



PROGRAM MATERIALS

Program #30152

June 1, 2020

How Technology Can Ethically Unite the Legal Community During Emergencies

**Copyright ©2020 by Daniel J. Siegel, Esq. - Law Offices
of Daniel J. Siegel, LLC.
All Rights Reserved.
Licensed to Celesq®, Inc.**

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969



How Technology Can Ethically Unite the Legal Community During Emergencies

Presented by:

Daniel J. Siegel, Esquire

About Daniel J. Siegel, Esquire


- Chair, Pennsylvania Bar Association Committee On Legal Ethics & Professional Responsibility
- Providing Ethical and Techno-Ethical Guidance To Attorneys & Law Firms
- Email dan@danieljsiegel.com



LAW OFFICES OF
DANIEL J. SIEGEL
DANIELJSIEGEL.COM 610-446-3457 LLC

Today's Goal

Providing practical advise about how to use technologically ethically to achieve your goals, regardless whether working remotely or at the office

A large orange circle on the left side of the slide, partially cut off by the edge.

A Dose of Reality

- Legal technology is a great equalizer



A Dose of Reality

- Regardless whether you are a solo, practice in-house, or are in a large firm, technology matters

A Dose of Reality

- Tech savvy lawyers understand how to leverage their technology skills to gain advantages not easily transferable to paper.

A Dose of Reality

- During emergencies, the difference between the tech-users and tech-Luddites is more distinct.



Today's Program

- This program will highlight why lawyers need to use technology, and how to do so ethically while assuring the best results.

Today's Program

- This program will highlight the underlying ethical considerations necessary to use technology during emergencies.



Today's Program

- This program will provide practical guidance applicable not only during challenging times, but also when attorneys are handling matters in more traditional times.

Today's Program

- This program will address the need for attorneys to become technologically competent in order to better serve clients, or their organizations.




**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...

A large orange circle is positioned on the left side of the slide, partially overlapping the text area.

What is
competence?

- For lawyers, is competence the ability to handle a legal matter properly?
- 
- A yellow dashed line is located in the bottom right corner of the slide, consisting of several short, curved segments.

What is
competence?

- Does a lawyer's technological competence matter?



What is competence?

Does a lawyer's technological competence matter?

- Yes it does.
- It impacts billing.
- It impacts his or her ability to understand the ever-changing legal landscape, which includes the requirement to know the impact of technology on clients, on practice, and on the entire legal world.

What is competence?

Does a lawyer's technological competence matter?

- Would you go to a doctor who didn't stay abreast of modern medical technology and its impact on patient care?

What is competence?

- Does a lawyer's technological competence matter?
- Is it a reflection of his or her true desire to be a more well-rounded lawyer?
- Is it a reflection of his or her refusal to change?
- What are the implications of the answers to those questions?

What is competence?

- Does a lawyer's technological competence matter?
- Is it a reflection of how he or she will deal with sudden changes and emergencies?

What is competence?

- There is basic technological competence, and there is basic legal technological competence.
- Both are important.
- Both are very important.

What is
competence?

- And what happens during an emergency situation?



What is
competence?

- And what happens during an emergency situation?





**STUFF
HAPPENS**

Now what?



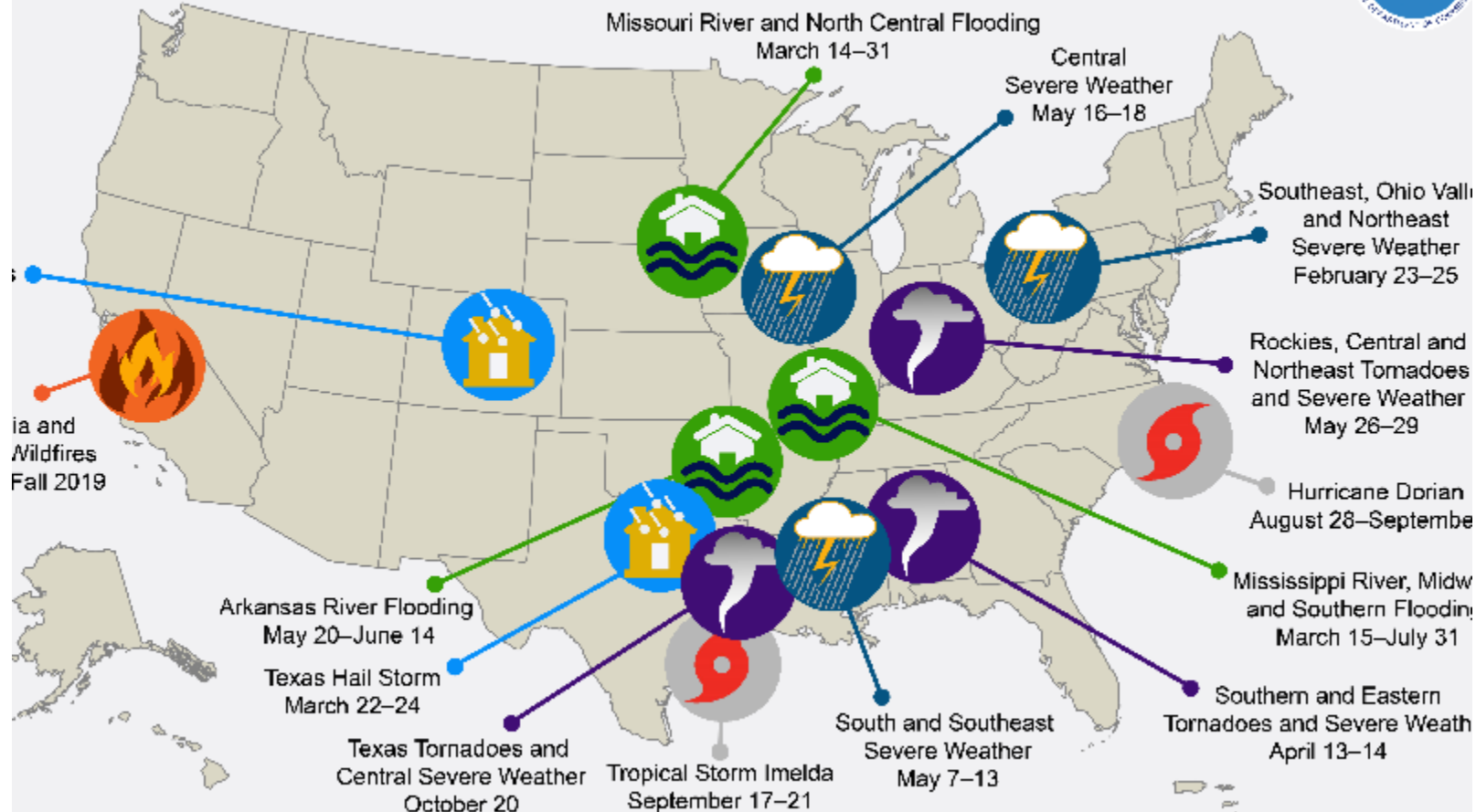
**STUFF
HAPPENS**

Like a
pandemic?

**Henny
Penny
Was
Right**



U.S. 2019 Billion-Dollar Weather and Climate Disasters



This map denotes the approximate location for each of the 14 separate billion-dollar weather and climate disasters that impacted the United States during 2019

We expect disasters



WE DIDN'T START THE VIRUS

Most businesses were not prepared

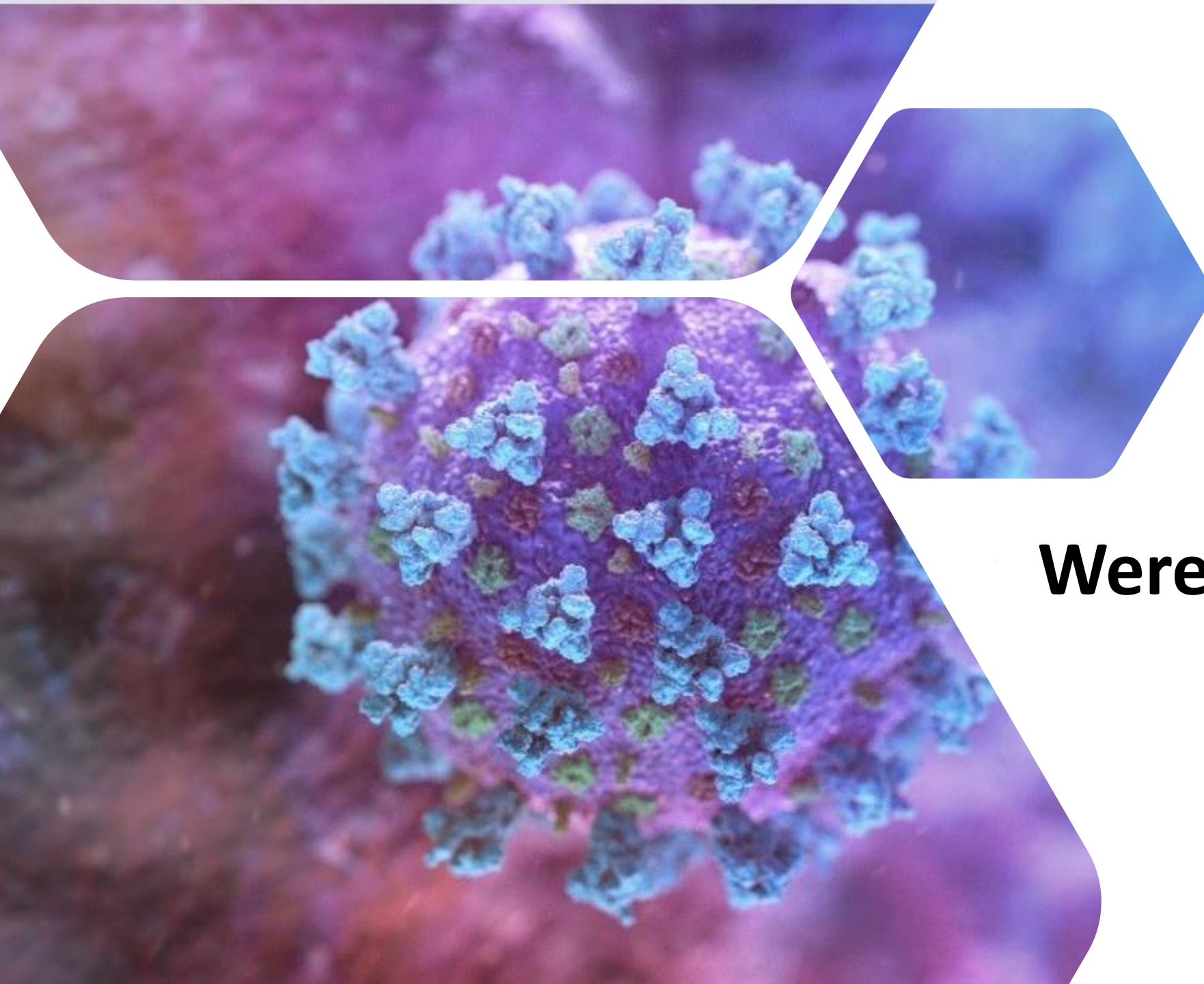


ARE YOU PREPARED SHOULD DISASTER STRIKE?

- > 75% of small businesses do not have a disaster contingency plan in place in the event of a natural disaster or emergency situation.
- > Learn how to be better equipped with our **Emergency Preparedness, Response and Recovery Guide**.



<https://iccwbo.org/media-wall/news-speeches/chambers-take-lead-help-prepare-businesses-next-big-disaster/>



**Were you prepared
for COVID-19?**

**Lawyers can't
keep their eyes
closed and bury
their heads in
the sand**



The background is a dark blue gradient with various abstract elements. There are several large, light blue question marks, some inside circles. There are also smaller, lighter blue question marks scattered around. The background is decorated with white dotted lines, small white squares, and white arrows pointing in different directions. There are also some blurred, glowing orange and yellow shapes that look like bokeh lights.

Most pandemic questions related to the use of technology

- Email
- Cell Phones
- Text Messages
- Remote Access
- Cloud Computing
- Video Chatting
- Teleconferencing

Security

Attorneys and staff working remotely must address the security and confidentiality of their client data, including the need to protect computer systems and physical files, and to ensure that telephone and other conversations and communications remain privileged.

This Isn't New!

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 477R*

May 11, 2017

Revised May 22, 2017

Securing Communication of Protected Client Information

American Bar Association Standing Committee on Ethics and Professional Responsibility Formal Opinion 477R (May 22, 2017)



AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 477R*

May 11, 2017

Revised May 22, 2017

Securing Communication of Protected Client Information

A lawyer generally may transmit information relating to the representation of a client over the [I]nternet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access.



AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 477R*

May 11, 2017

Revised May 22, 2017

Securing Communication of Protected Client Information

However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.



AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 482

September 19, 2018

Ethical Obligations Related to Disasters

**American Bar Association
Standing Committee on Ethics and Professional Responsibility
Formal Opinion 482 (September 19, 2018)**



AMERICAN BAR ASSOCIATION

STUDYING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 482

September 19, 2018

Ethical Obligations Related to Disasters

The Rules of Professional Conduct apply to lawyers affected by disasters. By proper advance preparation and planning and taking advantage of available technology during recovery efforts, lawyers can reduce their risk of violating the Rules of Professional Conduct after a disaster.



AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483

October 17, 2018

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

**American Bar Association
Standing Committee on Ethics and Professional Responsibility
Formal Opinion 483 (October 17, 2018)**



AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483

October 17, 2018

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.



AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483

October 17, 2018

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

Model Rule 1.4 requires lawyers to keep clients “reasonably informed” about the status of a matter and to explain matters “to the extent reasonably necessary to permit a client to make an informed decision regarding the representation.”



AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483

October 17, 2018

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.



AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483

October 17, 2018

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

What the ethics rules requires 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**



AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483

October 17, 2018

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

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

- **Duty to notify clients (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).



This Isn't New!



**PENNSYLVANIA BAR ASSOCIATION
COMMITTEE ON LEGAL ETHICS AND PROFESSIONAL RESPONSIBILITY**

April 10, 2020

FORMAL OPINION 2020-300

ETHICAL OBLIGATIONS FOR LAWYERS WORKING REMOTELY

Recognized that despite the many warnings, many attorneys and their staff were not prepared to work remotely from a home office.



**Numerous questions arose concerning
attorneys' ethical obligations.**

**Pa. Opinion:
Reasoning
Applies to All
Attorneys**



for everyone.

Massachusetts Board of Bar Overseers



ETHICS Q&A IN A COVID-19 WORLD

<https://bit.ly/COVID-Mass>

Reasoning applies to all

Applicable Rules of Professional Conduct

- Rule 1.1 (“Competence”)
- Rule 1.6 (“Confidentiality of Information”)
- Rule 5.1 (“Responsibilities of Partners, Managers, and Supervisory Lawyers”)
- Rule 5.3 (“Responsibilities Regarding Nonlawyer Assistance”)



Minimum
standards





May Store Data in the Cloud

- An attorney may ethically allow client confidential material to be stored in “the cloud” provided:
- (1) all materials remain confidential
- (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks.



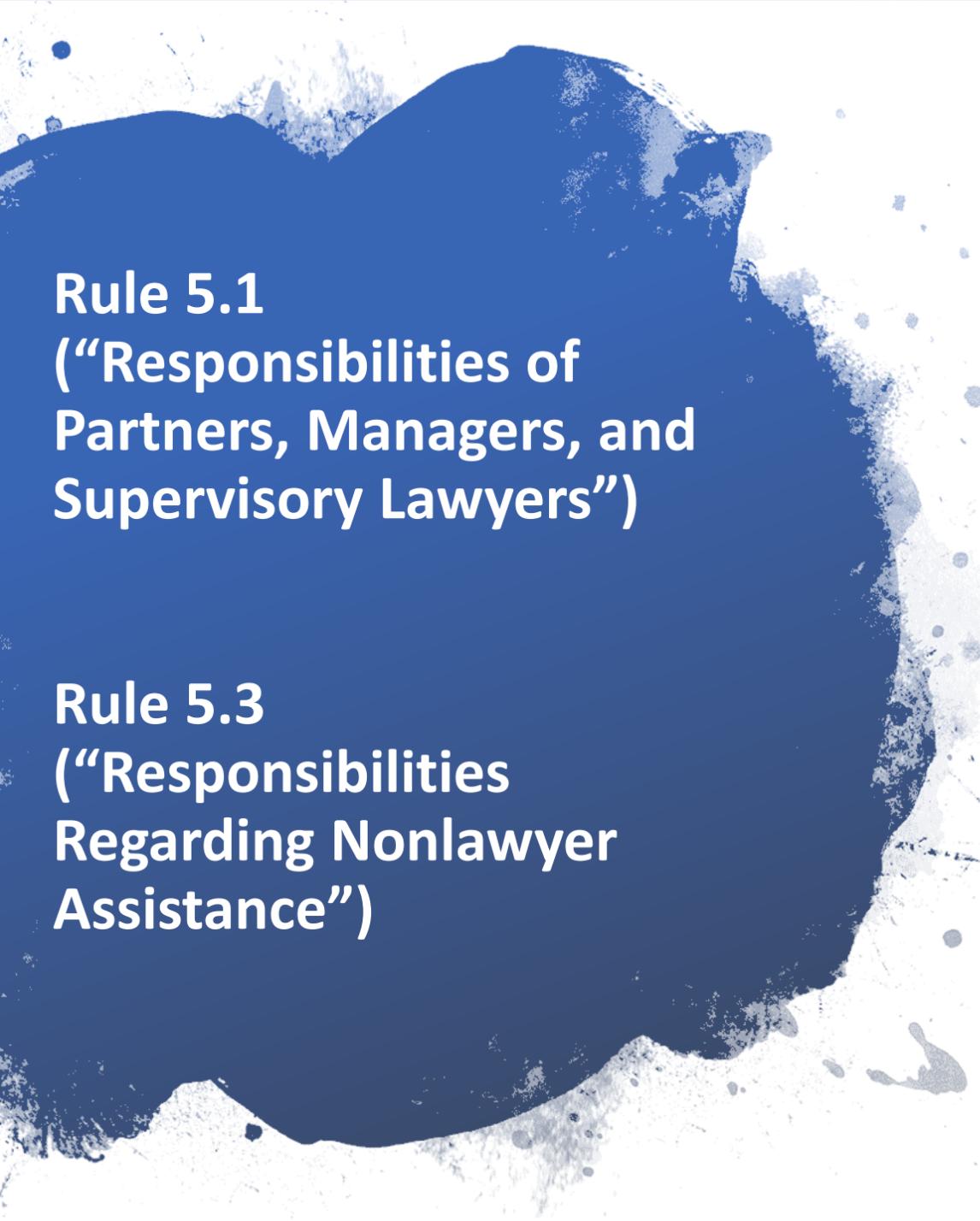
Rule 1.6 (“Confidentiality of Information”) Comment [26]

- **A lawyer must take reasonable precautions to prevent information relating to client representation from access by unintended recipients.**
- **No duty if method affords reasonable expectation of privacy.**
- **Special circumstances, however, may warrant special precautions.**



Rule 1.6 (“Confidentiality of Information”) Comment [26]

- **Factors to consider 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.**
- **Client may require a lawyer to implement special security measures or consent to the use of a means of communication otherwise prohibited by this Rule.**



Rule 5.1
(“Responsibilities of
Partners, Managers, and
Supervisory Lawyers”)

Rule 5.3
(“Responsibilities
Regarding Nonlawyer
Assistance”)

- **A lawyer must make reasonable efforts to ensure the firm has requirements that staff, consultants or others with access to confidential client information or data comply with the Rules of Professional Conduct with regard to data access from remote locations and that any discussions regarding client-related matters are done confidentially.**



at a
minimum

PBA Formal Opinion 2020-300 – *Conclusions* – *Applicable to All*

When working remotely, attorneys and staff have an obligation under the Rules of Professional Conduct to take *reasonable precautions* to assure that:

- All communications, including telephone calls, text messages, email, and video conferencing are conducted in a manner that minimizes the risk of inadvertent disclosure of confidential information



at a
minimum

PBA Formal Opinion 2020-300 – *Conclusions* – *Applicable to All*

When working remotely, attorneys and staff have an obligation under the Rules of Professional Conduct to take *reasonable precautions* to assure that:

- All communications, including telephone calls, text messages, email, and video conferencing are conducted in a manner that minimizes the risk of inadvertent disclosure of confidential information



at a
minimum

PBA Formal Opinion 2020-300 – *Conclusions* – *Applicable to All*

When working remotely, attorneys and staff have an obligation under the Rules of Professional Conduct to take *reasonable precautions* to assure that:

- Information transmitted through the Internet is done in a manner that ensures the confidentiality of client communications and other sensitive data



at a
minimum

PBA Formal Opinion 2020-300 – *Conclusions* – *Applicable to All*

When working remotely, attorneys and staff have an obligation under the Rules of Professional Conduct to take *reasonable precautions* to assure that:

- Their remote workspaces are designed to prevent the disclosure of confidential information in both paper and electronic form



at a
minimum

PBA Formal Opinion 2020-300 – *Conclusions* – *Applicable to All*

When working remotely, attorneys and staff have an obligation under the Rules of Professional Conduct to take reasonable precautions to assure that:

- **Proper procedures are used to secure and backup confidential data stored on electronic devices and in the cloud**



at a
minimum

PBA Formal Opinion 2020-300 – *Conclusions* – *Applicable to All*

When working remotely, attorneys and staff have an obligation under the Rules of Professional Conduct to take reasonable precautions to assure that:

- **Any remotely working staff are educated about and have the resources to make their work compliant with the Rules of Professional Conduct**



at a
minimum

PBA Formal Opinion 2020-300 – *Conclusions* – *Applicable to All*

When working remotely, attorneys and staff have an obligation under the Rules of Professional Conduct to take reasonable precautions to assure that:

- **Appropriate forms of data security are used**

Practical Considerations For *All* Lawyers & Law Firms



General Technology Considerations



Specifying how and where data created remotely will be stored and, if remotely, how the data will be backed up;



Requiring the encryption or use of other security to assure that information sent by electronic mail are protected from unauthorized disclosure;



Using firewalls, anti-virus and anti-malware software, and other similar products to prevent the loss or corruption of data;

General Technology Considerations



Limiting the information that may be handled remotely, as well as specifying which persons may use the information;

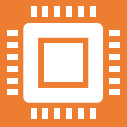


Verifying the identity of individuals who access a firm's data from remote locations;



Implementing a written work-from-home protocol to specify how to safeguard confidential business and personal information;

General Technology Considerations



Requiring the use of a Virtual Private Network or similar connection to access a firm's data;



Requiring the use of two-factor authentication or similar safeguards;



Supplying or requiring employees to use secure and encrypted laptops;

General Technology Considerations

Saving

Saving data permanently only on the office network, not personal devices, and if saved on personal devices, taking reasonable precautions to protect such information;

Obtaining

Obtaining a written agreement from every employee that they will comply with the firm's data privacy, security, and confidentiality policies;

General Technology Considerations



Encrypting electronic records containing confidential data, including backups;



Prohibiting the use of smart devices such as those offered by Amazon Alexa and Google voice assistants in locations where client-related conversations may occur;

General Technology Considerations



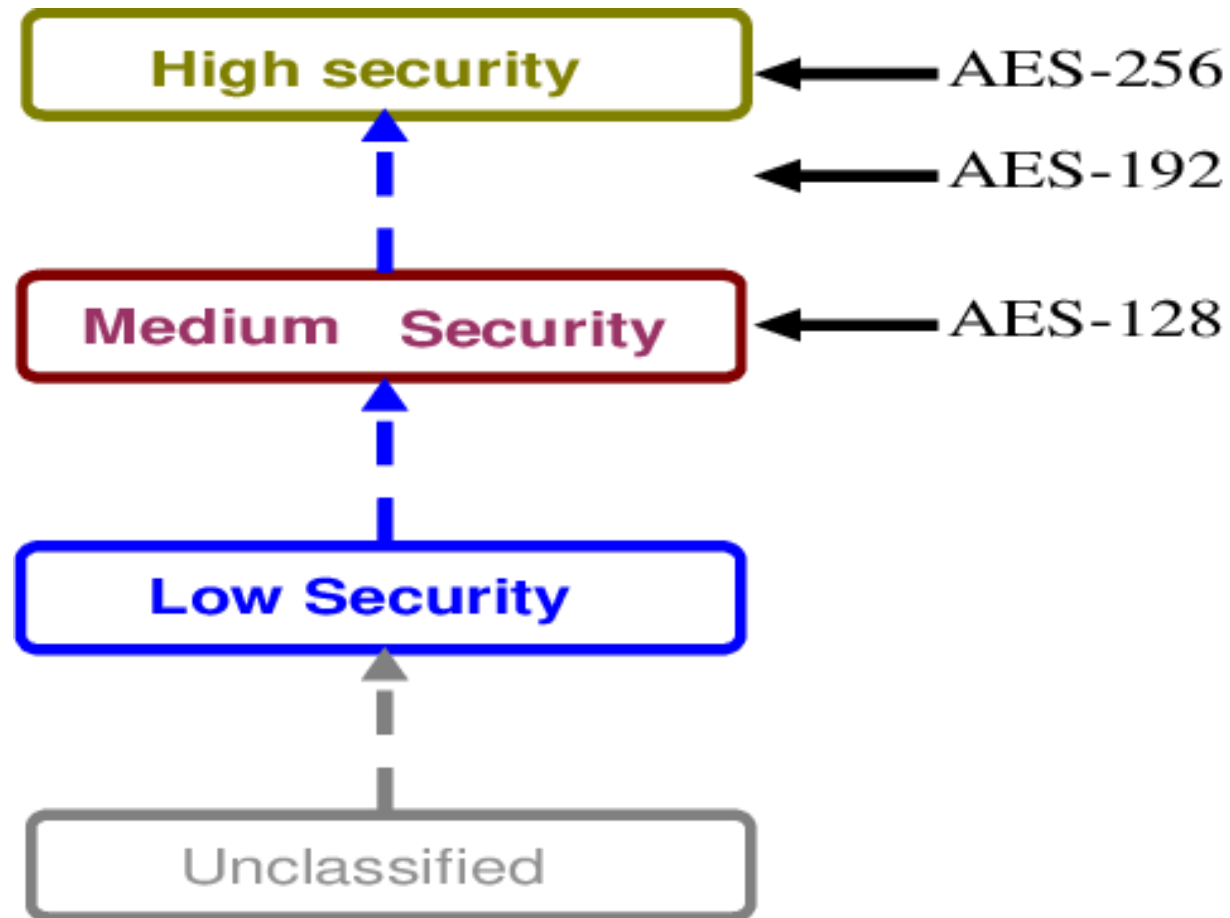
Requiring employees to have client-related conversations in locations where they cannot be overheard by other persons who are not authorized to hear this information; and,



Taking other reasonable measures to assure that all confidential data are protected.

Keep Conversations Private – From People & Devices





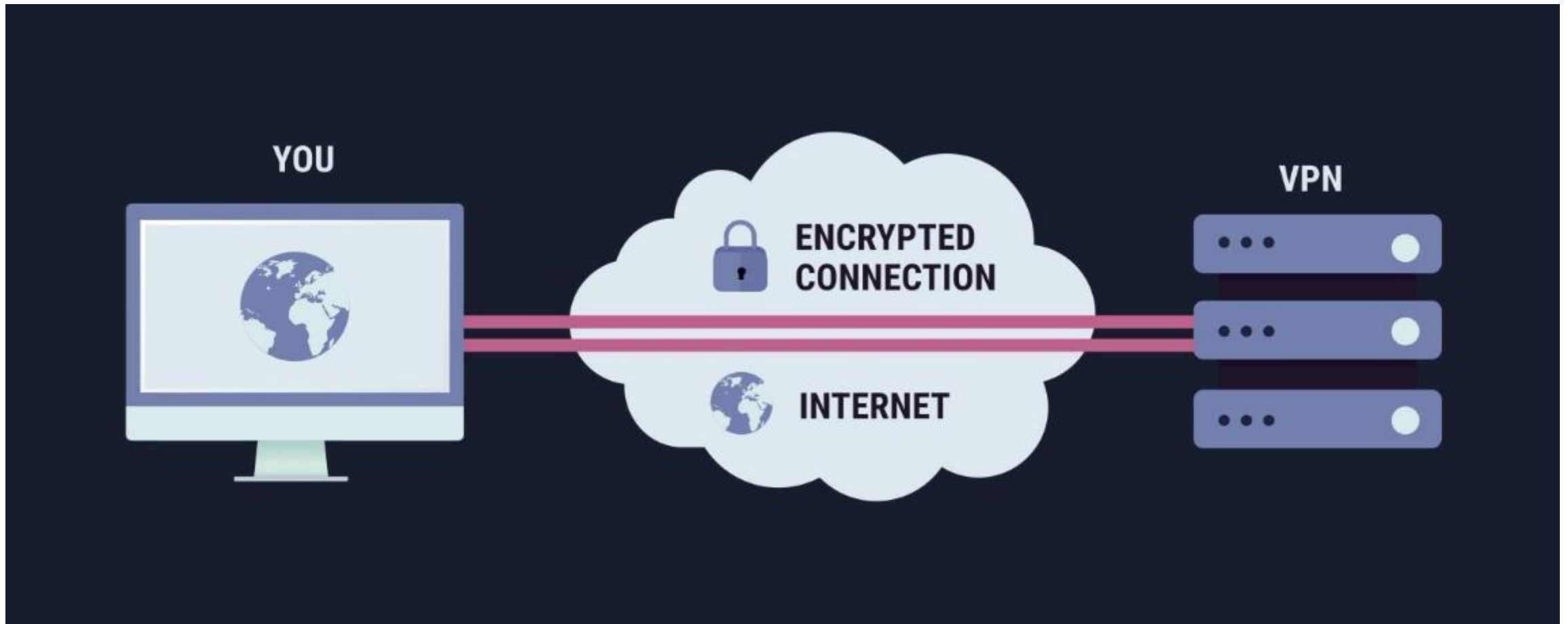
**The Duty to
Assure
Confidentiality &
to Encrypt
Depends Upon
the Information
Being
Transmitted**

Open WiFi

Open Network Security	Secure?
No password	NO!
No password, but has a web portal that requires login	No
Has a password, but is publicly available	No
Has a password, only available upon request	Most secure public WiFi option, but still not secure

**Avoid
Public
& Free
Wi-Fi**

Secure, Encrypted Connection/VPN



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

The background of the slide features a series of concentric, curved lines in a light gray color, creating a sense of motion or a digital environment. On the left side, there is a blue rectangular box with a white border and a small white triangle pointing downwards at the bottom center, resembling a speech bubble or a callout box.

Encrypt your data

- **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, theft/loss of an encrypted hard drive ≠ reportable breach.**

The background of the slide features a series of thin, curved lines in shades of gray, creating a sense of motion or a stylized globe. On the left side, there is a blue speech bubble graphic with a tail pointing towards the bottom left.

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.**

Two-factor authentication

Pick any two: Something you **know**, something you **have**, something you **are**



Use Two Factor Authentication

Or Multi-Factor Authentication

What's the difference between MFA and 2FA?

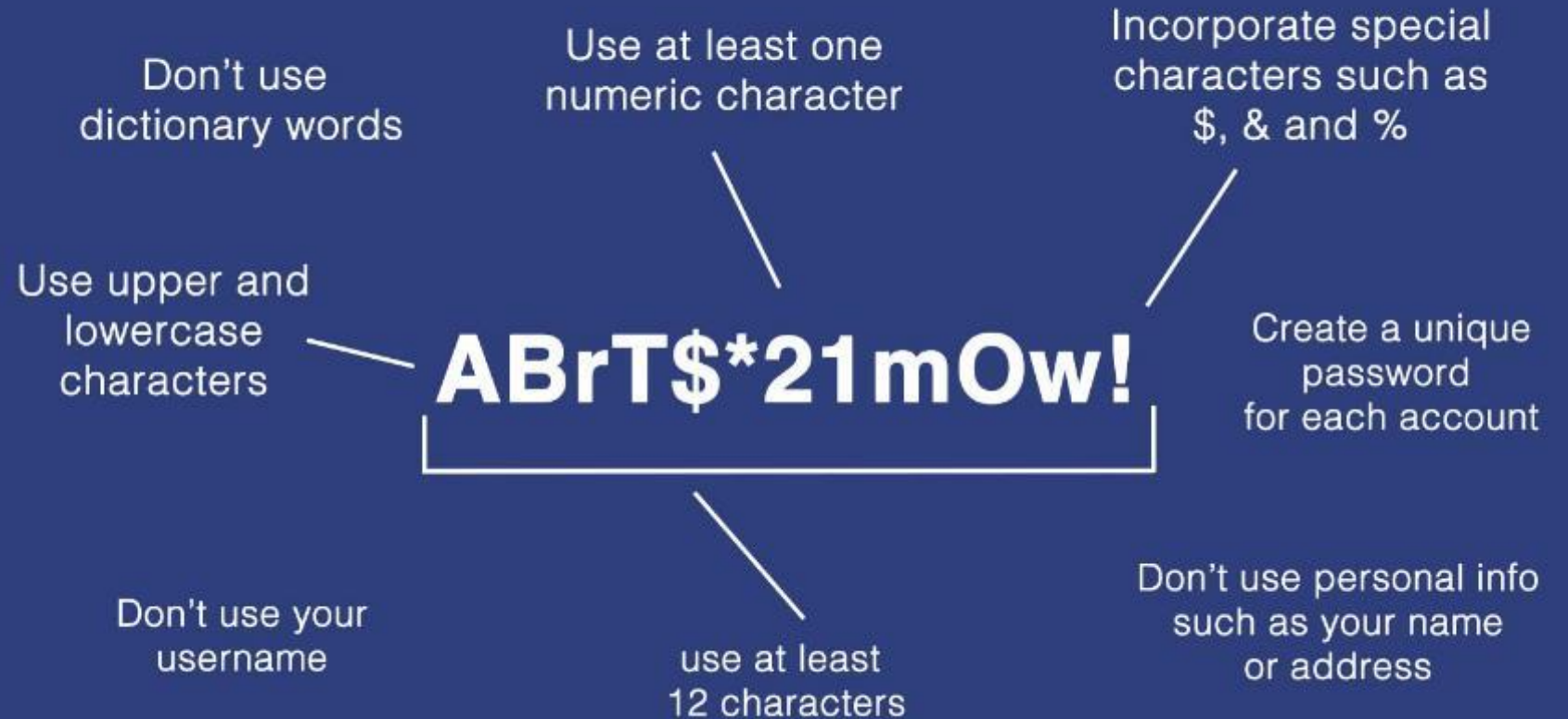
- **Two-factor authentication** always utilizes **two** of these **factors** to verify the user's identity.
- **Multi-factor authentication** could involve **two** of the **factors** or it could involve **all three**.
- “**Multi-factor**” just means any number of **factors** greater than one.

Multi factor authentication



**Use
Strong/
Complex
Passwords**

Creating a Complex Password



Use Strong/ Complex Passwords



Assess the strength of your passwords.



Consider a password manager.



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



Change your good passwords ... occasionally.

zoom



Preventing Zoom- Bombing



CYBERSECURITY INFORMATION

**NSA Guidance on Conferencing:
Selecting and Safely Using Collaboration Services for Telework**

https://bit.ly/NSA_Guidance

Videoconferences Best Security Practices



Password Protect All Meetings



Verify Attendees At Start Of & During Call



Use Video to Show Who You Are & Who Everyone Else Is



Avoid Shared Videoconference Links



Report Suspicious Activity



Use *Only* Secure Video and Phone Conference Services



All Conference Calls Should Have End-to-End Encryption

**Securely
Backup
All Data**





**Remember:
Security,
Security,
Security**

Thank You!



How Technology Can Ethically Unite the Legal Community During Emergencies

Presented by:

Daniel J. Siegel, Esquire





Selecting and Safely Using Collaboration Services for Telework

Summary

During a global pandemic or other crisis contingency scenarios, many United States Government (USG) personnel must operate from home while continuing to perform critical national functions and support continuity of government services. With limited access to government furnished equipment (GFE) such as laptops and secure smartphones, the use of (not typically approved) commercial collaboration services on personal devices for limited government official use becomes necessary and unavoidable.

We define collaboration services as those capabilities that allow the workforce to communicate via internet-enabled text, voice, and video, and can include the sharing of files and other mission content. Collaboration can occur between two people or widened to include a large group to support mission needs.

This document provides a snapshot of best practices and criteria based on capabilities available at the time of publication and was coordinated with the Department of Homeland Security (DHS), which is releasing a similar guide: "Cybersecurity Recommendations for Federal Agencies When Using Video Conferencing Solutions." This NSA publication is designed to provide simple, actionable, considerations for individual government users. The intent of this document is not meant to be exhaustive or based on formal testing, but rather be responsive to a growing demand amongst the federal government to allow its workforce to operate remotely using personal devices when deemed to be in the best interests of the health and welfare of its workforce and the nation.

Recommendations in this document are likely to change as collaboration services evolve and also address known vulnerabilities and threats. Users should be aware that even the most secure collaboration service cannot defend against a compromised user device.

Scope

This document provides security assessment guidance about commercially available collaboration services. It does not cover USG services designed specifically for secure communications, such as Defense Collaboration Services, Intelink Services, and others. NSA strongly recommends use of these dedicated government services, when possible, before any of the commercial services detailed below.

Assessment of individual services for this document focused on those which support multiple operating systems and platforms (e.g., both mobile and desktop).

Audience

The primary audience for this guidance are U.S. Government employees and military service members engaging in telework, especially telework employing personally owned devices such as smartphones and home computers. Teleworkers may not be able to access collaboration services on their respective government enterprise networks, and therefore turn to commercial services for collaboration on vital mission work. These services vary widely in the cybersecurity functionality and assurance that they offer. By using the objective criteria detailed below, government employees and organizations can make more informed decisions about which collaboration services meet their particular needs. By following the practical guidelines, users can draw down their risk exposure and become harder targets for malicious threat actors.

Note that individual departments and agencies may provide specific services or issue specific direction for their teleworkers. This document **does not** override or supersede any official guidance provided by your organization. Consult your department or agency IT support or CIO organization for further guidance.



Criteria to Consider When Selecting a Collaboration Service

The criteria below identifies risks and features to consider when choosing collaboration services to support your mission. All criteria should be strongly considered but may not be fully supported based on your own operating environment and constraints. The criteria is intended to align with related USG guidance to include NIST SP 800-171r2 – *Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations* (Feb 2020) and NIST SP 800-46r2 *Guide to Enterprise Telework, Remote Access and BYOD Security* (Apr 2016).

1. Does the service implement end-to-end encryption?

End-to-end (E2E) encryption means that content (text, voice, video, data, etc.) is encrypted all the way from sender to recipient(s) without being intelligible to servers or other services along the way. Some apps further support encryption while data is at rest, both on endpoints (e.g. your mobile device or workstation) and while residing on remote storage (e.g. servers, cloud storage). Only the originator of the message and the intended recipients should be able to see the unencrypted content. Strong end-to-end encryption is dependent on keys being distributed carefully. Some services such as large-scale group video chat are not designed with end-to-end encryption for performance reasons.

2. Are strong, well-known, testable encryption standards used?

Even in the absence of end-to-end encryption, NSA recommends the use of strong encryption standards, preferably NIST-approved algorithms and current IETF secure protocol standards. Many collaboration services protect data-in-transit between clients and servers via the Transport Layer Security (TLS) version 1.2 (or later) secure protocol, which is commonly used for sensitive but unclassified information. Use of published protocol standards, such as TLS and DTLS-SRTP, is preferred. If the product vendor has created its own encryption scheme or protocol, it should undergo an independent evaluation by an accredited lab. This includes not just cryptographic protocols, but also key generation.

3. Is multi-factor authentication (MFA) used to validate users' identities?

Without MFA, weak or stolen passwords can be used to access legitimate users' accounts and possibly impersonate them during use of the collaboration service. Multi-factor authentication requires that a second form of identification (code, token, out-of-band challenge, etc.) be provided to allow access to an existing account.

4. Can users see and control who connects to collaboration sessions?

The collaboration service should allow organizers to limit access to collaboration sessions to only those who are invited. This can be implemented through such features as session login passwords or waiting rooms, but preferably would support reasonably strong authentication. Users should also be able to see when participants join through unencrypted/unauthenticated means such as telephone calls.

5. Does the service privacy policy allow the vendor to share data with third parties or affiliates?

While collaboration services must often collect certain basic information needed to operate, they should protect sensitive data such as contact details and content. Collaboration information and conversations should not be shared with third parties. This could include metadata associated with user identities, device information, collaboration session history, or various other information that may put your organization at risk. Information sharing should be spelled out clearly in the privacy policy.

6. Do users have the ability to securely delete data from the service and its repositories as needed?

While no services are likely to support full secure overwrite/deletion capabilities, users should be given the opportunity to delete content (e.g. shared files, chat sessions, saved video sessions) and permanently remove accounts that are no longer used.



7. Has the collaboration service's source code been shared publicly (e.g. open source)?

Open source development can provide accountability that code is written to secure programming best practices and isn't likely to introduce vulnerabilities or weaknesses that could put users and data at risk.

8. Has the service and/or app been reviewed or certified for use by a security-focused nationally recognized or government body?

NSA recommends that cloud services (which collaboration apps rely on) be evaluated under the Office of Management and Budget (OMB) FEDRAMP program. NSA also recommends that collaboration apps be evaluated by independent testing labs under the National Information Assurance Partnership (NIAP) against the Application Software Protection Profile (PP) [1]. NSA has worked with the DHS S&T Mobile Security R&D Program to develop excellent semi-automatable testing criteria for app vetting based on the application PP [2]. These criteria include tests of how apps interact with platform resources, how they defend themselves from exploitation, the crypto libraries they use, what permissions they request, and many others.

9. Is the service developed and/or hosted under the jurisdiction of a government with laws that could jeopardize USG official use?

Since it is well documented that some countries require that communications be provided to law enforcement and intelligence services, it may not be wise for certain USG missions to be performed on services hosted or developed under certain foreign legal jurisdictions. Users should be aware that the country of origin where products were developed is not always public knowledge. This criterion was not assessed in the table on page 5.

Using Collaboration Services Securely

If possible, use government furnished equipment (GFE) that is managed and intended for government use only and secure services designed for government use.

No collaboration service can defend against a compromised device. Personal devices are often exposed to considerable risk of compromise due to failure to apply patches in a timely fashion and the installation of applications that users fail to recognize as being malicious (spyware). Resulting malware infections can access files, keystrokes, contacts, call histories, GPS locations, room audio or camera video (even when not on a call), and most any other information the device observes. Even the most secure collaboration service provides no protection against a compromised device.

Carefully managed GFE devices are often more secure than personal devices unless configuration control policies delay the deployment of critical patches. If GFE is available, it should be used. If GFE cannot be used, NSA recommends using a temporary secure operating system such as the Air Force's Trusted End Node Security (TENS) solution to create a "virtual GFE." If neither is practical, users should ensure all user accounts do not have administrator rights (which are only for managing the system) and if possible create a separate user account with low privileges for only work use. Consider using NSA's "Best Practices for Keeping Your Home Network Secure" guide to protect your personal devices.

If you download a collaboration service app, be sure you know where it came from.

Beware of potentially unwanted programs posing as legitimate collaboration apps. Many collaboration services require users to install specialized client software on their systems. If possible, install the correct client directly using the official app store. This helps ensure it is signed and legitimate. If you must download a client from a website, ensure it is from the properly signed secure (e.g. HTTPS) official website. Do not run or install clients from unexpected downloads, especially from links in email or other messaging that may have come from malicious senders. Some services allow users to avoid installing custom apps by using a web interface.

Ensure that encryption is enabled when initiating a collaboration session.

Most collaboration apps do not have specific settings to enable or disable encryption, but where they do, NSA



recommends enabling encryption. When using browser-based services, users should validate that HTTPS is enabled and check the website certificate to ensure it was issued by a trusted certificate authority.

Use the most secure means possible for meeting invitations.

Send meeting invites through other encrypted and authenticated collaboration services if possible. Do not post meeting invites in publicly accessible forums or sites. If invitations must be sent in the clear, organizers should send passwords or PINs by a separate method (e.g. email and SMS or email and phone call).

Verify that only intended invitees are participating before beginning, and throughout, each session.

Ensure that someone is in charge of verifying participants and checking if unknown participants have entered. If participants are not authenticated by the service, at least ensure that their voice or appearance is recognized. Use meeting waiting rooms if possible to allow access to be controlled.

Ensure that any information shared is appropriate for the participants.

Plan beforehand the topics to be covered and consider the implications if the conversation or materials are compromised so that you understand the risks. Be aware of screen-sharing features so that you only share your screen to display content salient to the collaboration session. If content is sensitive, ensure that it is appropriate to share with all participants. Be mindful of the affiliations of those with whom you connect.

Ensure that your physical environment does not provide unintentional access to voice, video, or data during collaboration sessions.

Be aware of your surroundings including any other communications going on (e.g. family members on phone calls or video chats, location hints if working from a sensitive location). Disable unnecessary app permissions (e.g. location services). Ensure there is no other software on your device that is actively sharing microphone data back to a remote server. Note that less-trusted devices, to include Internet of Things (IoT), often have microphones or cameras, so it may be wise to leave personal cell phones or computers in a different room if they are not being used for work.



Service	Basic Functionality	1 – E2E Encryption	2 – Testable Encryption	3 – MFA	4 – Invitation Controls	5 – Minimal 3 rd Party Sharing	6 – Secure Deletion	7 – Public Source Code Shared	8 – Certified Service (FedRAMP / NIAP)
Cisco Webex ^{®9}	a, b, c, d, e	Y ¹	Y	Y ¹²	Y ¹	Y	Client – Y Server – N ³	N	FedRAMP
Dust	a	Y	N ³	N	Y	N	Client – Y Server – Y	N	None
Google G Suite ^{™10}	a, b, c, d	N	Y	Y ¹	Y ¹	Y	Client – Y Server – Y ²	N	FedRAMP
GoToMeeting ^{®11}	a, b, c	Y ¹	Y	N	Y ¹	Y	Client – Y Server – N ³	N	None
Mattermost ^{™12}	a, b, c, e	Y	Y	Y ²	Y	N	Client – Y Server – N	Y	FedRAMP
Microsoft Teams ^{®13}	a, c, d, e	N	Y	Y	Y	Y	Client – Y ¹ Server – Y ¹	N	FedRAMP
Signal ^{®14}	a, b, d	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Skype for Business ^{™15}	a, c, d, e	Y ⁴	Y ⁴	Y	Y	N	Client – Y Server – N ³	N	None
Slack ^{®16}	a, c, d, e	N	Y	Y	Y	N ³	Client – N Server – N	N	FedRAMP
SMS Text	a, d	N	N	N	N	N	Client – Y Server – N	N	None
WhatsApp ^{®17}	a, c, d	Y	Y	Y	Y	Y	Client – Y Server – Y	N	None
Wickr ^{®18}	a, c, d, e	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Zoom ^{®19}	a, b, c, e	Y ¹⁴	Y	N	Y	Y	Client – Y Server – N ³	N	FedRAMP

Table of Assessments against Criteria

Legend: Y = Yes, N = No; (a) text chat, (b) voice conferencing, (c) video conferencing, (d) file sharing, (e) screen sharing.

¹ Configurable

² Free Version - N

³ No Published Details

⁴ Partial



Assessment of Common Collaboration Services Against the Criteria

The above table presents an initial assessment of how available commercial collaboration services satisfy our security criteria. The selection of services for this initial assessment was driven by inquiries and usage from across NSA's national security customer base; this is not a comprehensive list of services or possible criteria.

NSA analysts gathered factual material from published company literature and product specifications, supplemented by other openly published analyses and basic hands-on technical observation. No formal testing was performed on products or services for this analysis. These assessment findings are meant to serve as an input for government employees and organizations. Users of these services must exercise judgment when choosing a service for their particular mission telework needs.

Works Cited

- [1] NIAP (Mar. 1, 2019) Application Software Protection Profile, [Online] Available at <https://www.niap-ccevs.org/Profile/Info.cfm?PPID=429&id=429> [Accessed Apr. 20, 2020]
- [2] NSA (Sep. 18, 2018) Guide "Best Practices for keeping Your Home Network Secure" [Online] Available at <https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-best-practices-for-keeping-home-network-secure.pdf> [Accessed Apr. 20, 2020]

Disclaimers

Note that this does not constitute a Qualified Products List, within the meaning of the definition of Federal Acquisition Regulation (FAR) 2.101 or a Qualified Manufacturers List under FAR subpart 9.2—Qualification Requirements. The government has not undertaken any testing or evaluation of the products listed under this analysis, but has only reviewed the published attributes of the products. The list is not all-inclusive. This list may be amended and supplemented from time to time as market research discloses other items or new products become available. The descriptions and procedures explained in this document do not constitute or imply an endorsement by NSA/CSS, DoD, or USG of the products in question. It is intended solely for the non-commercial use of USG personnel for purpose of explaining and giving operating instructions for the use of the particular product in question. Any further use for other purposes is prohibited.

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov

⁹ Cisco Webex is a registered trademark of Cisco Systems, Inc.

¹⁰ Google G Suite is a trademark of Google, LLC

¹¹ GoToMeeting is a registered trademark of LogMein, Inc.

¹² Mattermost is a trademark of Mattermost, Inc.

¹³ Microsoft Teams is a registered trademark of Microsoft Corporation

¹⁴ Signal is a registered trademark of Signal Technology Foundation

¹⁵ Skype for Business is a trademark of Microsoft Corporation

¹⁶ Slack is a registered trademark of Slack Technologies, Inc.

¹⁷ WhatsApp is a registered trademark of WhatsApp, Inc.

¹⁸ Wickr is a registered trademark of Wickr, Inc.

¹⁹ Zoom is a registered trademark of Zoom Video Communications, Inc.

Technology Can Ethically Unite the Legal Community During Emergencies

[law.com/thelegalintelligencer/2020/04/23/technology-can-ethically-unite-the-legal-community-during-emergencies](https://www.law.com/thelegalintelligencer/2020/04/23/technology-can-ethically-unite-the-legal-community-during-emergencies)

By, Daniel J.
Siegel

Daniel J. Siegel.



The world is full of divides. There are socio-economic divides, cultural divides, religious divides and political divides. There are divides of every type.

In the legal community, there are divides that separate midsize and large firms from solo and small firms. During this COVID-19 pandemic, the economic parameters of that divide are even more distinct. For example, I sit on a board of a legal magazine, where 13 of the 18 board members have job assurance. In other words, when the pandemic ends, 13 of my colleagues know that they will be able to return to their offices and will have suffered none or minimal

economic hardship. As a result, those board members are able to devote part of the quarantine period to arguing in emails about irrelevant minutiae, while five of us must focus on how to pay our staff and ourselves until, we hope, the situation returns to “normal.”

There is one area, however, where lawyers can bridge the divide and size does not matter: legal technology. We all need to use technology, whether to work remotely or to connect with family during Passover or Easter dinners. And during a pandemic, technology can be an equalizer, or perhaps an advantage, not based upon firm size, but upon a firm’s and a lawyer’s willingness to recognize that technology is a friend, not the enemy.

This column will therefore explain the basics of what attorneys can do to thrive while working remotely. In general, attorneys must cross the Red Sea that divides the tech Luddites from their more tech-savvy colleagues and recognize the importance of employing

technology in a manner that maximizes efficiency while also complying with their ethical obligations to protect client confidentiality.

Legal technology is a great equalizer. Firms of all sizes use it, not just now but all the time to gain advantages not easily transferable to paper. Technology it is not necessarily expensive, and it often can be up and running quickly—even in a way that makes remote work relatively simply. Yet ever since we all discovered quarantined life, we have heard the screams.

One colleague sent the following email:

Everyone—I am forced to disconnect my office computer in about an hour or so, to take home, where I have no computer or INTERNET CONNECTION. I have to choose an ISP and learn how to get back on the internet to start working. Talk about a babe in the woods! So I am not on email till I get my ISP, get set up, and learn stuff. Please call me at home for anything important, including telephone or virtual meetings, etc.

Another wrote the following email:

What good is working from home? When I log into my computer all I see are a few things, but I can't work this way.

One columnist in this publication even lamented that the “stay-at-home orders and quarantines have proven disastrous” and are a “wake-up call” to “learn how to fix things on a computer and learn how to electronically file motions with the court without relying on secretaries and paralegals to do so for them.” His fear was so paralyzing that he believed that “If electronics did not work, most firms would go totally out of business, and run out of revenue very quickly.”

Of greater concern, his understanding of his ethical obligations was woefully lacking, as evidenced by his statement that “It is illegal to text or email anything of substance.” He is almost certainly not alone in that mistaken belief.

Working remotely is not new, it is something lawyers and countless other workers have done for a long time. Some lawyers even have virtual offices, where they serve clients online and do not have traditional brick-and-mortar locations.

Many companies devote their efforts to helping law firms and other businesses prepare not just for pandemics, but for when their employees need to work remotely. In my office, for example, one attorney was under the weather and worked remotely for weeks before the current quarantine period. Her work product did not change, but by having her work from home, we avoided catching whatever she had. And she wasn't using a typewriter to do her “home work.”

Perhaps that is why Google only lists two businesses in the results of a search for local typewriter stores, and lists seemingly endless pages of results when searching for “small business technology consultants in Philadelphia.”

Fortunately, there is help even for those searching for an internet provider. There is also ethical guidance to dispel any notion that the police will arrest lawyers who send “anything of substance” by email. To provide even more guidance, on April 14, the Pennsylvania Bar Association committee on legal ethics and professional responsibility issued Formal Opinion 2020-300 ([“Ethical Obligations For Lawyers Working Remotely”](#)), which summarizes the considerations relevant for attorneys working remotely, not just now, but whenever the need arises.

I was a primary author of the opinion and I am co-vice chair of the committee that issued the opinion. We issued the opinion to convey the information law firms needed in a nontechnical manner that would highlight that maintaining ethical obligations while working remotely is not difficult. To the contrary, it simply requires attorneys to take “reasonable” precautions, reasonable being the operative word. Of course, reasonable means that lawyers need to have basic technology, like the internet, a working desktop or laptop computer, and a working understanding of how to use the internet, and the software installed on those computers.

Opinion 2020-300 goes further. It explains what should be obvious, that “attorneys and staff working remotely must consider the security and confidentiality of their client data, including the need to protect computer systems and physical files, and to ensure that telephone and other conversations and communications remain privileged.” This merely means that attorneys must employ the same considerations as they do with physical files and in-office phone calls.

Next, the opinion adopts the reasoning in American Bar Association standing committee on ethics and professional responsibility Formal Opinion 477R, released in 2017, that a lawyer generally may transmit information relating to the representation of a client over the internet without violating the Rules of Professional Conduct provided the lawyer undertakes reasonable efforts to prevent inadvertent or unauthorized access. The ABA opinion notes, however, that, a “lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.” In other words, if the information being sent is sensitive or confidential, a lawyer should send it in a manner (using techniques such as encryption or password-protection) that avoids allowing “anyone” to see it.

None of this advice differs from what lawyers were taught years ago. For example, in the early 1980s, my law school professors emphasized the importance of keeping client communications confidential. That obligation remains, it just must be done with computers

now. In that regard, the PBA opinion explains that, at a minimum, when working remotely, attorneys and their staff have an obligation under the Rules of Professional Conduct to take reasonable precautions to assure that:

- All communications, including telephone calls, text messages, email and video conferencing are conducted in a manner that minimizes the risk of inadvertent disclosure of confidential information;
- Information transmitted through the internet is done in a manner that ensures the confidentiality of client communications and other sensitive data;
- Their remote workspaces are designed to prevent the disclosure of confidential information in both paper and electronic form;
- Proper procedures are used to secure and back up confidential data stored on electronic devices and in the cloud;
- Any remotely working staff are educated about and have the resources to make their work compliant with the Rules of Professional Conduct; and,
- Appropriate forms of data security are used.”

Section III of the PBA opinion helps lawyers understand their duties of competence and confidentiality when working remotely. The opinion notes that the Pennsylvania Rules of Professional Conduct were amended in 2013 to explain that a “competent” lawyer must understand the risks and benefits of technology. In addition, the Comments to Rule 1.6 highlight that, at times, as was explained in ABA Opinion 477R, a lawyer must take additional precautions when sending confidential information electronically.

The PBA opinion further explains that the duty to assure confidentiality depends upon the information being transmitted. Lunch plans, for example, are not confidential but a memo about the intricacies of a client’s merger are.

From there, the opinion urges attorneys to avoid using public Internet and free Wi-Fi, the type of connections found at coffee shops and other locations. Instead, lawyers should utilize technology such as virtual private networks (VPNs), two- or multi-factor authentication, and strong passwords to enhance the security of their communications.

The opinion also discusses the problems highlighted recently by the FBI about security risks with some videoconferencing services. And finally, there is guidance about other cybersecurity concerns. This is the same information often found in a daily newspaper’s technology column, just refocused for lawyers and their staff.

The COVID-19 pandemic has forced all lawyers, and judges, and virtually everyone else involved in the legal system, to recognize the need to work remotely in a secure manner that protects client confidentiality. Even if there were no computers during this period, lawyers would still have to communicate with clients in a confidential manner. Technology is just the means that we now use.

Technology in law is also not new. Shiva Ayyadurai invented email in 1971. Westlaw was released in 1975, in response to the launch of Lexis online research in 1973. Finally, by 1986, IBM discontinued sales of the Selectric typewriter, the mainstay of law firms and other businesses, because those staples of virtually every business were being supplanted by word processors and computers.

As social media entrepreneur Matt Mullenweg said, "Technology is best when it brings people together."

During the COVID-19 pandemic, it is technology that brings us together, not just for holiday celebrations, but as part of infrastructure that unites lawyers, law firms and clients.

Daniel J. Siegel, *principal of the Law Offices of Daniel J. Siegel, provides ethical guidance and Disciplinary Board representation for attorneys and law firms. He is the editor of "Fee Agreements in Pennsylvania (6th Edition)" and author of "Leaving a Law Practice: Practical and Ethical Issues for Lawyers and Law Firms (Second Edition)," published by the Pennsylvania Bar Institute. Contact him at dan@danieljsiegel.com.*



**PENNSYLVANIA BAR ASSOCIATION
COMMITTEE ON LEGAL ETHICS AND PROFESSIONAL RESPONSIBILITY**

April 10, 2020

FORMAL OPINION 2020-300

ETHICAL OBLIGATIONS FOR LAWYERS WORKING REMOTELY

I. Introduction and Summary

When Pennsylvania Governor Tom Wolf ordered all “non-essential businesses,” including law firms to close their offices during the COVID-19 pandemic, and also ordered all persons residing in the state to stay at home and leave only under limited circumstances, many attorneys and their staff were forced to work from home for the first time. In many cases, attorneys and their staff were not prepared to work remotely from a home office, and numerous questions arose concerning their ethical obligations.

Most questions related to the use of technology, including email, cell phones, text messages, remote access, cloud computing, video chatting and teleconferencing. This Committee is therefore providing this guidance to the Bar about their and their staff’s obligations not only during this crisis but also as a means to assure that attorneys prepare for other situations when they need to perform law firm- and client-related activities from home and other remote locations.

Attorneys and staff working remotely must consider the security and confidentiality of their client data, including the need to protect computer systems and physical files, and to ensure that telephone and other conversations and communications remain privileged.

In Formal Opinion 2011-200 (Cloud Computing/Software As A Service While Fulfilling The Duties of Confidentiality and Preservation of Client Property) and Formal Opinion 2010-200 (Ethical Obligations on Maintaining a Virtual Office for the Practice of Law in Pennsylvania), this Committee provided guidance to attorneys about their ethical obligations when using software and other technology to access confidential and sensitive information from outside of their physical offices, including when they operated their firms as virtual law offices. This Opinion affirms the conclusions of Opinions 2011-200 and 2010-200, including:

- An attorney may ethically allow client confidential material to be stored in “the cloud” provided the attorney takes reasonable care to assure that (1) all materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks.
- An attorney may maintain a virtual law office in Pennsylvania, including a virtual law office in which the attorney works from home, and associates work from their homes in various locations, including locations outside of Pennsylvania;
- An attorney practicing in a virtual office at which attorneys and clients do not generally meet face to face must take appropriate safeguards to: (1) confirm the identity of clients and others; and, (2) address those circumstances in which a client may have diminished capacity.

This Opinion also affirms and adopts the conclusions of the American Bar Association Standing Committee on Ethics and Professional Responsibility in Formal Opinion 477R (May 22, 2017) that:

A lawyer generally may transmit information relating to the representation of a client over the [I]nternet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

The duty of technological competence requires attorneys to not only understand the risks and benefits of technology as it relates to the specifics of their practices, such as electronic discovery. This also requires attorneys to understand the general risks and benefits of technology, including the electronic transmission of confidential and sensitive data, and cybersecurity, and to take reasonable precautions to comply with this duty. In some cases, attorneys may have the requisite knowledge and skill to implement technological safeguards. In others, attorneys should consult with appropriate staff or other entities capable of providing the appropriate guidance.

At a minimum, when working remotely, attorneys and their staff have an obligation under the Rules of Professional Conduct to take reasonable precautions to assure that:

- All communications, including telephone calls, text messages, email, and video conferencing are conducted in a manner that minimizes the risk of inadvertent disclosure of confidential information;
- Information transmitted through the Internet is done in a manner that ensures the confidentiality of client communications and other sensitive data;
- Their remote workspaces are designed to prevent the disclosure of confidential information in both paper and electronic form;

- Proper procedures are used to secure and backup confidential data stored on electronic devices and in the cloud;
- Any remotely working staff are educated about and have the resources to make their work compliant with the Rules of Professional Conduct; and,
- Appropriate forms of data security are used.

In Section II, this Opinion highlights the Rules of Professional Conduct implicated when working at home or other locations outside of a traditional office. Section III highlights best practices and recommends the baseline at which attorneys and staff should operate to ensure confidentiality and meet their ethical obligations. This Opinion does not discuss specific products or make specific technological recommendations, however, because these products and services are updated frequently. Rather, Section III highlights considerations that will apply not only now but also in the future.

II. Discussion

A. Pennsylvania Rules of Professional Conduct

The issues in this Opinion implicate various Rules of Professional Conduct that affect an attorney's responsibilities towards clients, potential clients, other parties, and counsel, primarily focused on the need to assure confidentiality of client and sensitive information. Although no Pennsylvania Rule of Professional Conduct specifically addresses the ethical obligations of attorneys working remotely, the Committee's conclusions are based upon the existing Rules, including:

- Rule 1.1 ("Competence")
- Rule 1.6 ("Confidentiality of Information")
- Rule 5.1 ("Responsibilities of Partners, Managers, and Supervisory Lawyers")
- Rule 5.3 ("Responsibilities Regarding Nonlawyer Assistance")

The Rules define the requirements and limitations on an attorney's conduct that may subject the attorney, and persons or entities supervised by the attorney, to disciplinary sanctions. Comments to the Rules assist attorneys in understanding or arguing the intention of the Rules, but are not enforceable in disciplinary proceedings.

B. Competence

A lawyer's duty to provide competent representation includes the obligation to understand the risks and benefits of technology, which this Committee and numerous other similar committees believe includes the obligation to understand or to take reasonable measures to use appropriate technology to protect the confidentiality of communications in both physical and electronic form.

Rule 1.1 ("Competence") states in relevant part:

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

Further, Comment [8] to Rule 1.1 states

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. To provide competent representation, a lawyer should be familiar with policies of the courts in which the lawyer practices, which include the Case Records Public Access Policy of the Unified Judicial System of Pennsylvania.

Consistent with this Rule, attorneys must evaluate, obtain, and utilize the technology necessary to assure that their communications remain confidential.

C. Confidentiality

An attorney working from home or another remote location is under the same obligations to maintain client confidentiality as is the attorney when working within a traditional physical office.

Rule 1.6 (“Confidentiality of Information”) states in relevant part:

(a) A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraphs (b) and (c).

...

(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.

Comments [25] and [26] to Rule 1.6 state:

[25] Pursuant to paragraph (d), a lawyer should act in accordance with court policies governing disclosure of sensitive or confidential information, including the Case Records Public Access Policy of the Unified Judicial System of Pennsylvania. 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 Rules 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 Rule 5.3, Comments [3]-[4].

[26] 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.

Comment [25] explains that an attorney's duty to understand the risks and benefits of technology includes the obligation to safeguard client information (1) against unauthorized access by third parties (2) against inadvertent or unauthorized disclosure by the lawyer or other persons subject to the lawyer's supervision. Comment [26] explains that an attorney must safeguard electronic communications, such as email, and may need to take additional measures to prevent information from being accessed by unauthorized persons. For example, this duty may require an attorney to use encrypted email, or to require the use of passwords to open attachments, or take other reasonable precautions to assure that the contents and attachments are seen only by authorized persons.

A lawyer's confidentiality obligations under Rule 1.6(d) are, of course, not limited to prudent employment of technology. Lawyers working from home may be required to bring paper files and other client-related documents into their homes or other remote locations. In these circumstances, they should make reasonable efforts to ensure that household residents or visitors who are not associated with the attorney's law practice do not have access to these items. This can be accomplished by maintaining the documents in a location where unauthorized persons are denied access, whether through the direction of a lawyer or otherwise.

D. Supervisory and Subordinate Lawyers

Rule 5.1 ("Responsibilities of Partners, Managers, and Supervisory Lawyers") states:

(a) A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.

(b) A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.

(c) A lawyer shall be responsible for another lawyer's violation of the Rules of Professional Conduct if:

(1) the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the other lawyer practices, or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Rule 5.3 ("Responsibilities Regarding Nonlawyer Assistance") states:

With respect to a nonlawyer employed or retained by or associated with a lawyer:

(a) a partner and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer.

(b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and,

(c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

(1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and in either case knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Therefore, a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, must make reasonable efforts to ensure that the firm has in effect requirements that any staff, consultants or other entities that have or may have access to confidential client information or data comply with the Rules of Professional Conduct with regard to data access from remote locations and that any discussions regarding client-related matters are done confidentially.

III. Best Practices When Performing Legal Work and Communications Remotely¹

A. General Considerations

In Formal Opinion 2011-200, this Committee concluded that a lawyer's duty of competency extends "beyond protecting client information and confidentiality; it also includes a lawyer's ability to reliably access and provide information relevant to a client's case when needed. This is essential for attorneys regardless of whether data is stored onsite or offsite with a cloud service provider." When forced to work remotely, attorneys remain obligated to take reasonable precautions so that they are able to access client data and provide information to the client or to others, such as courts or opposing counsel.

While it is beyond the scope of this Opinion to make specific recommendations, the Rules and applicable Comments highlight that the need to maintain confidentiality is crucial to preservation of the attorney-client relationship, and that attorneys working remotely must take appropriate measures to protect confidential electronic communications. While the measures necessary to do so will vary, common considerations include:

¹ These various considerations and safeguards also apply to traditional law offices. The Committee is not suggesting that the failure to comply with the "best practices" described in Section III of this Opinion would necessarily constitute a violation of the Rules of Professional Conduct that would subject an attorney to discipline. Rather, compliance with these or similar recommendations would constitute the type of reasonable conduct envisioned by the Rules.

- Specifying how and where data created remotely will be stored and, if remotely, how the data will be backed up;
- Requiring the encryption or use of other security to assure that information sent by electronic mail are protected from unauthorized disclosure;
- Using firewalls, anti-virus and anti-malware software, and other similar products to prevent the loss or corruption of data;
- Limiting the information that may be handled remotely, as well as specifying which persons may use the information;
- Verifying the identity of individuals who access a firm's data from remote locations;
- Implementing a written work-from-home protocol to specify how to safeguard confidential business and personal information;
- Requiring the use of a Virtual Private Network or similar connection to access a firm's data;
- Requiring the use of two-factor authentication or similar safeguards;
- Supplying or requiring employees to use secure and encrypted laptops;
- Saving data permanently only on the office network, not personal devices, and if saved on personal devices, taking reasonable precautions to protect such information;
- Obtaining a written agreement from every employee that they will comply with the firm's data privacy, security, and confidentiality policies;
- Encrypting electronic records containing confidential data, including backups;
- Prohibiting the use of smart devices such as those offered by Amazon Alexa and Google voice assistants in locations where client-related conversations may occur;
- Requiring employees to have client-related conversations in locations where they cannot be overheard by other persons who are not authorized to hear this information; and,
- Taking other reasonable measures to assure that all confidential data are protected.

B. Confidential Communications Should be Private

1. Introduction

When working at home or from other remote locations, all communications with clients must be and remain confidential. This requirement applies to all forms of communications, including phone calls, email, chats, online conferencing and text messages.

Therefore, when speaking on a phone or having an online or similar conference, attorneys should dedicate a private area where they can communicate privately with clients, and take reasonable precautions to assure that others are not present and cannot listen to the conversation. For example, smart devices such as Amazon's Alexa and Google's voice assistants may listen to conversations and record them. Companies such as Google and Amazon maintain those recordings on servers and hire people to review the recordings. Although the identity of the

speakers is not disclosed to these reviewers, they might hear sufficient details to be able to connect a voice to a specific person.²

Similarly, when communicating using electronic mail, text messages, and other methods for transmitting confidential and sensitive data, attorneys must take reasonable precautions, which may include the use of encryption, to assure that unauthorized persons cannot intercept and read these communications.

2. What is Encryption?

Encryption is the method by which information is converted into a secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography. Unencrypted data is also known as plaintext, and encrypted data is called ciphertext. The formulas used to encode and decode messages are called encryption algorithms or ciphers.³

When an unauthorized person or entity accesses an encrypted message, phone call, document or computer file, the viewer will see a garbled result that cannot be understood without software to decrypt (remove) the encryption.

3. The Duty to Assure Confidentiality Depends Upon the Information Being Transmitted

This Opinion adopts the analysis of ABA Formal Opinion 477R concerning a lawyer's duty of confidentiality:

At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors. In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method.

Therefore, in an environment of increasing cyber threats, the Committee concludes that, adopting the language in the ABA Cybersecurity Handbook, the reasonable efforts standard:

² <https://www.vox.com/recode/2020/2/21/21032140/alexa-amazon-google-home-siri-apple-microsoft-cortana-recording>

³ <https://searchsecurity.techtarget.com/definition/encryption>

. . . rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a “process” to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c)⁴ includes nonexclusive factors to guide lawyers in making a “reasonable efforts” determination. Those factors include:

- 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 fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances. Model Rule 1.4 may require a lawyer to discuss security safeguards with clients. Under certain circumstances, the lawyer may need to obtain informed consent from the client regarding whether to the use enhanced security measures, the costs involved, and the impact of those costs on the expense of the representation where nonstandard and not easily available or affordable security methods may be required or requested by the client. Reasonable efforts, as it pertains to certain highly sensitive information, might require avoiding the use of electronic methods or any technology to communicate with the client altogether, just as it warranted avoiding the use of the telephone, fax and mail in Formal Opinion 99-413.

In contrast, for matters of normal or low sensitivity, standard security methods with low to reasonable costs to implement, may be sufficient to meet the reasonable-efforts standard to protect client information from inadvertent and unauthorized disclosure.

In addition to the obligations under the Pennsylvania Rules of Professional Conduct, which are based upon the Model Rules, clients may also impose obligations upon attorneys to protect confidential or sensitive information. For example, some commercial clients, such as banks, routinely require that sensitive information be transmitted only with a password protocol or using an encryption method.

C. There Are Many Ways to Enhance Your Online Security

⁴ Pennsylvania did not adopt Comment [18] in its entirety.

While this Opinion cannot provide guidance about specific products or services, its goal is to provide attorneys and law firms with guidance about how they can meet their obligation of competence while preserving client confidentiality. The following subsections of this Opinion outline some reasonable precautions that attorneys should consider using to meet their ethical obligations.

1. Avoid Using Public Internet/Free Wi-Fi

Attorneys should avoid using unsecured free Internet/Wi-Fi hotspots when performing client- or firm-related activities that involve access to or the transmission of confidential or sensitive data. Persons, commonly called hackers, can access every piece of unencrypted information you send out to the Internet, including email, credit card information and credentials used to access or login to businesses, including law firm networks. Hackers can also use an unsecured Wi-Fi connection to distribute malware. Once armed with the user's login information, the hacker may access data at any website the user accesses.

2. Use Virtual Private Networks (VPNs) to Enhance Security

A VPN, or Virtual Private Network, allows users to create a secure connection to another network over the Internet, shielding the user's activity from unauthorized persons or entities. VPNs can connect any device, including smartphones, PCs, laptops and tablets to another computer (called a server), encrypting information and shielding your online activity from all other persons or entities, including cybercriminals. Thus, the use of a VPN can help to protect computers and other devices from hackers.

3. Use Two-Factor or Multi-Factor Authentication

Two-Factor or Multi-Factor Authentication is a security method that requires users to prove their identity in more than one way before signing into a program or a website. For example, a user might require a login name and a password, and would then be sent a four- or six-digit code by text message to enter on the website. Entering this additional authentication helps to ensure only authorized persons are accessing the site. Although these forms of enhanced security may seem cumbersome, its use provides an additional layer of security beyond simple password security.

4. Use Strong Passwords to Protect Your Data and Devices

One of the most common ways that hackers break into computers, websites and other devices is by guessing passwords or using software that guesses passwords, which remain a critical method of gaining unauthorized access. Thus, the more complex the password, the less likely that an unauthorized user will access a phone, computer, website or network.

The best method to avoid having a password hacked is by using long and complex passwords. There are various schools of thought about what constitutes a strong or less-hackable password, but as a general rule, the longer and more complex the password, the less likely it will be cracked. In addition, mobile devices should also have a PIN, pass code or password. The devices

should lock/time out after a short period of time and require users to re-enter the PIN code or password.

5. Assure that Video Conferences are Secure

One method of communicating that has become more common is the use of videoconferencing (or video-teleconferencing) technology, which allows users to hold face-to-face meetings from different locations. For many law offices, the use of videoconferences has replaced traditional teleconferences, which did not have the video component.

As the popularity of videoconferencing has increased, so have the number of reported instances in which hackers hijack videoconferences. These incidents were of such concern that on March 30, 2020 the FBI issued a warning about teleconference hijacking during the COVID-19 pandemic⁵ and recommended that users take the following steps “to mitigate teleconference hijacking threats:”

- Do not make meetings public;
- Require a meeting password or use other features that control the admittance of guests;
- Do not share a link to a teleconference on an unrestricted publicly available social media post;
- Provide the meeting link directly to specific people;
- Manage screensharing options. For example, many of these services allow the host to change screensharing to “Host Only;”
- Ensure users are using the updated version of remote access/meeting applications.

6. Backup Any Data Stored Remotely

Backups are as important at home as they are at the office, perhaps more so because office systems are almost always backed up in an automated fashion. Thus, attorneys and staff working remotely should either work remotely on the office’s system (using services such as Windows Remote Desktop Connection, GoToMyPC or LogMeIn) or have a system in place that assures that there is a backup for all documents and other computer files created by attorneys and staff while working. Often, backup systems can include offsite locations. Alternatively, there are numerous providers that offer secure and easy-to-set-up cloud-based backup services.

7. Security is Essential for Remote Locations and Devices

Attorneys and staff must make reasonable efforts to assure that work product and confidential client information are confidential, regardless of where or how they are created. Microsoft has published its guidelines for a secure home office, which include:

⁵ <https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic>. Although the FBI warning related to Zoom, one brand of videoconferencing technology, the recommendations apply to any such service.

- Use a firewall;
- Keep all software up to date;
- Use antivirus software and keep it current;
- Use anti-malware software and keep it current;
- Do not open suspicious attachments or click unusual links in messages, email, tweets, posts, online ads;
- Avoid visiting websites that offer potentially illicit content;
- Do not use USBs, flash drives or other external devices unless you own them, or they are provided by a trusted source. When appropriate, attorneys should take reasonable precautions such as calling or contacting the sending or supplying party directly to assure the data are not infected or otherwise corrupted.⁶

8. Users Should Verify That Websites Have Enhanced Security

Attorneys and staff should be aware of and, whenever possible, only access websites that have enhanced security. The web address in the web browser window for such sites will begin with “HTTPS” rather than “HTTP.” A website with the HTTPS web address uses the SSL/TLS protocol to encrypt communications so that hackers cannot steal data. The use of SSL/TLS security also confirms that a website’s server (the computer that stores the website) is who it says it is, preventing users from logging into a site that is impersonating the real site.

9. Lawyers Should Be Cognizant of Their Obligation to Act with Civility

In 2000, the Pennsylvania Supreme Court adopted the Code of Civility, which applies to all judges and lawyers in Pennsylvania.⁷ The Code is intended to remind lawyers of their obligation to treat the courts and their adversaries with courtesy and respect. During crises, the importance of the Code of Civility, and the need to comply with it, are of paramount importance.

During the COVID-19 pandemic, the Los Angeles County Bar Association Professional Responsibility and Ethics Committee issued a statement, which this Opinion adopts, including:

In light of the unprecedented risks associated with the novel Coronavirus, we urge all lawyers to liberally exercise every professional courtesy and/or discretionary authority vested in them to avoid placing parties, counsel, witnesses, judges or court personnel under undue or avoidable stresses, or health risk. Accordingly, we remind lawyers that the Guidelines for Civility in Litigation ... require that lawyers grant reasonable requests for extensions and other accommodations.

Given the current circumstances, attorneys should be prepared to agree to reasonable extensions and continuances as may be necessary or advisable to avoid in-person meetings, hearings or deposition obligations. Consistent with California

⁶ <https://support.microsoft.com/en-us/help/4092060/windows-keep-your-computer-secure-at-home>

⁷ Title 204, Ch. 99 adopted Dec. 6, 2000, amended April 21, 2005, effective May 7, 2005.

Rule of Professional Conduct 1.2(a), lawyers should also consult with their clients to seek authorization to extend such extensions or to stipulate to continuances in instances where the clients' authorization or consent may be required.

While we expect further guidance from the court system will be forthcoming, lawyers must do their best to help mitigate stress and health risk to litigants, counsel and court personnel. Any sharp practices that increase risk or which seek to take advantage of the current health crisis must be avoided in every instance.

This Opinion agrees with the Los Angeles County Bar Association's statement and urges lawyers to comply with Pennsylvania's Code of Civility, and not take unfair advantage of any public health and safety crises.

IV. Conclusion

The COVID-19 pandemic has caused unprecedented disruption for attorneys and law firms, and has renewed the focus on what constitutes competent legal representation during a time when attorneys do not have access to their physical offices. In particular, working from home has become the new normal, forcing law offices to transform themselves into a remote workforce overnight. As a result, attorneys must be particularly cognizant of how they and their staff work remotely, how they access data, and how they prevent computer viruses and other cybersecurity risks.

In addition, lawyers working remotely must consider the security and confidentiality of their procedures and systems. This obligation includes protecting computer systems and physical files, and ensuring that the confidentiality of client telephone and other conversations and communications remain protected.

Although the pandemic created an unprecedented situation, the guidance provided applies equally to attorneys or persons performing client legal work on behalf of attorneys when the work is performed at home or at other locations outside of their physical offices, including when performed at virtual law offices.

CAVEAT: THE FOREGOING OPINION IS ADVISORY ONLY AND IS NOT BINDING ON THE DISCIPLINARY BOARD OF THE SUPREME COURT OF PENNSYLVANIA OR ANY COURT. THIS OPINION CARRIES ONLY SUCH WEIGHT AS AN APPROPRIATE REVIEWING AUTHORITY MAY CHOOSE TO GIVE IT.

What Will It Take to Finally Get Lawyers Into the Tech Age?

[LAW law.com/thelegalintelligencer/2019/02/21/what-will-it-take-to-finally-get-lawyers-into-the-tech-age](https://www.law.com/thelegalintelligencer/2019/02/21/what-will-it-take-to-finally-get-lawyers-into-the-tech-age)

By Daniel J. Siegel | February 21, 2019 at 02:32 PM

Daniel J. Siegel.



Kicking and screaming. That's how many lawyers have proceeded into the age of technology. They know it's here, they know they should use it, they understand—but may not admit—that it makes them more efficient. But in the end, it seems that many lawyers are only adopting technology because they must. Not because they should.

Two recent studies confirm this trend. The first is the American Bar Association 2018 Legal Technology Survey Report, particularly Volume II, the "Law Office Technology" report. The second are two recent reports by Malwarebytes, one on the state of malware, the other on how little most people know about tracking.

Let's start with the ABA report, which is issued annually by the Law Practice Division's Legal Technology Resource Center. The report, which focuses exclusively on lawyers, shows that lawyers, particularly those practicing as solos or in small firms, tend to adopt technology in three ways. The first is that they "must." The second is that their practices "need" the technology. Finally, the third is that they "want" the technology.

Let's look at each of my categories. The "must" category is exemplified by PDFs and metadata. Because courts and other entities require lawyers to file documents, pleadings and other items electronically, lawyers must use PDF creation products such as Adobe Acrobat. On the other hand, there is metadata software. Although numerous bar association committees, including the Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility, have opined that lawyers have an ethical obligation to remove such data from files they produce to other attorneys, lawyers are not required to do so.

As a result, the survey reports that 96.6 percent of all lawyers responding have PDF creation software available at their firms, including 92.8 percent of solos, 97.2 percent of lawyers in firms with two to nine lawyers, 98.6 percent of lawyers in firms with 10 to 49 lawyers, and in 100 percent of lawyers in firms with 50 or more lawyers. Compare this with metadata software, which could reveal confidential client communications. The difference is staggering. Only 37 percent of solos have metadata analysis and removal software available, 41.1 percent of lawyers in firms with two to nine lawyers, 65.2 percent of lawyers in firms with 10 to 49 lawyers, 84.8 percent of lawyers in firms with 50 to 99 lawyers, and 97.2 percent of lawyers in firms with more than 100 lawyers use it. In addition, when I lecture about metadata software, it is always remarkable how many lawyers remain ignorant about it.

On the other hand, there are products law firms "need," but do not have to have to function. Two examples are case/matter management software and specialized practice software. Case or matter management software provide individual and firmwide calendars, individual case listings, document management and other features, all of which save attorneys significant time in handling their files. Specialized software is designed for a specific practice area, such as bankruptcy, real estate closing or estate administration.

The study revealed that the larger the firm, the greater likelihood such products were in use. Thus, only 30.8 percent of solos and 57.1 percent of lawyers in firms with two to nine attorneys had case management software available, whereas 68.1 percent of lawyers in firms with 100 to 499 lawyers, and 71.9 percent of lawyers in firms with more than 500 lawyers did. Similarly, only 23.4 percent of solos and 36.21 percent of lawyers in firms with two to nine attorneys had specialized practice-specific software available, whereas 52.2 percent of lawyers in firms with 100 to 499 lawyers, and 47.3 percent of lawyers in firms with more than 500 lawyers did.

Finally, we have the "want" category, software that is helpful but not necessary. This category includes software such as customer relationship manager products (CRM), designed to maintain relationships with clients and referral sources, etc. One would think that such software would be extremely valuable in smaller firms because so many such practices are dependent on the strength and length of these relationships. Despite this, only 23.1 percent of solos and 41.1 percent of lawyers in firms with two to nine attorneys had the software available, whereas 72.7 percent of lawyers in firms with 100 to 499 lawyers, and 68.9 percent of lawyers in firms with more than 500 lawyers had it.

Moving on to the reports from Malwarebytes Labs, the company that sells Malwarebytes, one of the leading malware removal productions. In the company's "State of Malware," it explained that in 2018 saw the advent of "information stealers ... variants of malware [that] focused their energies on ensnaring businesses, gleaning the most profit from ultra-sensitive data that could be sold on the black market for re-targeting in future campaigns." What types of data were these cyberthieves seeking? Personal data such as Social Security numbers, credit card information and information that could be used to steal a person's identity, that is, the type of data that law firms often retain about clients and opposing parties.

Lawyers have an ethical obligation, however, to understand the risks and benefits of technology. This obligation also includes a duty to protect confidential client data and sensitive information. Because every law firm uses the Internet in some way, whether to access email or to store information in the cloud, the risks cited in the Malwarebytes report are real, and lawyers must be vigilant to protect their data. This includes installing the proper onsite protection, vetting offsite/cloud vendors, and perhaps purchasing cyberinsurance to provide additional protection in the event of an attack.

Similarly, in the January 29, 2019 report, "What does 'consent to tracking' really mean?" Malwarebytes opens many eyes to the dangers of simply clicking yes when a user is asked to consent to some form of tracking as a condition of using a web-based service. The report explains that "Most platforms that engage in user tracking do so in ways that raise concern, but are not overtly alarming." The report explained, however, that another potential harm "is the use of tracking tags on sensitive websites. ... User tracking has progressed so far in sophistication that an average user most likely does not have the background necessary to imagine every possible use case for data collection prior to accepting a user agreement." In short, companies may be tracking far more than names, birthdays, trends in the hashtags we use, and our locations. Doing so raises privacy concerns, as well as concerns when third parties track an attorney's client-related online activities.

Everyone prefers to use the information and tools they are comfortable with. For lawyers, the ever-expanding world of technology presents benefits—such as case management software—and dangers, such as the risk of a ransomware attack that holds a law firm's data hostage until a ransom is paid. What recent studies confirm, however, is that lawyers do not take enough advantage of the tools that will help them, while also ignoring the ones that could render them subject to the whims of a cybercriminal.

Daniel J. Siegel, *principal of the Law Offices of Daniel J. Siegel, provides ethical guidance and Disciplinary Board representation for attorneys and law firms; he is the editor of "Fee Agreements in Pennsylvania (6th Edition)" and author of "Leaving a Law Practice: Practical and Ethical Issues for Lawyers and Law Firms (Second Edition)," published by the Pennsylvania Bar Institute. Contact him at dan@danielsiegel.com.*

Is 2019 the Year Lawyers Finally Learn Their Lesson About Technology?

law.com/thelegalintelligencer/2019/01/03/is-2019-the-year-lawyers-finally-learn-their-lesson-about-technology

By Daniel J. Siegel | January 03, 2019 at 01:26 PM

Daniel J. Siegel.



Lawyers, as a group, just don't seem to "get it." Some do, others try, but many lawyers still seem oblivious to the ever-changing swirls of ethics and technology that apply to our profession. Based on the feedback from this column, I can only conclude that many lawyers still do not recognize, or do not want to recognize, the extent to which technology and ethics intersect every aspect of their lives (both professional and personal), and how their failure to address these issues can impact their clients and their practices.

With that in mind, here's my top-eight wish list of techno-ethics matters for which I hope lawyers will finally "get religion" in 2019.

Metadata

Recently, I received a document from opposing counsel containing a draft of a proposed agreement. Sent in Microsoft Word format, the agreement seemed reasonable, but I wondered if it would be beneficial to add some additional language more favorable to my client. Finding that language was easy; in fact, opposing counsel provided it to me.

How? He had failed to scrub the document of metadata, that is, "information about data" contained in electronic materials not ordinarily visible to those viewing the information. Most commonly found in documents created in Microsoft Word, metadata is also present in other formats, including spreadsheets, PowerPoint presentations and Corel WordPerfect documents.

Although metadata generally contains seemingly harmless information such as spelling or punctuation changes, it may also contain privileged and confidential information, such as previously deleted text, notes and tracked changes, which may provide information about legal

issues, legal theories and other information presumably not intended to be disclosed to opposing counsel.

In this instance, I opened my metadata scrubber software, told it to analyze the document and—voila—I could review information removed by opposing counsel from the version of the document visible to him when he sent the document.

The issue of metadata isn't new. 2019 marks one decade since the Pennsylvania Bar Committee on Legal Ethics and Professional Responsibility issued Formal Opinion 2009-100, which concluded that an attorney sending electronic documents that may contain metadata has a duty of reasonable care to remove unwanted metadata before sending them to another party or counsel. While the opinion states that an attorney receiving a document with metadata should disclose the information if he believes the disclosure was inadvertent, the time has long since passed for the "inadvertent defense" to be viable.

Although 2009 was a long time ago. It was the year Michael Jackson died, the top movie was "Harry Potter and the Half-Blood Prince," and President Barack Obama was beginning his first term. The ensuing 10 years were certainly sufficient time for lawyers to learn about their ethical obligation to remove metadata from electronically transmitted documents.

Social Media—Privacy and Ignorance

Social media is "social," which means that its goal is to share information, ideas, messages, photos and lots of personal information. As a result, clients use social media, including everyone from corporations to individuals. Social media is also rife with information that can serve as ammunition for a well-armed opponent in litigation of all types, not just the personal injury cases that receive most of the publicity.

Despite the realities that would be part of a Social Media 101 class, many lawyers claim that because they don't use social media, and "never will," they do not have to address it in their practices. This is akin to saying that a doctor doesn't have to know the latest medical techniques

because they weren't invented when she was in medical school. Plus, lawyers forget that even if they are not using social media, clients and others can leave reviews of the attorneys, many of which are less than flattering.

As a result, lawyers need to recognize the importance of discussing social media with clients, and then confirming that discussion in the fee agreements and engagement letters. They also need to recognize that social media is a potential source of information in all types of matters, and take steps to either learn how to mine it, or to have staff who can.

In addition, lawyers must be mindful that even if a client believes their social media accounts are "private," if such a setting is really possible, their accounts and their personal information are far more public than they want to admit. Just read the front page of the New York Times, which reported on Dec. 19, that "Facebook Offered Users Privacy Wall, Then Let Tech Giants Around It."

Law Firms Can Survive Without Technology

It is not uncommon to hear lawyers, particularly more "seasoned" ones, lament that they miss the days when secretaries took shorthand, and the arrival of the mailman was the highlight of the day. Those days are long gone. And they are not coming back, nor are other relics like carbon paper, onionskin paper, or IBM Selectric typewriters, which were discontinued in 1986.

Instead, we now have smartphones, that is, cellphones more technologically advanced than the Apollo rocket. In fact, you can read the surprisingly entertaining code for the Apollo rocket <https://github.com/chrislgarry/Apollo-11>.

Law firms must recognize that they too must advance and understand technology, not just for ethical reasons. Yes, as discussed elsewhere in this column, state Supreme Courts are now including technological competence as a component of the Rules of Professional Conduct, and some states are mandating that lawyers take technology-focused CLEs as part of their CLE requirements. But more importantly, technology improves the delivery of client services, allowing lawyers and staff to accomplish more in less time.

Despite what some naysayers preach, technology need not replace the personal touch. My office uses cutting edge technology from client intake to document assembly to matter management and for trial, yet clients meet with us at an old mahogany conference table in an old home that was converted into office space, where we take notes on paper. Why? The technology we use enables our office to complete its work more efficiently but does not convert our client interaction into an impersonal experience.

Email Privacy

Email is one of the least private forms of communication, a fact evidenced by the repeated headlines highlighting the email hacking of the rich and famous. As nolo.com explains, "Email might feel like a private, one-to-one conversation safe from prying eyes, but email is about as

confidential as whispering at the White House. Your messages can be intercepted and read anywhere in transit, or reconstructed and read off of backup devices, for a potentially infinite period of time.”

Yet lawyers continue to attach confidential and sensitive information to emails, never considering how easily the information can get into the wrong hands. The American Bar Association warned attorneys in 2017 in Formal Opinion 477r (“Securing Communication of Protected Client Information”) that “a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.” In other words, lawyers should not attach confidential and sensitive information to emails unless they take reasonable steps, such as encrypting the data (for example, password-protecting the file).

This common-sense advice is lost on many attorneys. Would they leave confidential information in their office lobby or allow anyone to rummage through the cabinets housing their clients’ files? Of course not, yet they seem unconcerned with the disclosure of information in email.

The duty to protect confidential information is highlighted by the Pennsylvania Supreme Court’s implementation in 2018 of a Public Access Policy, which requires attorneys and litigants to redact confidential information from court filings and to file confidential documents separately so that the public, that is, the “nosy neighbor” and others, cannot view information, such as tax returns, Social Security numbers, and medical records in court-filed documents.

Carbon Copies

So, do you know the difference between a carbon copy and a blind carbon copy (bcc) of an email? Do you know that a person who receives a blind carbon copy can “Reply to All” and that the reply is sent to everyone who was emailed or copied on the prior email?

Apparently, many lawyers and their support staff do not know this presumably basic piece of email procedure. Recently, there has been a surge in situations where persons who were blind carbon-copied replied to all, arguably waiving attorney-client privilege, and potentially disclosing their email address and other information to opposing counsel. As a result, state ethics committees are drafting opinions focused on whether it is permissible to carbon copy or bcc a client on email with opposing counsel, and if so, does such action waive confidentiality?

It seems that this problem can be eliminated if lawyers and staff would receive basic email training. (See Item 10.)

Advertising

The American Bar Association has adopted a revision to the Model Rules of Professional Conduct that would eliminate most of the ethics rules relating to advertising. Under the proposal approved by the House of Delegates in 2018, Model Rule 7.1 (“Communications Concerning a Lawyer’s Services”) would state: “A lawyer shall not make a false or misleading communication about the lawyer or the lawyer’s services. A communication is false or misleading if it contains a material misrepresentation of fact or law, or omits a fact necessary to make the statement considered as a whole not materially misleading.”

Although the Pennsylvania Supreme Court has not adopted this proposed revision, or changes to other advertising rules, it is time for the court to recognize that Disciplinary Counsel will not enforce any ethics rules about advertising. Consequently, the court should decide whether it should adopt this revision with the knowledge that, as with the current rules, not one lawyer is likely to be disciplined for a violation, or eliminate all such rules.

Training

It has been nearly six years since the Pennsylvania Supreme Court amended the Comment to Rule of Professional 1.1 to clarify that “competence” includes understanding “the benefits and risks associated with relevant technology.” While this comment often is considered in light of cybersecurity dangers, the court did not limit it in scope. Lawyers must take 12 hours of continuing legal education courses annually, for example. They must also use technology in every practice regardless of age, practice area, etc. Yet many know little or nothing about how to use basic technology such as Microsoft Outlook or Adobe Acrobat or other programs used in most law firms. Worse yet, they don’t require that their staff learn how to use the tools essential to performing their daily activities.

In December 2018, North Carolina became the second state to require lawyers to take a CLE in technology, mandating one hour per year of CLE devoted to technology training. A recommendation for a similar provision is currently pending before the Pennsylvania Supreme Court. The North Carolina Supreme Court defined “technology training” as “a program, or a segment of a program, devoted to education on information technology (IT) or cybersecurity ... including education on an information technology product, device, platform, application or other tool, process, or methodology.” Hopefully, the Pennsylvania Supreme Court will follow suit.

Cybersecurity

Law firms, like other businesses, are targets and victims of hacking. Our files contain the types of sensitive information that cybercriminals covet. In addition, there has been a recent increase in “spear phishing” attacks, in which emails are sent to clients, which look exactly like the ones they receive from their attorneys, instructing them to wire funds for payment of taxes, fees, etc., except that the emails are bogus and those who follow the instructions will be transferring their money to generally untrackable criminals.

The technology that drives law firms and other businesses can be vulnerable, and lawyers must take reasonable precautions to protect office technology and the mobile technology that we often take for granted. One common vulnerable situation is the type of free Wi-Fi available at many businesses. Norton, one of the world's most respected security software companies, notes that users of free Wi-Fi are particularly at risk for man-in-the-middle attacks (where a hacker accesses the information you send over the internet from one device to another location), malware (software that exploits holes or weaknesses in your devices) and more.

To avoid these and other dangers, Norton recommends using a virtual private network (VPN), which secures your connections. VPN programs are inexpensive, work seamlessly in most circumstances, and eliminate the risks of public Wi-Fi.

Cybersecurity is a danger for every law firm. Hopefully, in 2019, more attorneys will recognize and prepare to prevent the risks inherent to technology.

These items are just a few of the techno-ethical areas where lawyers can improve their delivery of services and reduce the risks attendant with technology, while also assuring that confidential and sensitive information stays that way.

Daniel J. Siegel, *principal of the Law Offices of Daniel J. Siegel, provides ethical guidance and Disciplinary Board representation for attorneys and law firms; he is the editor of "Fee Agreements in Pennsylvania (6th Edition)" and author of "Leaving a Law Practice: Practical and Ethical Issues for Lawyers and Law Firms (Second Edition)," published by the Pennsylvania Bar Institute. He can be reached at dan@danieljsiegel.com.*

The Legal Intelligencer

Page printed from: <https://www.law.com/thelegalintelligencer/2018/06/28/laffaire-colangelo-and-its-lessons-for-attorneys-and-staff-part-i/>

'L'Affaire Colangelo' and Its Lessons for Attorneys and Staff (Part I)

As a college student, I dreamed of becoming a sportswriter, a career that would serve as a diversion from the daily stress of the news. Eventually, I settled on law as a profession, and discovered that the world of sports rarely intersects with the world of law.

By **Daniel J. Siegel** | June 28, 2018



Daniel J. Siegel.

As a college student, I dreamed of becoming a sportswriter, a career that would serve as a diversion from the daily stress of the news. Eventually, I settled on law as a profession, and discovered that the world of sports rarely intersects with the world of law. There remain times, however, when sports intrude into the legal arena and offer valuable lessons for attorneys.

None perhaps more than what I call “L’Affaire Colangelo,” the recent social media-based soap opera involving Bryan Colangelo, who is now the former-president of Basketball Operations for the Philadelphia 76ers

professional basketball team. Colangelo's story offers many lessons for attorneys, none more important than its reminder that lawyers and their staff should never share confidential client information with family members or others because such "unguarded talk" can lead to serious consequences, often very serious consequences.

For those who aren't aware, Colangelo and the team mutually agreed to part ways after a website discovered five Twitter accounts linked to him, or so it seemed. The accounts defended Colangelo's actions, but also did far more. Therein lie the lessons for lawyers and their staffs.

The Twitter accounts disclosed confidential information about the team and specific players, including information unavailable to the public or other teams, that is, the 76ers' competition. In addition, the Twitter accounts disclosed confidential medical information about players on the teams, information that was also unavailable to the public or other teams, that is, the 76ers' competition.

Colangelo claimed to be aware of one of the accounts, but insisted that he knew nothing about the other four, which were the accounts that revealed the sensitive and confidential information. He had a difficult time explaining how all five accounts were de-activated (removed from public view) within minutes after the website called the team and reported that it was aware of two of the accounts and their presumed connection with Colangelo.

After the call, the website released its story, highlighting the Twitter accounts and its revelations. From there, the story became a media circus. The team, of course, hired a law firm to investigate the allegations. And every sportswriter and column in the world, or so it seemed, was investigating the story and offering their opinions on how the team should handle the scandal.

Eventually, the team and Colangelo parted ways. Accompanying that announcement was a statement from Colangelo that said, "While I am grateful that the independent investigation conducted by the 76ers has confirmed that I had no knowledge or involvement in the Twitter activity conducted by my wife, I vigorously dispute the allegation that my conduct was in any way reckless. At no point did I ever purposefully or directly share any sensitive, non-public, club related information with her."

Although he termed his wife's actions "a seriously misguided effort to publicly defend and support me," Colangelo never explained how his wife obtained the information if she didn't learn it from

her husband.

L'Affaire Colangelo offers many lessons for lawyers because, like Bryan Colangelo, lawyers are privy to confidential and sensitive information about their clients, information that they may not disclose without violating the Rules of Professional Conduct.

Consider some examples. It could be a criminal lawyer who reveals to his wife that his client admitted committing the crime for which he was charged. As it turns out, the lawyer's wife was planning to divorce her spouse and, as part of her revenge upon him, she tells all her Facebook friends about the criminal's admission of guilt. Or it could be a lawyer who tells her children all about a client's sensitive medical information, only to discover that one of her daughters is friends with the client's daughter, and reveals that information to the girl. Or it could be a lawyer representing a major corporation that is trying to purchase a competitor, who boasts to his family about the enormous potential deal, only to see his son brag about his dad's big deal on Facebook, and therefore to the world. It could also be a staff member trying to impress a friend.

In each example, a lawyer or staff member revealed confidential information to a person not entitled to know about it. Regardless of the situation, the person revealed confidential information whose disclosure could prejudice a client, and whose disclosure violated Rule of Professional Conduct 1.6(a), which prohibits a lawyer from "revealing information relating to representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation." The rules also require a lawyer to assure that their staff also preserve confidential information.

Comment 2 to Rule 1.6(a) explains that "A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation. ... This contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct. Almost without exception, clients come to lawyers in order to determine their rights and what is, in the complex of laws and regulations, deemed to be legal and correct. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is upheld."

Some lawyers and their employees, like everyone else, like to talk, or perhaps brag, about their firms' clients, their influence, or their presumed importance; revealing interesting tidbits is one way to do so, albeit one that can place them in disciplinary hot water. But seemingly innocent revelations are not so innocent when they include confidential information.

That may well be what happened to Colangelo. His tenure in Philadelphia was filled with controversy, and he was not universally liked. It's possible that he had frustrating days dealing with players and their agents, or was upset about his players' injuries, and needed to vent. By including sensitive information with his comments, Colangelo may have revealed confidential team information as well as HIPAA-protected information about players.

Even if, as Colangelo claims, his wife was tweeting just to protect her husband, the only likely source of her information had to be her husband, whose poor judgment not only cost him his job, but also endangered relationships between the players and team management. If Colangelo were a lawyer, such revelations would likely signal the end of the attorney-client relationship and the beginning of a legal malpractice claim and possibly Disciplinary Board proceedings.

Breaches of confidentiality come in many forms, from table talk, to publication on the internet. In *Office of Disciplinary Counsel v. Wrona*, in his first case as primary attorney, attorney Eugene Wrona made untruthful statements in pleadings; he also wrote a letter to the editor of the major newspaper in the area, wrote a press release and posted it on the Internet, and breached confidentiality requirements regarding action before the Judicial Conduct Board. Because of these actions, the Pennsylvania Supreme Court disbarred him.

Colangelo's fate was sealed when his wife decided to "defend" her husband on the internet, without ever realizing that nothing is truly anonymous online. While the accounts were anonymous, the tipster who revealed the story told the website that revealed it that he used a data analysis tool to link the five "anonymous" Twitter accounts. The tipster noticed that the accounts at times revealed proprietary information that would have been available only to a small number of high-ranking 76ers officials. From there, the website and others connected the dots, which eventually led to Barbara Bottini and her husband's demise.

Lawyers have an obligation to protect confidential information. That means that they cannot discuss the information with family, friends or anyone outside their firms without client consent. Otherwise, they may find themselves in a fate like Colangelo's.

Sports are often used as metaphors for life. They also offer lessons about what lawyers and their staff must never do.

Daniel J. Siegel, *principal of the Law Offices of Daniel J. Siegel, provides ethical guidance and Disciplinary Board representation for attorneys and law firms; he is the editor of “Fee Agreements in Pennsylvania” (6th Edition) and author of “Leaving a Law Practice: Practical and Ethical Issues for Lawyers and Law Firms” (Second Edition), published by the Pennsylvania Bar Institute. Contact him at dan@danieljsiegel.com.*

L’Affaire Colangelo and Its Lessons for Attorneys (Part II)

law.com/thelegalintelligencer/2018/10/25/laffaire-colangelo-and-its-lessons-for-attorneys-part-ii

By Daniel J. Siegel | October 25, 2018 at 12:17 PM

Daniel J. Siegel.



When I first wrote about “L’Affaire Colangelo,” the social media-based soap opera involving Bryan Colangelo, former-Philadelphia 76ers president of basketball operations, my focus was on its lesson: that lawyers and their staff should never share confidential client information with family members or others. Otherwise, such “unguarded talk” could lead to very serious consequences, as Colangelo’s demise confirmed.

But as I said then, there were other lessons for attorneys in Colangelo’s rapid fall. These lessons become clear when you consider some of Colangelo’s quotes in response to the revelations that five Twitter accounts linked to him had disclosed sensitive or confidential

information about his team and its players.

- *“Like many of my colleagues ... I have used social media as a means to keep up with the news.”*
- *“I have never posted anything whatsoever on social media.”*
- *“I vigorously dispute ... that my conduct was in any way reckless.”*
- *“At no point did I ever purposely or directly share any sensitive, nonpublic ... information.”*

I removed all basketball- or team-related references from Colangelo’s quotes to permit you to consider his comments in the context of the many lawyers who assert that they know little, or know nothing—about social media—and believe that you do not have to know or learn anything about social media. ‘Au contraire.

Lawyers cannot use ignorance as a defense to social media missteps because ignorance is merely another word for incompetence, and lawyers must be competent in their professional actions. That’s why the American Bar Association amended Comment 6 Model Rule of Professional Conduct 1.1 in 2012 to explain that “competence” means that “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.” Pennsylvania adopted this amendment in 2013.

Designed to help attorneys practicing in PA, NJ and DW keep up with the changing rules and technologies in eDiscovery; special attention given to emerging eDiscovery issues.

[Get More Information](#)

Many lawyers shrugged at this rules change, and continued to ignore discussions about social media and its implications for clients—and for them. After all, they reasoned, if they don't use social media, or simply don't use much technology, they aren't in any danger.

But if Colangelo's saga demonstrated anything, it's that anyone, including lawyers, can get into a lot of trouble—perhaps lose their job—despite claiming technological ignorance as a defense.

As social media takes over more nuances of our lives, it is easier than ever for lawyers, and judges, to get into that kind of trouble.

Consider Jefferson County, Kentucky District Court Judge Sandra McLaughlin, who shared a news story on Facebook about a Jefferson County district court case, commenting that “This murder suspect was RELEASED FROM JAIL just hours after killing a man and confessing to police.” Those comments led to a public reprimand for the Judge.

Or consider attorney Aaron Schlossberg, who ranted about Spanish-speaking employees at a New York restaurant. Schlossberg never thought that another customer would film his rant and post it on Twitter, where it, quite predictably, went viral. While Schlossberg has not been publicly disciplined for his comments, his conduct has had an enormous impact on his reputation, as Google confirms.

First, when you perform a Google search for “attorney Aaron Schlossberg,” you will discover pages of results, the vast majority focusing on his comments, not on his professional skills or successes. Then look at Schlossberg's Facebook page, which appears prominently in the results. Schlossberg now has a 1.1 rating based on the opinions of 2,367 people. It is a safe guess that most of those opinions are based on Schlossberg's tirade, and are not clients or others who personally know him.

While McLaughlin's and Schlossberg's conduct have garnered broad attention, most attorneys' Colangelo-like failings are less newsworthy. While there are many ways lawyers' social media ignorance surfaces, there are four primary traps for the unwary:

- Believing in the myth of privacy;
- Forgetting that the Rules of Professional Conduct apply to social media;
- Misusing or failing to use social media as a discovery or investigatory tool; and
- Failing to counsel clients about their use of social media.

The myth of privacy—this is the idea that social media accounts are private, cannot easily be discovered or that no one except perhaps “friends” will ever know what we say online. In other words, it is the erroneous belief that when you are in a zone of privacy when you write a blog post or share your views on Facebook. That is simply not the case. There is a reason “social” is social media’s first name.

An example of this myth of privacy is former public defender Anya Cintron Stern, who learned about it in 2012 when she wrote a Facebook post that included a photo of the leopard print underwear her client’s family gave him to wear at his murder trial. Although her Facebook page was “private,” someone who saw the post informed the trial judge, who declared a mistrial.

Second, there are countless other examples of lawyers who do not realize that the Rules of Professional Conduct apply to their social media activity. Despite their ignorance, these attorneys should consider the Pennsylvania Bar Association committee on legal ethics and professional responsibility’s Formal Opinion 2014-300 (“Ethical Obligations for Attorneys Using Social Media”), which concluded:

- Attorneys may advise clients about the content of their social networking websites, including the removal or addition of information.
- Attorneys may connect with clients and former clients.
- Attorneys may not contact a represented person through social networking websites.
- Although attorneys may contact an unrepresented person through social networking websites, they may not use a pretextual basis for viewing otherwise private information on social networking websites.
- Attorneys may use information on social networking websites in a dispute.
- Attorneys may accept client reviews but must monitor those reviews for accuracy.
- Attorneys may generally comment or respond to reviews or endorsements, and may solicit such endorsements.
- Attorneys may generally endorse other attorneys on social networking websites.
- Attorneys may review a juror’s internet presence.
- Attorneys may connect with judges on social networking websites provided the purpose is not to influence the judge in carrying out his official duties.

This opinion provides an excellent analysis of the issues surrounding attorneys’ and clients’ use of social media, along with advice about how attorneys should address social media in an ethically compliant manner.

Third, attorneys often do not realize that the discovery of social media is a tool that they should use, or consider using, in every case, regardless whether they represent a plaintiff or defendant,

or a person or a corporation. While most news reports focus on how plaintiffs reveal damaging information on social media, or how criminals post information that helps lead to their arrest, corporations also misuse social media. Like individuals, corporations at times post information not intended to be public, or that can be damaging in future litigation. As a result, every attorney should research every opponent's social media, including blogs, Facebook, LinkedIn, Instagram and YouTube.

Finally, lawyers must counsel clients about their social media use, and the implications of their activities. Lawyers have always counseled clients not to discuss their cases with others, and not to destroy physical evidence. The advent of social media merely transforms that obligation to the electronic/online world.

Lawyers must advise clients to avoid posting information online that could impact their cases. Similarly, just like clients may not destroy physical evidence, so too must they not destroy electronic evidence. In that regard, the fact that the information is electronic is irrelevant, the advice remains the same.

Lawyers have always had an obligation to protect confidential information. The advent of social media means that they must heed that advice in a different forum. Otherwise, they may find themselves suffering a fate like Colangelo's.

L'Affaire Colangelo confirms that sports are not only a metaphor for life, they also offers lessons about what lawyers must never do.

Daniel J. Siegel, *principal of the Law Offices of Daniel J. Siegel, provides ethical guidance and Disciplinary Board representation for attorneys and law firms; he is the editor of "Fee Agreements in Pennsylvania" (6th Edition) and author of "Leaving a Law Practice: Practical and Ethical Issues for Lawyers and Law Firms" (Second Edition), published by the Pennsylvania Bar Institute. Contact him at dan@danieljsiegel.com.*