Group Legal Services Association

Solo, Small Firm, and General Practice Section

2016 Joint Spring Meeting

May 11-14, 2016, Key West, Florida

Ethically Using Technology to Take Your Practice to the Next Level: Easy as (Key Lime) Pie

---

Saturday, May 14
8:15 am – 9:15 am
Salon A-1

Presenter: Alan Klevan, Law Offices of Alan J. Klevan, Newton Highlands, MA

Alan Klevan

Alan Klevan is the principal of The Law Offices of Alan J. Klevan, P.C. in Newton, Massachusetts. He concentrates his practice in the fields of workers' compensation law, automobile tort law, and general negligence law. He is also the owner of Summit Law Practice Solutions, a legal consulting firm focused on assisting solo practitioners and small law firms leverage their skills with emerging and existing technologies in order to maximize efficiency and profitability.

As a practicing attorney for over twenty-five years, Alan has seen how technology has changed the shape of how law is both practiced and marketed. Passionate about both his business and personal injury law practice, Alan has given over one hundred presentations since 2001 about how there has been a gradual paradigm shift in the last decade from mid-size and large law firm practice being the norm to solo and small firm practice, thus creating greater competition among lawyers for business.

Successful law practice management is comprised of four distinct categories – marketing, finance, practice and technology. There must be a balance among all four of these in order to run and maintain a successful law practice. Alan created Summit Law Practice Solutions to provide support to solo practitioners and small law firm practices in each of these categories.

In August of 2009, the American Bar Association's General Practice, Solo and Small Firm Division awarded Alan its "Solo and Small Firm Trainer of the Year Award" for his contribution to educating lawyers and law students about the opportunities of a small and small firm practice. Presently, Alan serves on the Editorial Board of the American Bar Association's General Practice Solo and Small Firm magazine board, Chairs the ABA's Technology Section, and serves on the long range planning committee.

Alan lives in Newton, Massachusetts. In his spare time, Alan serves as Executive Chef at his temple and travels along the east coast hoping to find the ultimate lobster roll.

You may find Alan in cyberspace
at www.summitlps.com, www.klevanlawfirm.com, www.linkedin.com/in/alanklevan
or www.twitter.com/AlanKlevan.

(857) 383 3250 | info@masslomap.org

C'mon, C'mon, C'mon, Let Me Show You What It's All About: Encryption ABC's, Easy as 1-2-3

The Massachusetts Data Protection statutes and rules compel encryption in certain scenarios; and, a modern interpretation of the Massachusetts Rules of Professional Conduct would suggest that encrypting data is the appropriate move in certain circumstances; but, beyond that, it's also a pretty good idea, as a general practice, to encrypt your clients' sensitive data. Fortunately, it is not all that difficult to encrypt your files. In fact, as suggested by the title of this post, it's as easy as 1-2-3.

When you're determining a process for encrypting your law firm data, you'll need to ask yourself three basic questions: (1) What are you encrypting? (a single document, a DVD, a device, etc.) (2) How often will you need to encrypt? (one document every so often, document packages, pretty much every email you send, etc.) (3) Which encryption platform will you use? (a PDF conversion tool, email encryption, whole disk encryption, etc.)

The most useful way to flesh out the practical responses to your encryption choices is to examine six scenarios, based on the above-relayed factors, and to determine a course of action respecting each. The more often you encrypt, the more automated a solution you

Search ...

Popular Recent

Automate Your Email with Simple Scheduling Tools
August 22, 2014

Guest Post: Sundown, You'd Better Take Care: Windows XP Extended Support to End Next Year
July 19, 2013

should seek. The following situations represent the most common encryption questions we receive at LOMAP:

If You're Encrypting One Document at a Time . . . You'll be able to encrypt your documents in as few as four simple steps: select security option, create password, reenter password, save document. Popular options for encrypting single files include Adobe Acrobat and Microsoft Word, through which you can lump additional document security on top, if you wish. If Acrobat and Word are too expensive for your tastes, there are a number of cheaper document creation tools out there, including: Open Office and Libre Office; on the PDF side, there are, among others: Nuance PDF Converter, CutePDF and PDF Forge.

If You're Encrypting Document Packages . . . You'll be able to use the same tools listed above; but, you should wait to apply your encryption to the document package until the entire package has been completed; though, certainly, you could, and likely should, encrypt individual inclusions, if you will maintain those separately.

If You're Encrypting Emails . . . If you're sending few emails with matter that should be encrypted, it's probably easier to just encrypt the document(s), or the document package(s), that you send. If you send email that needs to be encrypted on the regular, it probably makes more sense to use a tool built into your email system, that will allow you to encrypt on-the-fly, often via the use of a trigger word of some kind, to turn on (or turn off) the encryption protocol. There are a number of options in this line, likely not to cost you more than $10/month/email account. An alternative would be to use a completely encrypted email system, like Hushmail; but, that only works with other Hushmail users; and, modern business uses generally require a wider flexibility than that.

If You're Encrypting Devices . . . If you have a significant number of files that must be encrypted, and that are saved to your device, there are paid services (like Symantec's PGP) and freeware options (like TrueCrypt) that will allow you to apply encryption to your entire device. Some systems feature built-in encryption tools, such as Microsoft Office's BitLocker. Smartphones remain an outlier, as the platforms on which those devices run utilize different encryption protocols. Inquire with your provider as to what might work best respecting your particular phone.

If You're Encrypting Folders . . . If you don't want to encrypt your entire device, you could only encrypt those folders that contain

TECHSHOW + Tell: ABA Resurrects Popular Legal Technology Fair Every Spring
March 24, 2011

Post Topics

Apple (2)

Career Planning (66)

Client Relations (219)

Internet (297)

Law Firm Management (271)

Lawyer's Quality of Life (105)

Marketing (220)

MS Outlook (52)

Planning (227)

Productivity (188)

Risk Management (185)

Software (198)

Starting a law practice (210)

sensitive documentation, or place all of your sensitive documentation into one folder that you would then encrypt — though, that latter method could conceivably wreak havoc upon your file organization. Most of the tools available to encrypt devices would allow you to encrypt individual folders, as well.

If You're Storing to the Cloud . . . Most of the reputable cloud providers will provide something like 'government-level' encryption, in much the same way that carmakers used to offer the application of 'space age polymers' to their construction plans. With any data retention system, the application of a secure password is essential; but, that requirement takes on a further importance in relation to cloud-based systems, where access is almost completely predicated on password manipulation. Turn on two-factor authentication if it is offered by your provider. But, keep in mind that, if you rely on vendor encryption, the vendor will apply and know (in most cases) the encryption codes for your documents. If you want to overturn the tables, and take back that power, I've written on a number of methods for accomplishing that, representing various sorts of usage frequency, and automation levels; that's here.

It's inarguable that encryption technologies provide an additional lawyer of security for electronic business documents; but, objections to the use of encryption remain, mostly centered around the administrative burden created by the steps required for applying encryption protection. But, even though encryption does often require at least one extra step, the benefit of securing your client's data is worth it. In any event, the application of the correct tools, specific workflows and general process can reduce the time spent handling individual tasks.

This post originally appeared in the Massachusetts Bar Association's eJournal.

Share This Story, Choose Your Platform!

About the Author: Jared Correia

Technology (331)

Uncategorized (45)

Archives

2016
2015
2014
2013
2012
2011
2010
2009
2008

Jared is a regular contributor to local and national legal publications, including Attorney at Work, where his monthly column, 'Managing', appears. Jared is the author of the American Bar Association publication 'Twitter in One Hour for Lawyers'. He is the co-host of the 'Legal Toolkit' podcast on Legal Talk Network, and is featured on a quarterly podcast at Solo Practice University. Jared presented at ABA TECHSHOW 2013, on remote access and social media marketing.

Related Posts

Leave A Comment

Comment...

Name (required) | Email (required) | Website

Post Comment

ABOUT MASSLOMAP

Contact Info

How We Help

Staff Bios

JOIN US ON SOCIAL MEDIA

SEARCH OUR SITE

Search ...

RECENT BLOG POSTS

Moving to the Cloud: Recap from ABA TECHSHOW 2016 [Video]

Webconferencing Session: Recap from ABA TECHSHOW 2016 [Video]

Like a Boss: 2016 Marketing Conference is June 2-3

Do You Have a Contentious Relationship with Social Media? Revise Your Practice [Video]

Time-Saving Email Tips [Video]

SERVICES & RESOURCES

Consultations

eNewsletter

Legal Toolkit Podcasts

Lending Library

LoMac: Law Office Macs

Lunch Hour Legal Marketing

Start-Up Kit

Start-Up Meetings

White Papers | Articles

Fee Agreement Templates

(857) 383 3250 | info@masslomap.org

Secure Your Data: Part 2, Top Digital Data Security Tips

In my first post of this series on securing your data, I addressed the Massachusetts Data Privacy Laws, which provide standards for businesses that keep certain types of personal information. Part of the my discussion followed the insights of a panel of experts at a data security program held at the Social Law Library in May 2014. One panelist noted that solo and small firms tend to be easy targets for hackers because they typically don't have proper security safeguards in place.

While hackers certainly pose a security risk to your practice, so do lost mobile devices, emails mistakenly sent to the wrong party, unrecoverable data due to faulty or non-existent backups, and use of free wifi at your local Starbucks.

In this post, I've given you my top security tips so that you can start to implement better security safeguards in your practice today.

Drum roll . . .

#1 Strong Passwords. A strong password can drastically reduce the risk of unauthorized access to your firm's data. It's probably the single

Search ...

Popular Recent

Automate Your Email with Simple Scheduling Tools
August 22, 2014

Guest Post: Sundown, You'd Better Take Care: Windows XP Extended Support to End Next Year
July 19, 2013

most important step you can take now to protect your data (ok, finish reading this post first). And, if you need any convincing, try out a few of your current passwords on this site: https://howsecureismypassword.net.

What are the essential elements of a strong password?

- It is unique; used for one service only .
- It is long and uses multiple characters.
- It is not a common word or phrase (i.e. “password” or “monkey”); or, one of the passwords on this list of common passwords.

The best password is one that is randomly generated. A password manager can generate random passwords, as well as store and organize all your passwords, requiring only one master password to access your safe. Thus, you need not remember all your passwords nor do you need to keep them on sticky notes next to your computer (not exactly the safest option). Some of the top password manager programs include 1Password, LastPass, KeePass, and Dashlane. If it helps, I’ve forced every member of my immediate (and some extended) family onto one of these programs. That’s how much I value these services.

#2 Two-Factor Authentication. When you store data in the cloud, you lose some control over that data. Thus, you want to take extra steps to protect that data. Using two-factor authentication provides that extra protection. A basic example of two-factor authentication is the use of your ATM card to retrieve money from an ATM – first, you must swipe your card, then you must enter your PIN number. Two-factor authentication access requires something you know (i.e. PIN or password), in addition to something you have in your physical possession (i.e. your ATM card or cell phone), thus creating a stronger security barrier. Popular cloud-services, such as Google, Dropbox, and Evernote, all provide two-factor authentication for users.

#3 Backups. A scenario more likely to hit your law office than a breach is the loss of data due to some disaster or computer failure. You should have a redundant backup system as a failsafe. Ideally, electronic data should be backed up regularly through a combination of physical hard drives and cloud providers. Seagate, Western Digital, and Drobo are some of the top external hard drive brands. A few cloud back-up providers include Mozy, Carbonite, Crashplan, and Backblaze . Further, there are services that offer combo packages for physical plus cloud components, such as SpaceMonkey. Don’t

TECHSHOW + Tell: ABA Resurrects Popular Legal Technology Fair Every Spring
March 24, 2011

Post Topics

Apple (2)

Career Planning (66)

Client Relations (219)

Internet (297)

Law Firm Management (271)

Lawyer's Quality of Life (105)

Marketing (220)

MS Outlook (52)

Planning (227)

Productivity (188)

Risk Management (185)

Software (198)

Starting a law practice (210)

confuse cloud storage services like Dropbox and Google Drive with a dedicated backup cloud service. Using a cloud storage service as your backup is akin to having a real estate attorney draft a special needs trust. The purpose of Dropbox and Google Drive services is to sync files across systems, not to act as a backup system. If you delete a file on one device, it will be deleted on all other devices (including in the cloud). And, you shouldn't count on it remaining in your trash folder (ex. Dropbox permanently deletes files in the trash after 30 days). Once you've secured your backups, remember that they won't do you any good unless you test them by conducting periodic restores of non-essential data. In the event of an unexpected data loss, you should know precisely how to access and restore your data in just a few simple steps .

#4 Computer Updates. Your computer and mobile devices should be running the most up-to-date systems, software, and anti-virus programs. Developers constantly update software to both increase performance and to enhance security. Set your computer to automatically check for system and software updates, and then install those updates when prompted. This applies to your mobile devices as well. Pay attention to notifications on your device and install updates when they become available.

#5 Secured Networks. Ensure that your wireless network is set up securely. Change your router's default password and enable WPA or WPA2 encryption. Confirm that your router is running the most up-to-date firmware. For extra protection, configure your router to whitelist all your office computers and devices (using their MAC address – Media Access Control Address) so that even if a hacker was within range of your network it would need to break the encryption in addition to have the MAC address of one of your devices listed. When you are out of your office, don't use unsecure networks (read: free wifi). If you must, at the very least set up your computer's firewall protection (see this article for Mac and this one for PC). Alternatives to using free wifi include setting up your own private VPN connection with a service such as Cloak, using a portable router to establish a private connection, such as with the D-Link DIR-510L, buying a MiFi device from a mobile carrier, or activating your mobile phone's tethering plan.

#6 Encryption. Encryption is one of the best methods of protecting your electronic data. It takes the contents of a document and scrambles it such that it is rendered unreadable. What can and should be encrypted? According to the Massachusetts Data Privacy Laws (see M.G.L. c.93H and 93I, and implementing regulations, 201 CMR

Technology (331)

Uncategorized (45)

Archives

2016
2015
2014
2013
2012
2011
2010
2009
2008

17.00), certain personal information that travels wirelessly must be encrypted. That might include transmission of emails and documents, documents stored in the cloud, laptop hard drives, and USB storage devices. The simplest way to send encrypted data over email is to encrypt and attach a document to an email. Fortunately, it is not difficult to encrypt electronic information. You can encrypt documents with tools native to a Mac computer and with programs such as Adobe Acrobat for a PC. Both Mac and PC computers also have tools (FileVault and BitLocker, respectively) to enable full-disk encryption, that is, encryption of your entire hard drive and attached external drives such as a USB device or external backup drive. You can look forward to more on encryption later in this series.

#7 Vetting Providers. Due diligence is warranted before using a third-party service that may have access to confidential client information. This applies to both physical and electronic data, but my focus here is solely on electronic data, particularly that which is stored in the cloud. The Massachusetts Data Privacy Laws require that a business maintaining the statutorily protected personal information contract with third parties to provide assurances that their service complies with the statute. But, as we've written about previously, here and here, it may be difficult to do so, and thus in those situations the most practical course of action (albeit not strictly compliant with the statute) is to vet the provider and then document the steps you've taken. Furthermore, you have ethical obligations to protect your client's electronic information. Based on guidance by the Massachusetts Bar Association Ethic's Committee, see Opinion 12:03, storing confidential client data in the cloud does not violate the rules as long as the attorney "undertakes reasonable efforts to ensure that the provider's data privacy policies, practices and procedures are compatible with the Lawyer's professional obligations" (i.e. the vetting process). Here is what the Committee indicates are "reasonable efforts" (along with my own explanatory comments):

- examination of the provider's terms of use and data privacy policies and procedures; and ensuring that those policies *[You can typically find these terms conspicuously posted on the provider's website; if you cannot, that's your first tell-tale sign that you might not want to store your data with that provider.]* :
    - "prohibit unauthorized access to data" and allow access by the provider only to "convey[] or display [] the data to authorized users;" *[You don't want the vendor's employees or other third parties snooping through your data, nor do you want the*

company to quickly (without notice to you) hand over your data if served with a subpoena.]

    - provide sufficient access to the attorney user in the event of a service disruption *[You own your data, and the vendor's policies should confirm that. If the vendor goes out of business or you terminate the service, you should be able to get your data out.]*
- examination of the provider's reputation and history, including encryption, password protection, backups, and history of breaches; and *[Rather than starting from scratch, find a service that other attorneys and/or practice advisors recommend. Then engage in your own due diligence.]*
- conducting a periodic review of the provider's policies to ensure continued compliance. *[Most vendors draft their policies with a provision subjecting it to infinite change. Review your provider's policies at least on an annual basis and whenever you are notified by your provider that their policies have changed.]*

#8 Policy and Training. Your firm should have a policy that sets out how your it safeguards confidential information, which might include necessary training for staff on how to manage firm-wide network security as well as training for individual staff computer use (i.e. passwords, computer updates, logoff requirements), encryption procedures, protocols for protecting mobile devices that access firm information, handling of third-party access to data (i.e. cloud storage providers), and remediation procedures in the event of a data breach. Moreover, this type of policy (a "Written Information Security Program") is indeed required by the Massachusetts Data Privacy Laws for businesses that keep certain personal information as implicated by the statute.

—

While it is impossible to ensure that your data (whether physical or electronic) is 100% safe, taking the foregoing steps to protect your digital data will help you significantly mitigate security risks. Later in this series, I will expand upon some of these topics as well as discuss specific protections for a variety of computer systems and devices. I know that you will be eagerly awaiting . . .

—

APPropos

TextExpander Touch: Create custom shortcuts for frequently used words and phrases. Makes drafting on a small device much more efficient.

Songza: A Pandora replica, but with less advertisements. Curating playlists based on mood, activity, and day/time.

Drafts: An integrated note-taking app. Draft a note and export to a variety of services or create your own custom actions.

Share This Story, Choose Your Platform!

About the Author: Heidi Alexander

Heidi S. Alexander, Esq. is a Law Practice Management Advisor at the Massachusetts Law Office Management Assistance Program (MassLOMAP), where she advises lawyers on practice management matters and provides guidance in implementing new law office technologies. She frequently makes presentations to the legal community and contributes to publications on law practice management and technology, including ABA Law Technology Today, Attorney at Work, and Technolawyer. She is in the process of completing a book on Evernote as a Law Practice Tool; to be published by the ABA's Law Practice Division.

Related Posts

Leave A Comment

Comment...

Name (required) | Email (required) | Website

Post Comment

ABOUT MASSLOMAP

Contact Info

How We Help

Staff Bios

JOIN US ON SOCIAL MEDIA

SEARCH OUR SITE

Search ...

RECENT BLOG POSTS

Moving to the Cloud: Recap from ABA TECHSHOW 2016 [Video]

Webconferencing Session: Recap from ABA TECHSHOW 2016 [Video]

Like a Boss: 2016 Marketing Conference is June 2-3

Do You Have a Contentious Relationship with Social Media? Revise Your Practice [Video]

Time-Saving Email Tips [Video]

SERVICES & RESOURCES

Consultations

eNewsletter

Legal Toolkit Podcasts

Lending Library

LoMac: Law Office Macs

Lunch Hour Legal Marketing

Start-Up Kit

Start-Up Meetings

White Papers | Articles

Fee Agreement Templates

(857) 383 3250 | info@masslomap.org

Secure Your Data: Part 3, Encryption Basics

This series began with a post on the Massachusetts Data Privacy Laws, which provide standards for businesses that keep certain types of personal information. Following up that statutory and regulatory update, I provided you with my top digital security tips, including tip #6: Encryption.

In this third post, you'll learn about encryption. I promise no techie language, only what you need to know.

What is encryption?

"[T]he conversion of data into a form called a ciphertext that cannot be easily understood by unauthorized people." I pulled this quote from David G. Ries, Sharon D. Nelson, and John W. Simek, *Encryption Made Simple for Lawyers* (American Bar Association 2015). For everything you need to know about the history of encryption, "ciphertext", as well as "how to", I suggest checking out this book. It is now available in our lending library.

What you should know about encryption is that it is essentially the best way to protect your digital data. It can be used to protect electronic data that resides on your hard drive, external drives, USBs,

Search ...

Popular Recent

Automate Your Email with Simple Scheduling Tools
August 22, 2014

Guest Post: Sundown, You'd Better Take Care: Windows XP Extended Support to End Next Year
July 19, 2013

servers, cloud storage, smartphones, and tablets, as well as data that is transmitted wirelessly (i.e. e-mail communications).

Why should you use it?

Well, you've got an obligation to protect your client's data pursuant to Rule 1.6. New rules, previously approved by the SJC and soon to be promulgated on July 1, 2015 (more information to come on this blog), add the following language to the Rule:

"(c) 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."

As the authors of *Encryption Made Simple for Lawyers* point out,

[i]nadvertent disclosure includes threat like leaving a briefcase, laptop, or smartphone in a taxi or restaurant, sending a confidential e-mail to the wrong recipient, producing privileged documents or data, or exposing confidential metadata. Unauthorized access includes threats like hackers, criminals, malware, and insider threats.

In terms of ethical obligations, there is no requirement that attorneys encrypt client data (see Massachusetts Bar Association Ethics Committee Opinion 00-01). However, under the Massachusetts Data Privacy Laws, certain types of data must be encrypted. That has been covered previously at our blog, stemming back from this post.

When should you use it?

As noted in our previous blog posts regarding the Massachusetts Data Privacy Laws, the law requires encryption of "all transmitted records and files containing personal information that will travel across public networks, []encryption of all data containing personal information to be transmitted wirelessly[, and] . . . [e]ncryption of all personal information stored on laptops or other portable devices." (See 201 CMR 17.00).

In basic terms, what that means for you, is that if you collect "person information" as defined by the statute and store it on a laptop or portable hard drive and/or send it via e-mail, it must be encrypted.

If you are not holding onto personal information, do you still need to encrypt? I'll give you my lawyerly answer: It depends. It's a cost-benefit / risk analysis. How sensitive is the information? What type of

TECHSHOW + Tell: ABA Resurrects Popular Legal Technology Fair Every Spring
March 24, 2011

Post Topics

Apple (2)

Career Planning (66)

Client Relations (219)

Internet (297)

Law Firm Management (271)

Lawyer's Quality of Life (105)

Marketing (220)

MS Outlook (52)

Planning (227)

Productivity (188)

Risk Management (185)

Software (198)

Starting a law practice (210)

security safeguards have you implemented? Have you vetted third-party providers? Are you using free or premium/enterprise level service providers to store electronic data? How much will it cost you in time and money to encrypt your data?

How to use it?

I know, you are all saying, get on with it Heidi. What we really want to know is how to encrypt. Ok, ok, here it is.

Files, Folders, Hard Drives, and External Drives

1) Mac OS X Encryption. Mac's native features make it easy to encrypt documents, folders, and hard drives.

For encryption of:

- Mac Hard Drive: Use Apple's native full disk encryption tool, FileVault. Available in all OS X versions Lion and later.
- External Drives: Right-click on the drive and set encryption.
- Folders: Use Apple's native Disk Image feature found in Disk Utility.
- Files: For PDFs, use Apple's Save as PDF tool. For Word, Excel, and Power Point documents, use Microsoft Office's encryption feature.

In just ten minutes, this video walks you through, step-by-step, how to encrypt using your Mac. Here is a link to the same instructions with screen shots: http://www.lawtechnologytoday.org/2013/12/encryption-made-easy-a-primer-for-mac-users/.

2) PC Windows Encryption.

For encryption of:

- Windows Hard Drive: Use BitLocker, Window's native full disk encryption tool. Available in Windows Vista Enterprise and Ultimate and Windows 7 Enterprise and Ultimate, and Windows 8 and 8.1 Professional and Enterprise.
- External Drives: Use BitLocker to Go, available as part of BitLocker.
- Folders: Use Window's Encrypting File System (EFS).
- Files: There is no native Windows product to protect PDFs. Alternatives include Adobe Acrobat Professional or Standard,

Technology (331)

Uncategorized (45)

Archives

2016
2015
2014
2013
2012
2011
2010
2009
2008

Nuance Power PDF, PDFCreator, or WinZip. For Word, Excel, and Power Point documents, use Microsoft Office's encryption feature.

3) External Drives. You can also purchase USB drives with built-in encryption. For example, IronKey, Kingston, and SanDisk all make devices.

Tips: When you encrypt files, folders, and external drives, you'll need to set an encryption key. It's the passcode you'll enter to decrypt the data for use. Use a strong passcode or even a phrase with a minimum of 14 characters, symbols, lower and upper case letters, and numbers. (See *Encryption Made Simple*, pp. 64-65).

Next up in my data security series: email, mobile, and cloud-storage encryption. Stay tuned . .

—

APPropos – "Mobile Apps for Your Practice"
Hopper: Airline price prediction tool. Discover when to fly and buy tickets.Pomodoro Timer: Based off the Pomodoro time management technique, this app helps you schedule your work in discrete intervals to eliminate burnout and manage distractions.

Chrometa: Automatic call tracking and manual time entry. Exports to billing and law practice management programs.

About the Author: Heidi Alexander

Heidi S. Alexander, Esq. is a Law Practice Management Advisor at the Massachusetts Law Office Management Assistance Program (MassLOMAP), where she advises lawyers on practice management matters and provides guidance in implementing new law office technologies. She frequently makes presentations to the legal community and contributes to publications on law practice management and technology, including ABA Law Technology Today, Attorney at Work, and Technolawyer. She is in the process of

completing a book on Evernote as a Law Practice Tool; to be published by the ABA's Law Practice Division.

Related Posts

Leave A Comment

Comment...

Name (required) | Email (required) | Website

Post Comment

ABOUT MASSLOMAP

Contact Info

How We Help

Staff Bios

JOIN US ON SOCIAL MEDIA

SEARCH OUR SITE

Search ...

RECENT BLOG POSTS

Moving to the Cloud: Recap from ABA TECHSHOW 2016 [Video]

Webconferencing Session: Recap from ABA TECHSHOW 2016 [Video]

Like a Boss: 2016 Marketing Conference is June 2-3

Do You Have a Contentious Relationship with Social Media? Revise Your Practice [Video]

Time-Saving Email Tips [Video]

SERVICES & RESOURCES

Consultations

eNewsletter

Legal Toolkit Podcasts

Lending Library

LoMac: Law Office Macs

Lunch Hour Legal Marketing

Start-Up Kit

Start-Up Meetings

White Papers | Articles

Fee Agreement Templates

LAW SITES

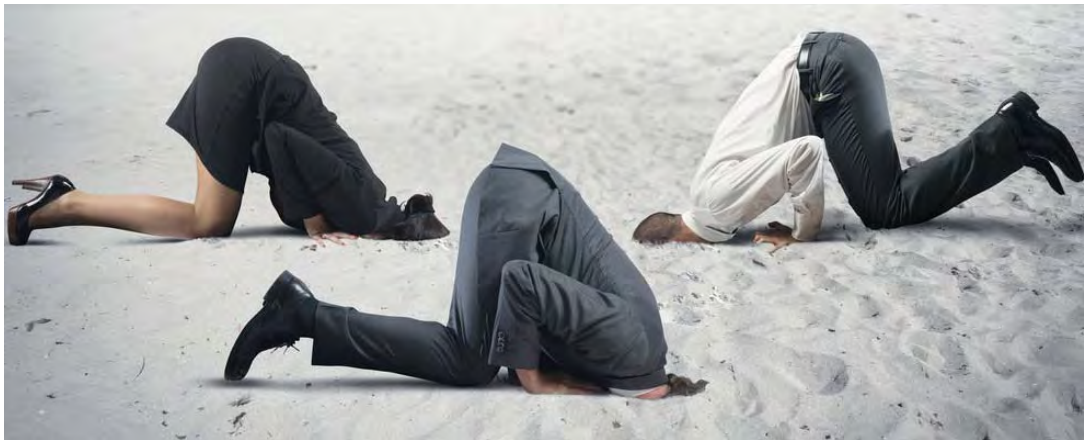
BY ROBERT AMBROGI

TRACKING NEW AND INTRIGUING WEBSITES AND PRODUCTS FOR THE LEGAL PROFESSION.

MARCH 16, 2015

~~13~~ ~~15~~ ~~17~~ ~~18~~ 20 States Have Adopted Ethical Duty of Technology Competence

by Robert Ambrogi



*[Update: As of Dec. 23, 2015, it is 20 states, with the **addition of Iowa and Utah**.]*

*[Update: As of Dec. 17, 2015, it is 18 states, with the **addition of Virginia**.]*

*[Update: As of Nov. 11, 2015, it is 17 states, with the **addition of two more**.]*

*[Update: As of Oct. 15, 2015, it is 15 states, with the **adoption of the rule** in Illinois.]*

*[Update: It is now 14 states. See my **3/27/15 post** on the rule's adoption in Massachusetts.]*

In 2012, something happened that **I called** a sea change in the legal profession: The American Bar Association formally approved a change to the **Model Rules of Professional Conduct** to make clear that lawyers have a duty to be competent not only in the law and its practice, but also in technology.

More specifically, the ABA's House of Delegates voted to amend Comment 8 to Model Rule 1.1, which pertains to competence, to read as follows:

> Maintaining Competence
>
> 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. (Emphasis added.)

Of course, the Model Rules are just that — a model. They provide guidance to the states in formulating their own rules of professional conduct. But each state is free to adopt, reject, ignore or modify the Model Rules. For the duty of technology competence to apply to the lawyers in any given state, that state's high court (or rule-setting body) would first have to adopt it.

So, roughly 30 months after the ABA approved this amendment, how many states have adopted the duty of technology competence? By my count, ~~13~~ 15 states have so far formally adopted the revised comment to Rule 1.1. They are:

- Arizona, **effective Jan. 1, 2015**.
- Arkansas, **approved June 26, 2014**, effective immediately.
- Connecticut, **approved June 14, 2013**, effective Jan. 1, 2014.
- Delaware, **approved Jan. 15, 2013**, effective March 1, 2013.
- Idaho, **approved March 17, 2014**, effective July 1, 2014.
- Illinois, **approved Oct. 15, 2015**, effective Jan. 1, 2016.
- Iowa, **approved Oct. 15, 2015**, effective Oct. 15, 2015.
- Kansas, **approved Jan. 29, 2014**, effective March 1, 2014.
- Massachusetts, **approved March 27, 2015**, effective July 1, 2015.

- Minnesota, **approved Feb. 24, 2015**.
- New Hampshire, **approved Nov. 10, 2015**, effective Jan. 1, 2016.
- New Mexico, **approved Nov. 1, 2013** (**text of approved rules**), effective Dec. 31, 2013.
- New York, **adopted on March 28, 2015**, by the New York State Bar Association.
- North Carolina, **approved July 25, 2014**. Note that the phrase adopted by N.C. varies slightly from the Model Rule: "… including the benefits and risks associated with the technology relevant to the lawyer's practice."
- Ohio, **approved Feb. 14, 2015**, effective April 1, 2015.
- Pennsylvania, **approved Oct. 22, 2013** (**text of approved rules**), effective 30 days later.
- Utah, **adopted March 3, 2015**, effective May 1, 2015.
- Virginia, **approved Dec. 17, 2015**, effective March 1, 2016.
- West Virginia, **approved Sept. 29, 2014**, effective Jan. 1, 2015.
- Wyoming, **approved Aug. 5, 2014**, effective Oct. 6, 2014.

On Feb. 28, 2015, the Virginia State Bar Council **voted to adopt** the Rule 1.1 change. However, the change does not take effect unless and until it is approved by the Virginia Supreme Court.

~~In Massachusetts, where I am located, the Supreme Judicial Court has **issued a notice** stating that it will adopt a package of proposed rule changes that includes Comment 8. However, the SJC said that it will not issue a formal order adopting the rules or set an effective date until it announces its decision on other proposed changes for which it has scheduled oral arguments. More information on the proposed changes and their status **can be found here**.~~

Some other states, while not having formally adopted the change to their rules of professional conduct, have nonetheless acknowledged a duty of lawyers to be competent in technology. For example, the New Hampshire Bar Association, in **Advisory Opinion #2012-13/4** concerning cloud computing, **said**:

> Competent lawyers must have a basic understanding of the technologies they use. Furthermore, as technology, the regulatory framework, and privacy laws keep changing, lawyers should keep abreast of these changes.

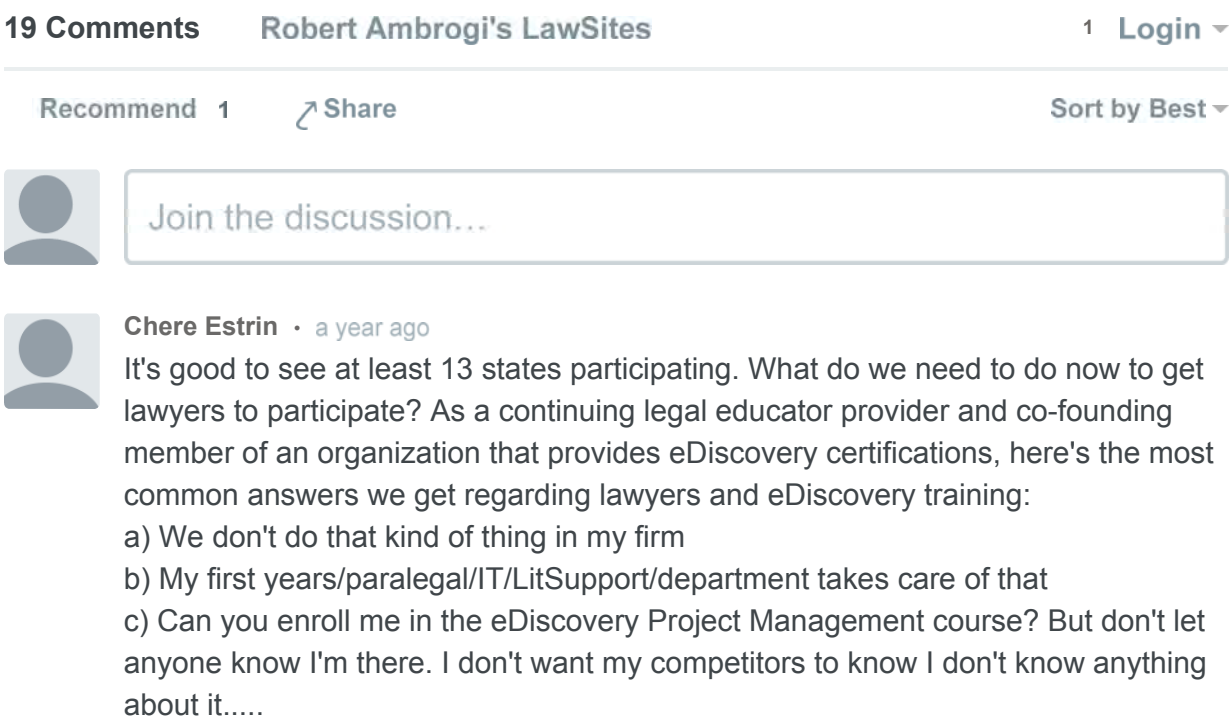
And in California, a proposed ethics opinion of the State Bar of California (**Proposed Formal Opinion Interim No. 11-0004**) would require attorneys who represent clients in litigation either to be competent in e-discovery or associate with others who are competent. The opinion expressly cites the ABA's Comment 8 and states:

> Maintaining learning and skill consistent with an attorney's duty of competence includes "keeping abreast of changes in the law and its practice, including the benefits and risks associated with technology."

If you know of other states I have missed, please let me know.

What does all this mean to you? It is simple. You cannot assess the benefits and risks associated with various kinds of technology if you know nothing about the technology. Even if your state has yet to adopt this change, it is only a matter of time before it does. Don't be a Luddite who fears or resists technology. Neither do you have to become a geek. Make an effort to understand the basics of the technology you use. Get on social media, if you're not already. Ask questions. Learn. When it comes to technology, there is no more burying your head in the sand.

Posted in: General
Tagged: legal ethics



« Previous | **Home** | **Next »**