free application like CrystalDiskInfo (http://crystalmark.info/software/CrystalDiskInfo/index-e.html) can give you early warning of potential problems.

Encryption (Phil Brown)

Regardless of whether you are synchronizing your files across multiple devices, uploading them to the internet, or backing them up to the cloud or a local hard drive, encryption is a way to create enhanced protection for your files and the data contained in them. Encryption can be applied to data while it is transit (this is usually done automatically if you are accessing the internet through a secure connection, which is designated by a website beginning with https://) or to information that is stored statically, which is what this section will address. To understand what exactly encryption is, consider the following analogy: if using a password is the equivalent locking your filing cabinet, then using encryption is like having all of the files in that cabinet translated into Esperanto. When they have been encrypted, you need the specific encryption key (the instruction on how to unscramble the contents) to access the information.

Encryption keys can obviously be used in addition to passwords to provide an added layer of protection whether you are storing information in your office, on your laptop, or in the cloud. Without the correct encryption key, even if the password is broken and the content is accessed, it will only be seen as gibberish.

Encryption is fairly easy to apply to your files. There are a number of free and paid software options available for installation on your computer to encrypt confidential information, such as

Truecrypt (http://www.truecrypt.org/), Meo (http://www.nchsoftware.com/encrypt/index.html), MacKeeper (http://mackeeper.zeobit.com/mac-encryption), and Symantec Endpoint Encryption (http://www.symantec.com/business/endpoint-encryption). You should consider using encryption on *all* of your client files *all* the time, but, at a minimum, you should consider using it when you have information leaving the confines of your office, or if you are transferring it to mobile devices that *may* leave your office, such as USB drives or external hard drives.

Encryption is an easy solution to implement and can save you have to call clients later to tell them you have lost their confidential information and advise them they should consider retaining other counsel to look into the possibility of suing you.

Privacy and 3rd Party Service Providers (Phil Brown)

Any of the above mentioned programs or services that transmit or store your data in the cloud can be considered 3rd party service providers. Where the program or service itself is hosted exclusively in the cloud (as opposed to being installed locally on your computer) it is known as Software as a Service (SaaS). The Law Society of Upper Canada does not prohibit the use of cloud based service providers, including SaaS, however the use of any of these programs or services must be approached with the appropriate amount of caution and planning.

If you are using a 3rd party service provider in relation to your confidential client information, you must bear Rule 2.03 of the *Rules of Professional Conduct* in mind. The Rule states that it is incumbent on the lawyer to protect the client's information at all times, and that the lawyer shall not divulge any client information unless expressly or impliedly authorized to do so. This makes it extremely important to investigate the proposed 3rd party service provider with due diligence before entrusting any confidential information to them. The following are some preliminary questions which should be asked before entering into any agreements:

- How long has the provider been around? Is it a company that will be around in a few years or are they under-capitalized?

- In the event of a dispute, who controls the information? (You must have control over it, obviously.)
- How will you recover your information when the relationship ends or the company fails?
- In what form will the company return your data? Will it be in an accessible format?
- How much will it cost to recover information from the company?
- If the company fails, is there an escrow company that will hold your information until you retrieve it?
- Where are the company's computer servers located?
- What kind of security do they provide?

The answers to these and other important questions will often be found in the Terms of Service Agreement that you will have to agree to before using the program or service.

One such example, from the online practice management service "Rocket Matter" (http://www.rocketmatter.com), states:

> If an account is terminated for any reason (by you or us), data existing in the account (including, but not limited to, contacts, calendar entries, uploaded documents, tasks, and so forth) is subject to immediate deletion and in all cases will be permanently deleted within approximately 100 days of account termination. If you do chose to leave us, it's extremely important that you remove your data prior to the expiration for the paid term in effect. [Emphasis added]

In contrast, a second example, from the online practice management service "Clio" (www.goclio.com), states:

> Upon cancellation or termination of a subscription, all Content associated with such subscription will be immediately, and irrevocably deleted from the Service. All Escrowed Data, if any, will continue to remain available for a period of six months upon cancellation or termination of a subscription in accordance with the terms of the Escrow Agreement.

Obviously the second company backs up your information to an escrow provider and, although your information is immediately deleted from their servers, it continues to be backed up on an

escrow server until you recover it. These are the kind of terms you should be looking for before you sign on with any service provider.

In addition to issues of security and recoverability of your information, you should also consider where the information is stored geographically. Most cloud companies are using servers in the USA and this may expose your client information to scrutiny by American authorities, since those servers are subject to American law. If you are using a web based third party provider for services or storage you should consider disclosing the arrangement to your client as part of your retainer agreement to avoid any confusion and to make your client aware of potential risks.

Presenting in Court With Technology (Jacob Jesin)

For the vast majority of criminal cases that are tried by a judge alone, case presentation software and techniques will not be necessary. However, in a jury trial (or a complex case), the impact of utilizing technology to present evidence and submissions in court can make all the difference in the outcome of a case.

In order to effectively present your case in court, you will need to either purchase the appropriate hardware that will allow you to present your material, or ensure (well in advance of trial) that the court support office can provide it. You will likely be using your own laptop or tablet device, but the other items you will need include:

1) Projector with appropriate inputs for your laptop or tablet device
2) Projection screen
3) Power bars and extension cords for all of you devices
4) Cords with the appropriate adapters to connect your laptop or tablet with the projector
5) External speakers and appropriate wires if your material has sound (keeping in mind that internal or cheap external speakers will likely not be loud or clear enough to be heard by everyone in court)

For the most part, the software you need will already be on your computer. Many people have had success using PowerPoint or Keynote presentations in their closing arguments to a jury. The presentation allows you to lay out a difficult case in visual blocks for the jury so that they can follow along during the presentation. You can add video clips, pictures, copies of exhibits, charts, graphs, sound clips, and virtually any other media you can think of, to your presentation in order to consolidate your theory of the case before the jury. If your case involves multiple exhibits that need to be examined side by side, it can be helpful to put a copy or picture of those exhibits up on the screen so that the jury can see the comparison while you talk about it.

It is a good idea to have someone else operate the technology during your presentation. There is nothing more distracting than a lawyer fumbling with his presentation and having trouble getting the materials displayed on screen while they are trying to also talk about the materials.

It is also a good idea to do a few rehearsals, ideally in the court with the same hardware you will be using, before the date of the actual presentation. You should consider having a backup plan in case the hardware does not work. That might include a second copy of your presentation on a flash drive, a second laptop, extra power cords, and, ultimately, paper copies of your presentation. Despite your best efforts with technology, it often seems to not work when it is most needed. You should ensure that you are effectively able to present your case the old fashioned way if that happens.

There are a number of software developers out there that have created programs specifically for case presentation in the courtroom. Some of these programs can be used on devices like an iPad, and are available from Apple's App Store for less than $100. For example TrialPad ($90, http://www.trialpad.com/), Exhibit A ($10, http://www.lecturaapps.com/), or RLTC: Evidence ($5, http://www.rosenltc.com/app.html). Their features vary greatly and it is a good idea to do your research about any of these programs before you buy them to ensure that it will address your specific needs.

Internet in Court (Taro Inoue)

It seems that whenever they build a new courthouse they have grandiose plans for how "wired" or "wireless" it will be. The end result has often been disappointing. The solution to this problem is: Get your own internet! Don't rely on court administration to provide it. Not only will this keep things simple and under your control, it will give you an advantage over the Crown!

Mobile internet options include “rocket sticks”, such as the one from Rogers (https://www.orderrogers.ca/rocket/stick#/overview) or tethering your smart phone with data plan to your computer using a USB cable or Bluetooth and a program like Tether (http://tether.com/).

Recording Testimony in Court (Jacob Jesin and Taro Inoue)

One of the least known uses of technology in a trial practice is the ability to record witness testimony at a trial for later review. Section 136(1) of the *Courts of Justice Act* generally prohibits the taking of audio recordings of a court hearing, however, the following exception is contained in subsection (2)(b):

> Nothing in subsection (1) prohibits a lawyer, a party acting in person or a journalist form unobtrusively making an audio recording at a court hearing, in the manner that has been approved by the judge, for the sole purpose of supplementing or replacing handwritten notes.

On April 10, 1989, the Ontario Courts Advisory Council approved the following practice direction by Chief Justice W. G. C. Howland, the Chief Justice of Ontario:

> Subject to any order made by the presiding judge as to non-publication of court proceedings, and to the right of the presiding judge to give such directions from time to time as he or she may see fit as to the manner in which an audio recording may be made at a court hearing pursuant to section 146 [now section 136] of the *Courts of Justice Act* the unobtrusive use of a recording device from the body of the courtroom

> by a solicitor, a party acting in person, or a journalist for the sole purpose of supplementing or replacing hand written notes may be considered as being approved without an oral or written application to the presiding judge.

There is some debate as to whether this practice direction is still in effect and you should probably request permission from the trial judge to avoid any potential problems down the road.

There are a number of programs that allow you to simultaneously record audio on your laptop while taking typed notes at the same time. The main feature of these programs is their ability to put a place marker at each line of notes and match that place marker to the correct point in the recorded audio file. This allows you to click on the different place markers throughout the document and actually hear what was being said in court as you were typing out that specific line in your notes.

Many people are surprised to learn that the newest versions of Microsoft Word for both Mac and Windows already come with this function built in. In Word for Mac you must open a new document template in the "Word Notebook Layout" in order to access the audio controls that will allow you to record as you type. Microsoft OneNote also allows you to perform the same function.

There are also a number of other notebook programs that can be used to record audio and typewritten notes in the same way. Each of these programs has their own set of features which you might find useful within your practice. Two examples are Circus Ponies Notebook for Mac (www.circusponies.com) and Evernote for Mac and PC (http://www.evernote.com/).

For those of you who don't feel comfortable taking notes on a laptop and still want to use a pen and paper, you might consider one of the special note recording pens on the market. One of the more popular ones is the Livescribe Pen (http://www.livescribe.com) for both Windows and Mac. With the Livescribe Pen you write notes in specially printed notebooks (of actual paper). The pen simultaneously records a digital image of the notes that you are writing on the page as well as the audio in the room. You can then download the handwritten notes to your computer

from the Pen, along with the audio recording. When you click on a section of the notes, you will be able to hear what was actually being recorded while you were writing.

For any of these options that involve recording audio, you might want to consider buying an external microphone attached to your laptop for input in order to better increase the range and clarity of the audio recording.

With current technology there is no accurate way to have this kind of recorded testimony transcribed without human input. In other words, you cannot simply take the audio recording and feed it into transcription software, such as Dragon Naturally Speaking (http://nuance.com/dragon/index.htm), and expect a transcript of the recording to be produced. Generally, transcription software needs to be trained to one specific voice for it to accurately transcribe that person's voice.

Appendix of Products and Services Referenced Throughout the Paper

It should be noted that we are not specifically endorsing any of the programs or services mentioned in this paper. Whether any of the programs or services we have mentioned serve your particular needs is a determination you will have to make after fully assessing your needs and investigating your options. It should also be noted that the programs and services we have mentioned are not an exhaustive list. There are many more available and you may well find one that suits your needs even better.

Product	Website	Page Ref.	Product Description
Hello Fax	https://www.hellofax.com/	2	Allows you to files on your computer to physical fax machines, also allows you to receive faxes directly to your computer
Fujitsu ScanSnap S1500	http://www.fujitsu.ca/products/scansnap/s1500/	2	Document scanner
Dropbox	http://www.dropbox.com	7	File synchronization service
Sugarsync	www.sugarsync.com	7	File synchronization service
Box.net	www.box.net	7	File synchronization service
Google Docs	https://docs.google.com/	8	File synchronization service
Google Cloud Connect	http://tools.google.com/dlpage/cloudconnect	8	File synchronization service
Windows Live Mesh	http://explore.live.com/windows-live-mesh	8	File synchronization service
LogMeIn	https://secure.logmein.com/	9	Creates a virtual private network
GoToMyPC	http://www.gotomypc.com/	9	Creates a virtual private network
BackToMy MAC	A feature in MAC OS X 10.5 Leopard and later	9	Creates a virtual private network
Tonido	http://www.tonido.com/	9	Creates a virtual private network
Mozy	www.mozy.com	10	Online backup service
Carbonite	www.carbonite.com	10	Online backup service
Acronis	www.acronis.com	11	Software for creating your own backups
Norton	http://us.norton.com/ghost/	11	Software for creating your own

Ghost			backups
CrystalDisk Info	http://crystalmark.info/software/CrystalDiskInfo/index-e.html	12	Hard drive diagnostic tool
TrueCrypt	http://www.truecrypt.org/	13	Encryption Software
Meo	http://www.nchsoftware.com/encrypt/index.html	13	Encryption Software
MacKeeper	http://mackeeper.zeobit.com/mac-encryption	13	Encryption Software
Symantec Endpoint Encryption	http://www.symantec.com/business/endpoint-encryption)	13	Encryption Software
Rocket Matter	http://www.rocketmatter.com	14	Online practice management software
Clio	www.goclio.com	14	Online practice management software
Trial Pad	http://www.trialpad.com/	16	Court presentation software for iPad
Exhibit A	http://www.lecturaapps.com/	16	Court presentation software for iPad
RLTC: Evidence	http://www.rosenltc.com/app.html	16	Court presentation software for iPad
Rogers Rocket Stick	https://www.orderrogers.ca/rocket/stick#/overview	17	Mobile internet
Tether	http://tether.com/	17	Mobile internet
Circus Ponies	www.circusponies.com	18	Electronic note taking with simultaneous audio recording
Evernote	http://www.evernote.com/	18	Electronic note taking with simultaneous audio recording
LiveScribe Pen	http://www.livescribe.com	18	Physical note taking with simultaneous audio recording
Dragon Naturally Speaking	http://nuance.com/dragon/index.htm	19	Voice transcription software