We hope that you enjoyed Veritext’s TechnoEthics class. As part of this informational program we’ve created a supplemental iBook, which further details the items referenced in the class. If you are reading this as a PDF or paper document, be sure to download our free iBook from the iTunes bookstore in order to gain full access to the interactive content. Enjoy, and as always, if you have any questions, please give us a call!

Veritext
www.veritext.com
P: 800-567-8658
First Bug
Back on September 9, 1945, U.S. Navy Officer Grace Hopper was operating one of the earliest computers. While running the programs, Grace kept seeing errors, and since the code was correct, the errors did not make sense. After a lengthy investigation, she discovered a computer bug. It was the first computer bug actually, but not the type of bug you might be thinking. It was an actual bug. A moth had become stuck in the machine causing it to malfunction. What you see here is that actual bug taped to her notes for that day. You’re looking at the first computer bug. We’ve come a long way since then considering many of the computers we use these days have chips that are not even the size of that bug!
The birth of the world’s first digital electronic computer was ushered by war. Completed in 1946, ENIAC was a behemoth of a computer. It measured 8.5 feet by 3 feet by 80 feet (2.6 m x 0.9 m x 26 m), covered an area of 680 sq. feet (167 m²), and weighed 27 tons. The complex machine contained 17,468 vacuum tubes, 7,200 crystal diodes, 70,000 resistors, 10,000 capacitors, 1,500 relays, 6,000 manual switches, and over 5 million hand-soldered joints. The machine was so power-hungry it required 150 kilowatts of electricity. It was rumored that, when ENIAC was turned on, Philadelphia suffered brownouts!

Ethical Obligations

Why is it important to look at the ethical issues surrounding the use of technology in the legal field? Looking at the myriad of ethical opinions, one major topic is that of technology and security. A major aspect of that is the confidentiality of your clients' information. There are several parts of the *ABA Model Rules of Professional Conduct* that address the ethics of technology:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education, and comply with all continuing legal education requirements to which the lawyer is subject. Rule 1.1 (8)

A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. Rule 1.6 (C)

A client may require the lawyer to implement special security measures not required by this Rule... Rule 1.6 (18)

When transmitting a communication that includes information relating to the representation [for instance email] of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. Rule 1.6 (19)
Why a Reporting Company?

Why is a court reporting company talking about the ethics of technology? We would make the argument that it is even more important for a court reporting company to take the confidentiality of clients’ information seriously. Not only do we have one firm’s clients’ data, we have hundreds, if not thousands, of sometimes highly, highly confidential pieces of information. Whether it is the transcript itself or the exhibits attached to it, we handle confidential information on a large scale. Last year, Veritext took over 300,000 depositions, hearings, mediations and trials. You can imagine how much confidential information was included in those millions of pages. We see social security numbers, medical records, financial information, trade secrets, and the list goes on and on. We have to take information security seriously, which is why we put this CLE together. We wanted to share, not only industry concerns and best practices for information security, but also the experiences we went through while shoring up our security.

Two Types of Information

Information is interesting. There are two basic types of private information: disposable and detrimental. Disposable information would be something like a credit card. If someone obtained it, you could call your credit card company and have the account cancelled. They would send you a new card, and there would be minimal damage and no ongoing damage. You could move on with a new card or account. (Chances are the credit card company would eat the charges anyway.) But then there is the detrimental information, such as medical information or proprietary company information. If your medical records are released, there is no going back. There is no way to get that “genie back in the bottle.” The news is out. The same goes for company information. Once the secret ingredients to Coca Cola are out, they are out. Everyone knows. There is no way to “start a new account” like a credit card. So you can see how this second type of information is much more significant. Chances are you deal much more frequently with detrimental information than disposable information. Either way, you have an ethical obligation to keep both private.
**Ever-Evolving Technology**

Technology moves fast. Really fast. Much faster than the law. However, that is no excuse. We need to keep up. Just as ignorance of the law does not protect you, ignorance of computers does not either. Years ago we could buck this trend and continue to practice law the “old-fashioned” way, yet this is no longer an option. Our other CLEs cover how to use the latest and greatest tools available, but this one will not. This one will examine the ethical obligations that surround the use, or even misuse, of technology. This being equally as important and potentially much more dangerous a topic to ignore. From sending emails to encryption even to what the future holds with quantum computing, this CLE will show you what your ethical responsibilities are as an attorney and as a firm.

**What Hacking Isn’t**

Despite the hundreds of movies and TV shows that show hackers hard at work, usually zooming through 3D models of a computer, and with a few clicks cracking the most sophisticated networks, it is a far cry from that. Often, it is countless hours of boring code or network analysis, looking for a flaw or flaws that will give them access. That said, there are much more user-friendly hacking “packages” that are available for sale or downloading, giving hacking an unfortunately low barrier to entry.

**Movie 1.1 What Hacking Isn’t**

Packet Sniffing

If you are a road warrior, you probably send a fair amount of email from café hotspots or hotel hotspots, a wifi connection that potentially anyone can be surfing with you or even Packet Sniffing with you. What is Packet Sniffing? As you communicate via wifi, packets of information are sent through the air between you and the hotspot. These packets contain the information you are accessing. It could be your password being sent to your email server to access your email, or it could be the emails themselves. The hotspot is not the only one who can read these packets; they are floating through the air after all. Packets can be sent as “clear text” (unencrypted), which means anyone can read them and they are in plain English. Packets can also be sent on an encrypted connection, which means even though people can see them, all they can see is garbled characters.

If you are communicating with a client and including confidential information, such as medical information, proprietary company info, social security numbers, et cetera, you will want to make sure no one can see that.

Let’s go back to talking about email and wifi. When sending email, especially over a public wifi network, it is imperative to use an encrypted connection. This means there are several ways to send email. Most of you probably use Exchange, the premiere email server by Microsoft. If you have the latest version and use encrypted connections, you are all set. However, if you use a protocol like POP (commonly used in webmail services) you are sending email in the clear.

For example, if you are using the initial connection to the webmail service, you will see your user name and password being entered. A few lines later, there is the email that you typed. Everything is right there for anyone to read. Someone could be sitting just feet away from you, sipping their coffee, capturing everything you do online. The best part is the software they use to do this is freely available, which is called “Wire Shark.” If you are ever feeling “techie,” you can download it. You will be amazed at the sheer volume of information that is sent via wifi. Even when you think your computer is just sitting there, it is actually communicating online. Here is just a 10-
second loop of the wifi activity in our office. Pretty staggering, isn’t it?

**Virtual Private Network (VPN)**

If your firm has its own email server, for instance, Microsoft Exchange, the best solution is to use a VPN connection to your network. This is a secure tunnel that funnels all your web activity, completely encrypted, through your firm’s secure connection. This is the most secure way to browse and work on open access points or public wifi. This is definitely something to talk with your IT department about setting up for mobile attorneys. To give you a few examples of VPN software, there is Open VPN. This is an open source product, freely available. Another option is to use the built-in VPN functionality with Windows. While it does not have as many features as a stand-alone VPN solution, it might be all you need. The VPN we use at Veritext is Aventail Connect from Dell. Connecting with this VPN, the computer can be used the same way as if it were sitting in the office. It can access network drives, printers, email, and the intranet.

How do we handle email? We treat this with the upmost security. On our desktops, we require a VPN connection in order to check our email via Outlook. This VPN connection requires two factor identification. This means it requires two pieces of identification from you in order to connect. In our case, we use our Windows password as well as a token generator. This prevents someone who stole a password from accessing our information. They would need both the password and the token generator to gain access, making it much more difficult.

The same is required for our webmail. On our mobile devices we use an app called Good for Enterprise. This gives us the most sophisticated control over our mobile devices. Good not only checks our services each and every time email is accessed, to ensure that account is still active, but also gives us great control over the mobile devices. With this, we can enforce pass codes on the phones and wipe (erase) lost or stolen devices instantly. With Good installed on iPhones, iPads, Androids, and Blackberry
devices, our IT department has complete control over all our mobile devices, while still allowing employees to use the latest mobile hardware and apps.

**Multi-Factor Authentication**

In the unfortunate event that your password does fall into the wrong hands, what can be done to add an extra layer of security? Normally when logging into a network, a website, et cetera, it will ask you for two factors of authentication: your username and your password. This means the hacker only needs to gather two pieces of information to access your files. What if we add one more layer? In fact, what if we add a layer that requires a physical piece of equipment to access your files? It will substantially increase the security by adding one more piece of information required for access: a token code. This is a small device that generates number “tokens” at fixed intervals. The user simply clicks a button, and the code is displayed. These codes are time sensitive, so if not used immediately, the user needs to generate a new one. This means that unless the hacker has the actual physical device in addition to your user name and password, they cannot get access. This extra layer of security can drastically reduce your chances of unauthorized access. Normally, these are used in conjunction with VPN access but are even now available in such servers as Gmail, Dropbox, online banking and more.

**Cloud Services**

If this was web 1.0 or early internet, web 2.0 or cloud services, or the modern internet, they leverage the Cloud to allow us to do some pretty amazing things. But what is the Cloud anyway?

When engineers were diagramming computer networks, times include the what shape the internet? They just drew a shape. This cloud represented the internet. Over time, people referred to services that leveraged the internet as “Cloud Services.” This really just means they use a computer somewhere out there on the internet.
How does this impact the legal field? If the services you are using use the cloud, that means your data is stored on some other computer, some place out there on the internet. You are required to make sure the data on that machine is just as secure as the computer on your desk. You need to ensure the services you use keep their data secure, encrypted and backed up. You need to review their security policies and ensure they comply with your own firm policies.

For example, Siri. IBM actually banned the use of Siri, the voice transcription service on iPhones, due to security concerns. With Siri, your voice is recorded, sent to a server for transcription, and then sent back. In order to improve their transcription quality, Nuance occasionally examines the recordings. IBM was concerned their confidential, proprietary information might be leaked. While this example might be a little paranoid, it exemplifies the fact that you do need to be concerned with any data in the “cloud.”

(www.pcmag.com/article2/0,2817,2404786,00.asp)

http://www.pcmag.com/article2/0,2817,2404786,00.asp

When you use Siri or Dictation, the things you say will be recorded and sent to Apple in order to convert what you say into text and to process your requests. Your device will also send Apple other information, such as your first name and nickname; the names, nicknames, and relationship with you (e.g., “my dad”) of your address book contacts; and song names in your collection (collectively, your “User Data”). By using Siri or Dictation, you agree and consent to Apple's and its subsidiaries' and agents' transmission, collection, maintenance, processing, and use of this information, including your voice input and User Data, to provide and improve Siri, Dictation, an dictation functionality in other Apple products and services.


Another example of a great cloud service that could potentially expose your firm is DropBox. This is an incredibly easy way to share files with multiple computers, which is exactly why we at Veritext blocked it. You can imagine the incredible amount of confidential data we deal with every day. From medical records, to social security numbers, to confidential movie star gossip, we needed to ensure it was not a simple drag-n-drop for someone to steal that data. These are the things you need to be aware of when crafting an IT policy. It is not just the security of the data, but the ease in which a rogue employee might steal that data.

The ABA compiled a great chart that shows the opinion of many states on cloud computing. You can find the whole chart online here:

http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html
Flaws in internet security are not always specific to one particular service. In our previous example, the bug effected only Dropbox. However, sometimes vulnerabilities arise that effect a multitude of services and websites. The Heartbleed Bug is an example of a bug in an encryption tool known as Open SSL that is used by over 500,000 websites. Open SSL (stands for secure sockets layer) is an open-source tool that is utilized to encrypt activity while using secure websites. You probably already know that most url’s start with HTTP, but sometimes you might notice that url’s of the sites you use switch from HTTP to HTTPS. The url switches to HTTPS indicating that entered a “secure” layer of the internet that is now using encryption so your activity can not be observed. That is, until, the heart bleed bug was discovered.

The heart bleed bug is an inherent flaw in Open SSL and anyone that knew how to exploit it could look in on all activity that was being encrypted by Open SSL. This meant that an individual could potentially get access to the master keys themselves (the keys used to encrypt everything) and decrypt all activity! This became a problem for hundreds of thousands of services and websites. Bank accounts, cloud storage and backups, email accounts, etc., were all potentially vulnerable to such an attack.

Luckily an update was developed for Open SSL that resolved the Heartbleed Bug, but only those that installed the update corrected the vulnerability. This means that the Heartbleed Bug still exists today! Bugs like this will always come up, and it’s important for companies to pay attention and make sure their security is up to date. This also means that its integral for common users to pay attention to those email alerts that come from the services that we use; they could potentially be an alert notifying us of a flaw that has made the service insecure.

The password service LastPass created a test site where you can enter URLs and it will assess the status of the site against the Heartbleed Bug: https://lastpass.com/heartbleed/

Also the security firm Qualys has another testing platform that they created as well (https://www.ssllabs.com/ssltest/index.html).

You can run the check on both sites. Keep in mind this is to check URL’s that are using Open SSL so the URL will start with HTTPS.
Virtual Depositions
As the cost and inconvenience of travel grows, many attorneys have looked for other alternatives. For a while now, videoconferencing has been a great alternative and still is; however, people realized that nearly everyone has a webcam built into their laptop. So why not use Skype? Skype is a fantastic tool for staying in touch with relatives but is not a business level application. For instance, take the use of Skype in the recent Zimmerman trial. Lacking the needed security of an enterprise level application, numerous other calls disrupted the questioning resulting in a very embarrassing event and a very upset judge. Just like an in-person deposition, access to the “room” needs to be strictly controlled. You can’t have anyone just wander in to the preceding. Additionally, enterprise services enable many parties to participate, a limitation of Skype. Virtual depositions are fantastic and will greatly reduce costs for clients while improving your productivity; however, they need to be conducted with the level of responsibility a deposition requires.

Movie 1.3 How to NOT Take Remote Testimony

Movie 1.4 How to Take Remote Testimony
Password Policies

There has been a newly updated list of the most popular Internet passwords for 2014. Because these passwords are the most common, they’re also the most vulnerable when it comes to digital security.

1. 123456
2. password
3. 12345678
4. qwerty
5. abc123
6. 123456789
7. 111111
8. 1234567
9. iloveyou
10. adobe123


You don’t have to acknowledge if the password you use is on that list, but you should rush to change it if it is. Additionally, take a look around for anyplace you wrote the password down that is visible. Maybe it is written on a post-it note attached to your monitor. Often users ask the IT department why they can’t install programs on their computer without IT’s approval, basically asking why they don’t have Admin privileges over their own machine.

To address these objections, IT Admins will usually walk over to the nearest desk, flip over the phone, and underneath it is written their password. Frequently, it is the name of the company. This is something that would take a hacker about two seconds to guess.

While it may be frustrating to remember long passwords and have to change your passwords often, it is the simplest precaution you can do to protect yourself. It can be equated to a seatbelt: a simple act that can have life-saving ramifications. So how do you create a complicated password and then remember it? What if we add a few extra charac-
ters? There is a very useful site called www.howsecureismypassword.net. Here you can enter your password, and the site will tell you just how long it will take a hacker to crack that password. A common practice among IT professionals to create secure passwords was to use L33T speak (pronounced “Leet” speak). It is simply replacing characters with other characters to break up a word. But even passwords with common substitutions like “dr4mat1c” can be vulnerable to attackers’ increasingly sophisticated technology, and random combinations like “j%7K&yPx$” can be difficult to remember. One way to create more secure passwords that are easy to recall is to use passphrases — short words with spaces or other characters separating them. It’s best to use random words rather than common phrases. For example, “cakes years birthday” or “smiles_light_skip?” smart.

Security is a teeter-totter. You cannot have the best of both worlds. You cannot either have “ease of use” or “security” or a balance of each. For instance, it is hard to have a 32-digit, completely random password, however, very secure. Likewise, it is very easy to remove a password altogether, but completely unsecure. The trick is to find that balance between “ease of use” and “security”. There is no simple solution.

There are a few applications called password managers. A few particular favorites are LastPass and 1Password. These will help you generate incredibly secure passwords, but help you remember them. These are great tools because they help to avoid a big pitfall in security, and that is using the same password on multiple sites. This becomes a problem when just one of the
sites has a security breach. For instance, in July 2012, many Dropbox users experienced SPAM. It was discovered that this was not a flaw with Dropbox but, in fact, another service that had a breach. The users that had the same login and password for that service as Dropbox were not vulnerable. While it is difficult to remember a variety of passwords to a variety of sites, it can go a long way if one of those sites has a breach. This is another thing a program like LastPass can help with.

**Where Computers Go When They Die**

If Phillip K. Dick asked, “Do Androids Dream of Electric Sheep?” we ask, “Where do computers go when they die?” This is actually a serious matter. The majority of the world’s electronic waste ends up in a small corner of Ghana called Agbogbloshie. Commonly referred to as the world’s “digital dumping” ground, chances are your old computers and their hard drive’s contents are sitting there right now. This is a problem because organized criminals have been able to retrieve confidential information from major governments and corporations due to the fact that most hard drives are just thrown away, not erased prior to disposal.

A specific incident involving a HIPAA breach in hard drive security occurred in 2013 and involved Affinity Health Plan, Inc. Over 300,000 individuals may have been affected when Affinity impermissibly disclosed the protected health information of the affected individuals when it returned multiple photocopy agents to leasing agents without erasing the data contained on the copier hard drives.

For more information on safeguarding sensitive data stored in hard drives of digital copiers, click HERE.
An application that will erase your old hard drives before disposal is KillDisk. This application will comply with the most stringent standards adhered to by many governments, including our own. This is a far more effective process than just deleting the files before disposal. Just deleting files does not actually delete the files. It simply tells the hard drive it can now use that space if it needs it. The data is actually still sitting there, which is why forensic data technicians can recover old, “deleted” files. KillDisk, or a similar application, will actually write over the data with new data, often several times, ensuring none of the original information is retained. While it may seem like a lot of extra work, just imagine throwing away a client file without shredding it first.

**Things to Remember**

In closing, there are some crucial items to remember that will ensure you are compliant with your ethical duties to keep clients’ information safe and secure.

- Two types of information: Disposable and Detrimental
- While all confidential information should be kept secret, particular care must be used when dealing with the second type of information. Once that cat is out of the bag, there is no going back.
- When traveling, connect via a VPN
- Having that secure tunnel to the internet is imperative while traveling. There is no knowing who is sitting around you “listening” in on everything you send.
- Implement multi-factor authentication
- Passwords can be guessed, discovered or leaked, but with another factor of authentication standing between the hacker and your files, you are much safer.
- Use caution when using cloud services
• The ease and functionality of cloud based services are alluring, but ensure they have safeguards in place to keep your data private. Also, refer to your local state’s opinion on using cloud services.

• **DO NOT** use Skype for depositions

• When participating in virtual depositions, ensure you are using enterprise level tools and leave the Skyping for the relatives.

• Use secure passwords

• One of the simplest things you can do to ensure better security.

• Thoroughly erase your old hard drives

• Just as you would never throw away an unshredded client file, make sure your hard drives are digitally “shredded.”

**• Stay updated on technology!**

Technology changes and changes fast. While it can be difficult to stay up on the latest tools, it is imperative for an attorney wanting to practice in this modern age.