FORDEFENCEMAG 33-1-F2

For the Defence — The Criminal Lawyers' Association Newsletter

For the Defence — Vol. 33, No. 1
33-1-F2 — Integrating Technology Into Your Trial Practice

33-1-F2 — Integrating Technology Into Your Trial Practice

Contributors: Jacob Jesin, Taro Inoue, David Whelan, and Phil Brown

Compiled by: Simon Borys

Adapted From the Paper Presented at the Criminal Lawyers Association 2011 Fall Conference.

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. This article is 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); it is simply promoting some of the ways that technology *may* assist you.

In this article 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.

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.

The Paperless Office

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 paper, 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 and disclosure), and scanning everything you can't get electronically. But scanning takes work and everyone tends to procrastinate, 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 purpose built scanner (as opposed to an all-in-one machine), such as the Fujitsu ScanSnap S1500[FN1] is a good choice for a small office.

The backbone of an effective paperless office is not actually the scanner but the document naming system you implement. There is no one right way to name your files, but whatever system you chose should have both uniformity and clarity and should closely mirror your existing paper filing system. A good example of a document naming system, which the system described in the original paper is based on, is Donna Neff's.[FN2]

File Synchronization

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 can also be accessed 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 finally 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 confusion with different versions.

Some of the common file synchronization services are Dropbox,[FN3] Sugarsync,[FN4] and Box.net.[FN5] Each has slightly different features, including the amount of storage space and the encryption protection they offer. These services also offer premium accounts where you can purchase better security and more space, as well as additional features. You may need to purchase the premium account in order to get the complete set of features and security you need to properly store confidential client files online.

Google Docs[FN6] is a more robust file synchronization service. In 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 editing in 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[FN7] 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 ever

out of the office and need emergency access.

If you use any kind of file synchronization service, remember that you should consider locking files down with passwords and/or encrypting them to add an extra layer of protection (encryption is described in its own section below). If you are still uncomfortable with the idea of having your files flying through the internet to be synced from one computer to another, you can just leave them on your primary office computer and access them remotely through what is known as a Virtual Private Network (VPN). A VPN allows you to access not just your files but your entire computer, including all of your software, meaning you can essentially temporarily turn another computer, or even a mobile device, into your office computer.

A VPN can be set up using either applications built into your operating system, third party software you install on your computer, or subscription service like LogMeIn,[FN8] GoToMyPC,[FN9] or Tonido.[FN10]

A VPN 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.

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.

Backing Up Your Files

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 synchronization services described in the section above (excluding the VPN option) as a backup, because the files are stored on multiple computers. However, those services are generally not used for file types other than documents, nor can they back up your applications or software. If you use a standalone computer and have specialized software installed or files other than documents that you need preserved, you should consider a backup site such as Mozy[FN11] or Carbonite.[FN12] 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.[FN13]

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 regularly. Remember that the bandwidth 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, or even if your entire office is destroyed, you can still recover quickly by 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. The advantage physical backups have over online backups is that they allow you to access your backups in the event that you need them and you cannot access the internet for any 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 the external drive 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 [FN14] or Norton Ghost.[FN15]

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.

All backups (cloud based or local), should be routinely tested to make sure they are viable and will be there when you need them.

Encryption

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 gibberish. When they have been encrypted, you need the specific encryption key (the instruction on how to unscramble the contents) to access the information. Therefore, encryption keys can 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.

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,[FN16] Meo,[FN17] MacKeeper,[FN18] and Symantec Endpoint Encryption.[FN19] 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 confidential information leaving the confines of your office, or if you are transferring it to portable devices that has the potential to be removed from your office, such as USB drives or external hard drives.

Encryption is an easy solution to implement and can save you having 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.

Encryption is an easy solution to implement and can save you having 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 Third-Party Service Providers

Any of the companies that provide the above mentioned services or programs can be considered third-party service providers. The Law Society of Upper Canada does not prohibit the use of third-party service providers that transmit or store data in the cloud, however the use of any such programs or services must be approached with the appropriate amount of caution and planning.

If you are using a third-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 third-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?
- 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?
- In the event of a dispute, who controls the information? (You must have control over it, obviously.)

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.

In addition to issues of security and recoverability of your information, you should also pay particular attention to where the information is stored geographically. Most 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 third party provider for file transfer 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.

If you are using a third-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 third-party service provider with due diligence before entrusting any confidential

information to them.

Presenting in Court With Technology

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 other items you will need include: a projector, a projection screen, power bars and extension cords, external speakers, and the appropriate connectors for everything.

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 aid 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 their presentation and having trouble getting the materials displayed on screen while they are also trying to 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[FN20] ($90), Exhibit A[FN21] ($10), and RLTC: Evidence[FN22] ($5). 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

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,[FN23] or tethering your smart

phone with data plan to your computer using a USB cable or Bluetooth and a program like Tether.[FN24]

Recording Testimony in Court

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, subsection (2)(b) contains an exception for lawyers to "unobtrusively" make audio recordings "in a manner that has been approved by the judge" for the sole purpose of supplementing or replacing their 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 specific 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 typed 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 in your practice. Two examples are Circus Ponies Notebook for Mac[FN25] and Evernote for Mac and PC.[FN26]

For those 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[FN27] 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 handwritten 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 micro-

phone 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 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.

FN1. http://www.fujitsu.ca/products/scansnap/s1500/

FN2. http://apps.americanbar.org/lpm/lpt/articles/ftr09091.shtml

FN3. http://www.dropbox.com

FN4. www.sugarsync.com

FN5. www.box.net

FN6. https://docs.google.com/

FN7. http://tools.google.com/dlpage/cloudconnect

FN8. https://secure.logmein.com/

FN9. http://www.gotomypc.com/

FN10. http://www.tonido.com/

FN11. www.mozy.com

FN12. www.carbonite.com

FN13. http://www.backupreview.info/category/top25/

FN14. www.Acronis.com

FN15. http://us.norton.com/ghost/

FN16. http://www.truecrypt.org/

FN17. http://www.nchsoftware.com/encrypt/index.html

FN18. http://mackeeper.zeobit.com/mac-encryption

FN19. http://www.symantec.com/business/endpoint-encryption

FN20. http://www.trialpad.com/

FN21. http://www.lecturaapps.com/

FN22. http://www.rosenltc.com/app.html

FN23. https://www.orderrogers.ca/rocket/stick#/overview

FN24. http://tether.com/

FN25. www.circusponies.com

FN26. http://www.evernote.com/

FN27. http://www.livescribe.com

END OF DOCUMENT