T H E

T E N N E S S E E

L A W

I N S T I T U T E

PRESENTS

THE

FORTY-EIGHTH ANNUAL

REVIEW SEMINAR

SPEAKERS

Sarah Y. Sheppeard, a shareholder of Lewis, Thomason, King, Krieg and Waldrop PC, is the 2019-2020 President of the Tennessee Bar Association. She is a Past-President of the Knoxville Bar Association and a Rule 31 Mediator listed by the Tennessee Supreme Court. She has a diverse civil practice, with a focus on domestic cases. She was a member of the Tennessee Law Review, and is a Fellow of the American, Tennessee, and Knoxville Bar Foundations. She is a recipient of the TBA's President's Award, the KBA's Governor's award, and the Don Paine Lawyer Legacy Award.

Lucian T. Pera of Memphis is a member of Adams and Reese LLP. His practice includes commercial litigation and media law, as well as counseling and representing lawyers and law firms on questions of legal ethics. He chaired the TBA committee that drafted Tennessee current ethics rules and served on the committee that substantially revised the ABA Model Rules of Professional Conduct in 2002. He has served as Treasurer of the ABA and as President of the TBA.

Wade V. Davies is the Managing Partner at Ritchie, Dillard, Davies & Johnson, P.C. in Knoxville. His practice is primarily criminal defense. He is a Fellow of the American College of Trial Lawyers and serves on the Federal Criminal Procedure Committee. He has served two terms as a member of the Board of Professional Responsibility. He is a past President of the Knoxville Bar Association and is serving his third term on the Board of Directors of the Tennessee Association of Criminal Defense Lawyers.

THE ONES WE MISS

Donald F. Paine started the Tennessee Law Institute in 1972 and was our mentor, chief researcher, beloved leader and great friend to the bench and bar alike, even as he fought cancer for over 34 years. His death in November of 2013 left a huge void in our hearts, but his research techniques and teaching style have continued, making TLI the quality program it has been for over four decades.

John A. Walker, Jr. joined TLI in its second year and was an integral part of the commercial law aspects of our program until his retirement for health reasons in 2011. John passed away in September 2016.

John M. Smartt, although never a lecturer, was TLI's administrator for fifteen years. He was our ringmaster, cheerleader, and was even known to talk a legal secretary into pulling an attorney out of a deposition for an important message: "Joe, I see you haven't signed up for the seminar yet, and I sure wouldn't want you to miss it!" Ironically, John's death was within a week of Don's.

We miss them all, as we continue to carry on the mission of TLI.

TLI Ethics 2019
Lawyer Cybersecurity:
Very Specific Things to Do Today to Be Safer Tomorrow

Lawyer cybersecurity is scary.

Does it have to be?

"Personal computers are just too hard to use, and it isn't your fault."
– Walter S. Mossberg, The Wall Street Journal, October 17, 1991

Today's approach: Lawyer cybersecurity is scary; it isn't our fault; it doesn't have to be; and we can each be safer tomorrow than today.

How? By learning a few things today, and by committing to continue learning a little bit about tech, a little bit at a time, continuously.

Today's topic

A few minutes on our ethical obligations to protect client confidential information. (ABA Ops. 477, 482, and 483)

A smorgasbord of things you can do today to protect yourself from viruses, hackers, phishing, ransomware, and other threats – as well as from everyday dangers to your tech health, like losing your phone or laptop.

The goal:

- ***Not*** to be perfectly safe.
- Not to ***merely*** meet your ethics obligations
- But to be safer tomorrow from all those dangers than you are today.
- And to continue to improve your security gradually over time.

Resources

Resources as to this program will be posted online.

But remember to talk with your new best friend, your Tech Guru.

And consider the ABA's ***2019 Solo and Small Firm Legal Technology Guide***, by Sharon D. Nelson, John W. Simek, and Michael Maschke ($89.95; $67.45 for ABA members), available at: https://www.americanbar.org/products/inv/book/355399637/.

Oh, and clients are watching.

Client outside counsel guidelines

"7 Questions to Ask Your Lawyer About Data Security"

1. Who has access to my information inside and outside your firm?
2. Why does [a third party or a role in the law firm you don't understand] have access to my information?
3. When are you encrypting my information?
4. How are you ensuring the physical security of my data?
5. What does your firm do to avoid social engineering risks?
6. How are you ensuring that the vendors you use are protecting my information?
7. If you use local counsel, how are you ensuring that they will protect my information?

– Lisa Morgan, "7 Questions to Ask Your Lawyer About Data Security," *Inc*. (Feb. 9, 2017), available at: https://www.inc.com/lisa-morgan/is-your-lawyer-safeguarding-your-information-7-questions-to-ask.html.

1. Know your ethical obligations.

Sources of obligations

- Ethics rules
- Standard of care
- Fiduciary duty
- Contract (*e.g.*, client's outside counsel guidelines)
- Other law (*e.g.*, HIPAA, data breach notification laws)

Primary ethical touchstones: Rules 1.1 and 1.6(c)

Rule 1.1 (Competence), Comment [8]:

> 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 1.6 (Confidentiality):

> (d) 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.

Comment [18]:

> The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made ***reasonable efforts*** to prevent the access or disclosure.

ABA Op. 477R, Securing Communication of Protected Client Information (May 19, 2017) quotes Rule 1.6 Comment [18] on factors to guide lawyers on "reasonable efforts:"

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and
- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (*e.g.*, by making a device or important piece of software excessively difficult to use).

ABA Op. 483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack (Oct. 17, 2018).

What the ethics rules require concerning data breaches and cybersecurity incidents:

- Duty to monitor for a data breach
- Duty to determine what happened
- Duty to respond to data breach and restore systems

ABA Op. 483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack (Oct. 17, 2018).

What the ethics rules require concerning data breaches and cybersecurity incidents:

- Duty to notify clients (and maybe others)… Question: Duty to notify former client?
- Notification duty under data breach laws.

Remember, we may have obligations ***other than*** ethics obligations (*e.g.*, fiduciary duty, HIPAA, client outside counsel guidelines).

ABA Op. 482, Ethical Obligations Related to Disasters (Sept. 19, 2018).

Obligations in the event of disaster (*e.g.*, hurricanes, floods, tornadoes, fires, earthquakes).

Ethical obligation to have a disaster recovery plan.

2. Become *really* good friends with your Tech Guru.

Check your phone.

Every lawyer needs a legal technology expert.

- To answer routine tech questions (*e.g.*, Why is my email not working?)
- To advise on less routine questions (*e.g.*, Can I safely use the file-sharing service my client wants to use?)
- To help in an emergency (*e.g.*, My phone was just stolen – what do I do?)

3. Patch and update your software promptly and consistently.

Software that has not been kept up-to-date accounts for a very large proportion of all hacks.

- Verizon Data Breach Report 2016: Of all detected exploits, most came from vulnerabilities dating to *2007*. Next was 2011.
- Vulnerabilities dating to 2003 still account for a large portion of hacks of Microsoft software.

MORAL: Patch and update software promptly and consistently.

Set devices and software to automatically update software.

Do not use out-of-date software or devices.

4. Tweak your software toward improved security.

Many devices and apps have features that can enhance security. Consult your Tech Guru!

Examples:

DropBox – allows 2FA; use add-ins to encrypt files and folders

Microsoft Office 365 – "Secure Score" app within service

- Evaluates security of selected options and points to recommendations
- Default settings – 79 of 273

Mobile devices (cell phones, pads, laptops)

- Password
- Encryption
- Find My iPhone
- Backup
- Remote wiping (through carrier or mobile device management (MDM))
- Absolute's LoJack for Laptops or Prey (P-R-E-Y).
- Add a VPN (more below…)

5. Learn where your data lives.

To protect your data, you need to know where it is.

6. Encrypt your data.

"Encryption" = scrambling or enciphering data so it can be read only by someone with the means to return it to its original state.

Two types of encryption:

- Data "at rest" – on a hard drive, flash drive or other storage medium
- Data "in transit" – in process of being sent by email, text or other method

Encrypting data "at rest" can help protect against hacking of a server hard drive or retrieval of data on lost or stolen devices.

Encrypting data in transit can help protect against unauthorized access to email, texts and similar messages.

In most states (*not* Tennessee), theft/loss of an *encrypted* hard drive ≠ reportable breach.

7. Backup your data.

Critical to any recovery plan

Good backups:

- Complete
- Regular
- Routine (not dependent on humans)
- Redundant
- Encrypted

Ransomware

The value of the cloud

Have your tech guru restore your backup data occasionally

8. Use good passwords.

Assess the strength of your passwords.

Consider a password manager.

Examples: 1Password, LastPass, KeePass, and Dashlane.

Change your good passwords … occasionally.

Talk with your Tech Guru about whether your systems can be set to use fewer overall passwords.

9. Use a secure file-sharing solution.

Email is ***not*** an effective or efficient tool for sharing large files.

But excellent file-sharing services are out there.

Examples: DropBox, Box, Citrix ShareFile …

But also: Apple iCloud, Microsoft OneDrive….

Work with your Tech Guru to:

1. Evaluate security of service up front.
2. Tweak settings to insure secure installation.

10. Use a metadata scrubber.

Almost any document shared with others (*e.g.*, Word, PDF, and Excel documents, photos) includes metadata (*i.e.*, data about data).

Metadata can include dates of creation or modification, user/editor identity, substance of modifications, tracked changes, location where photo was taken.

Metadata may be confidential.

Lawyer's obligation to protect confidential information.

Example: PayneGroup's Metadata Assistant

11. Use other people's WiFi safely … or not at all.

Opinion is divided…

- ***Never ever*** use public WiFi. Always use your own WiFi

…or…

- ***Exercise great care*** in using public WiFi. ***Always*** use a VPN.

Consult your Tech Guru.

If you fall in the first, hyper-paranoid camp…

- Use a WiFi hotspot on your cell phone.
- Buy a separate WiFi hotspot service (and use a VPN).

If you fall in the second, plain-old-paranoid camp…

- Don't be stupid. Check the WiFi you're using.
- Always use a VPN. Check with your Tech Guru about what VPN to use and how.

12. Get a regular security assessment.

A thorough, periodic security review of the office or firm's technology.

- Know, limit, and monitor who has access (including remote access) to your systems.
- Assess physical security of your system.
- May include penetration testing.

Some clients are now requiring them (*e.g.*, banks and financial, health care, collections).

13. Vet your vendors, including your cloud vendors.

Numerous large data breaches and cybersecurity attacks have come through vendors (*e.g.*, Target).

Engage in thoughtful due diligence – with your Tech Guru's help – on all technology, online, and security vendors and vendors who have ***any*** access to your systems.

Some factors to consider:

- Terms of service
- Reputation for security and cybersecurity
- Experience in dealing with law firms and lawyers
- Level and scope of access to your confidential information

14. Start preparing and implementing a disaster recovery plan.

ABA Op. 482, Ethical Obligations Related to Disasters (Sept. 19, 2018).

Consider the possibilities (*e.g.*, tornado, wildfire, flood, earthquake, power outage).

Plan might include:

- Emergency contact with personnel
- Electrical power (*e.g.*, UPS, generator)
- Internet connection
- Alternative email
- Access to all contacts
- Data backup
- Redundant equipment

15. Start preparing and implementing an incident response plan.

Begin making and implementing a plan.

Consider lining up a security expert now.

Talk with your broker about cyber-incident insurance (*before* your next renewal).

16. Train to spot phishing and other email attacks.

Phishing: fraudulent practice of sending emails purporting to be from known senders or reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

And there are other threats from email…

- Legit-seeming requests for money (*e.g.,* fake instructions from the boss; gift cards).
- Malware in attachments or links.

Remedies

- Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA)
- Training

Training Programs:

- Videos
- Realistic email tests

17. Check client requirements.

Increasing tempo and intensity of client demands concerns regarding cybersecurity.

- Often contained in outside counsel guidelines.
- Common to certain industries (*e.g.*, financial sector, health care, collections).
- Some use separate cyber requirements or questionnaires.

Find and review them.

Issues:

- Lawyers oblivious to requirements
- Law firm ignorant of lawyer agreement to requirements
- Onerous requirements beyond capacity of law firm
- Requirements that go beyond ethical requirements
- Requirements that violate ethical obligations

Remedies:

- Promptly identify and centrally review requirements.
- Comply or push back on demands.

Consider your Tech Guru a resource on whether you can meet demands.

18. Improve your communication with clients about confidentiality.

Suppose a new client may communicate with her lawyer…

… about her employment claim on work email or work computer.

… about his divorce on home computer to which spouse has access.

… about her divorce on family-plan cellphone where her spouse has access to messages or location.

Then the lawyer has a duty to advise the client about how to maintain client confidentiality.

- ABA Op. 11-459, Duty to Protect the Confidentiality of E-Mail Communications with One's Client (Aug. 4, 2011).
- The need for better lawyer-client conversation.

Consider…

- Reviewing client intake process.
- Prohibiting some forms of communication (*e.g.*, Facebook, texting).
- Including better discussion of issues in engagement letter.
- Targeted discussions in some cases (*e.g.*, divorce, employment law, cases involving medical information).
- More thoughtful retention of records (*e.g.*, engagement letter provisions on retention period, paper-v.-electronic).

19. Evaluate your firm's policies, written and otherwise.

Consider whether your firm has, or should have written policies on:

- Client confidentiality
- Password security
- Physical security of offices
- Remote access to firm systems
- Providing client information to others

Consider whether your firm has, or should have written policies on:

- Personal use of firm systems.
- Use of personal devices or systems (*e.g.*, email or texts) for client work.
- Terminating access of former employees to firm systems.

Questions:

- Do you have a policy?
- Are you following it?
- Is it the right policy?

20. Commit to routinely and continuously improving your tech competence.

Tech competence is an ethical requirement (Rule 1.1), and tech security is a part of tech competence.

- Pick one or two topics we've talked about today and learn to be safer in the next month.

But ***also***… ***RESOLVE*** to routinely and continuously improve your personal, basic tech competence, including your security competence.

Learn *from* and *with* others in your office – lawyers *and* others.

Examples:

- How to e-file a document.
- How to *securely* redact a PDF.
- How to electronically "sign" or edit or comment on a PDF.
- How to use Track Changes in Word.
- How to scan and OCR a paper document into a PDF.
- How to scan and OCR a paper document into a PDF *using your phone*.

RULE 1.1: Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.

Comment

….

Maintaining Competence

[8] 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 1.6: Confidentiality of Information

....

(d) 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.

Comment

....

Acting Competently to Preserve Confidentiality

[18] Paragraph (d) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. *See* RPCs 1.1, 5.1, and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (d) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, *see* RPC 5.3, Comments [3]-[4].

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

....