



Attorney Conduct: Future-Focused Ethics

Sponsored by the Cincinnati Bar Association Professionalism Committee

Tuesday, November 13, 2018



Attorney Conduct: Future-Focused Ethics

November 13, 2018

Agenda

- 9 a.m. Ethics and Technology: Where the Rubber Meets the Road TAB A**
Gregory L. Adams, Esq., *Croswell & Adams Co. LPA*
Phyllis G. Bossin, Esq., *Phyllis G. Bossin & Associates*
Melissa Thompson-Millard, Esq., *Barbara J. Howard Co. LPA*
- 9:45 a.m. Social Media: Common Sense and Caution TAB B**
Brian R. Redden, Esq. and Brett Renzenbrink, Esq.,
Buechner Haffer Meyers & Koenig Co. LPA
- 10:15 a.m. Break**
- 10:30 a.m. Ethics and Professionalism Panel Discussion**
Moderator:
Carolyn Taggart, Esq., *Porter Wright Morris & Arthur LLP*

Panelists:
Gregory L. Adams, Esq., *Croswell & Adams Co. LPA*
Phyllis G. Bossin, Esq., *Phyllis G. Bossin & Associates*
Melissa Thompson-Millard, Esq., *Barbara J. Howard Co. LPA*
Brian R. Redden, Esq. and Brett Renzenbrink, Esq.,
Buechner Haffer Meyers & Koenig Co. LPA
- 11:15 a.m. Substance Abuse and Mental Health Issues TAB C**
Patrick Garry, Esq., *OLAP*
- 11:45 a.m. Adjourn**

Faculty Bios

TAB D

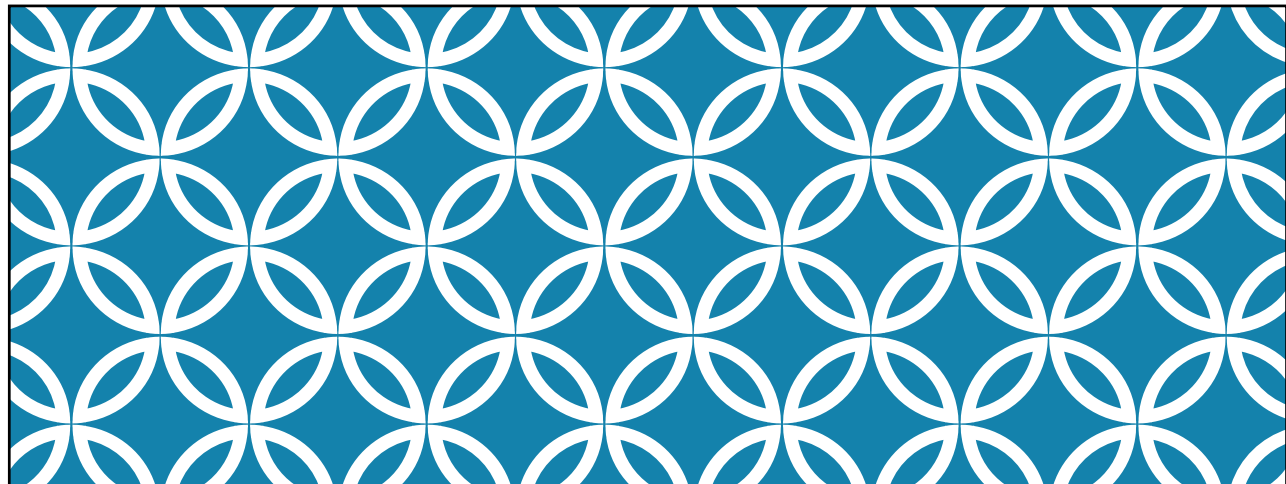


CBA WiFi Network: cbawireless
CBA WiFi Password: cba3818213

TAB A



Cincinnati Bar
ASSOCIATION



ETHICS AND TECHNOLOGY: WHERE THE RUBBER MEETS THE ROAD

Gregory L. Adams, Esq.
Phyllis G. Bossin, Esq.
Melissa Thompson Millard, Esq.

WHY SHOULD YOU CARE?

Effective 4/1/2015, the Ohio Supreme Court adopted amendments to the Rules of Professional Conduct concerning technology and confidentiality.

We now have an explicit ethical obligation to understand the risks and benefits of technology in our practices.

Malpractice liability?

RULE 1.1 COMPETENCE

Rule 1.1 Competence: “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation *reasonably* necessary for the representation.

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

RULE 1.6 — CONFIDENTIALITY OF INFORMATION

Rule 1.6(c): “A lawyer shall make *reasonable* efforts to prevent the inadvertent or unauthorized disclosure of or unauthorized access to information related to the representation of a client.”

- Comment 18: Rule 1.6 is not violated “if the lawyer has made reasonable efforts to prevent disclosure.”

AM I MAKING “REASONABLE EFFORTS”?

Comment 18: “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).”

HOW AM I AFFECTED?

We have to consider Rule 1.1 and Rule 1.6 when we:

- Store data in / work in “the cloud”
- Communicate with our clients via email
- Exchange discovery documents with opposing counsel by email [ex: tax returns, business records]
- Provide documents to our experts by email [ex: business valuator, psychological evaluator]
- Handle clients’ protected health information (as defined by HIPAA)
- Have case-related information on our electronic devices (iPhones, tablets, laptops, flash drives)
- Access our work email using a non-secure WiFi network

ABA FORMAL OP. 477 (MAY 11, 2017)

- (1) Understand the Nature of the Threat.
- (2) Understand How Client Confidential Information is Transmitted and Where It Is Stored.
- (3) Understand and Use Reasonable Electronic Security Measures.
- (4) Determine How Electronic Communications About Clients' Matters Should Be Protected.
- (5) Label Client Confidential Information.
- (6) Train Lawyers and Nonlawyer Assistants in Technology and Information Security.
- (7) Conduct Due Diligence on Vendors Providing Communication Technology.

OHIO DATA PROTECTION ACT

Are you familiar with Ohio's Data Protection Act (S.B. 220)?

- Provides a legal safe harbor for business facing data breach claims
- Serves as an affirmative defense from tort claims resulting from a data breach
- Business must have implemented cybersecurity controls: one that "reasonably conforms to an industry recognized cybersecurity framework."
- Aims to incentivize businesses to invest in cybersecurity frameworks
- Ohio is the first state to enact this type of safe harbor law

What are our industry standards?

How many of your firms have written cybersecurity policies?




The Data Protection Act

In 2017, 61 percent of small businesses experienced a cyberattack.

Small to medium-sized businesses spent an average of \$1 million increase of damage from cyberattacks in 2017.

An average data breach of a small to medium-sized business involves 9,000 individual records.

Source: "2017 State of Cybersecurity in Small & Medium-Sized Businesses" by Ponemon Institute

The Data Protection Act is the first piece of legislation introduced as a result of Ohio Attorney General Mike DeWine's CyberOhio Initiative. Gov. John Kasich signed the act, Senate Bill 220, into law in August 2018. The law encourages businesses to voluntarily adopt strong cybersecurity practices to protect consumer data.

The Data Protection Act specifies industry-recognized security frameworks for Ohio businesses to incorporate into their cybersecurity policies. Effective protections save customers from the expense, embarrassment, and harm caused by having their personal information compromised. The act does not create a minimum cybersecurity standard and is intended to be an incentive for businesses to achieve a higher level of cybersecurity through voluntary action. If a business has a cybersecurity program that meets one of the act's requirements, it is eligible to use the affirmative defense in the event of a lawsuit from the result of a data breach.

Affirmative defense

The purpose of the act is to provide an affirmative defense to a lawsuit that alleges a data breach was caused by a business' failure to implement reasonable information security controls. (An affirmative defense allows a defendant to introduce evidence, that if found credible, can negate civil liability, even if the allegations are true.)

Flexible programs

Under this act, a cybersecurity program is scalable to each business based on:

- Size
- Complexity
- Nature
- Cost
- Resources

Supported security frameworks

The cybersecurity frameworks incorporated into the act:

- National Institute of Standards and Technology (NIST)
- Federal Risk and Authorization Management Program (FedRAMP)
- Center for Internet Security (CIS) Controls
- International Organization for Standardization (ISO) 27000
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Federal Information Security Management Act (FISMA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Payment Card Industry Data Security Standard (PCI DSS)

Launched in 2016, the goal of CyberOhio is to help foster a legal, technical, and collaborative cybersecurity environment to help Ohio businesses thrive. In addition to promoting legislation, other parts of the initiative include training opportunities for businesses, development of cybersecurity workforce personnel, and expansion of the Ohio Attorney General's Identity Theft Unit.

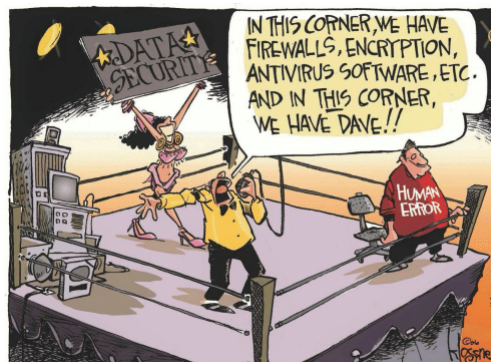


MIKE DEWINE
OHIO ATTORNEY GENERAL
www.OhioAttorneyGeneral.gov

For more information, contact CyberOhio@OhioAttorneyGeneral.gov or call **800-282-0515**.

BASIC DATA SECURITY

EDUCATE YOURSELF (AND YOUR STAFF)



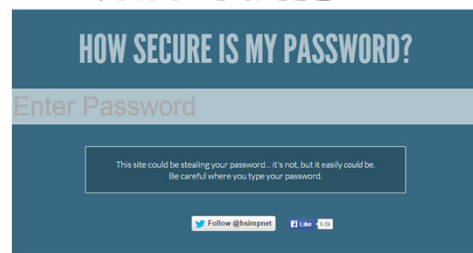
PASSWORD SECURITY

Standard is now 12 characters, with letters, numbers, and characters (!@#\$%&)

Check your password security at www.howsecureismypassword.net

Generate a random password at <https://www.random.org/passwords/>

Consider a password manager (ex: LastPass)



PHISHING EMAILS

From: OutlookOffice365 <frank.greg254@coremail.net>
Sent: Tuesday, October 2, 2018 3:50 AM
To: [REDACTED]
Subject: Action Needed

Hello,
Message is from trusted source.

Your Incoming messages has been blocked

Hi [REDACTED]

Most of your recently sent emails couldn't be delivered.

When the sender tried to send messages to you, the receiving email server reported an error. Kindly follow the instruction below to manage your [22] Undelivered Messages as of the 1st of October 2018.

To import the blocked messages click here to [FIX ERRORS](#)
To delete the blocked messages click here to [DELETE](#)
To save in archive click here to [ARCHIVE](#)

Sincerely,
Microsoft IT Administrator

Microsoft Corporation | One Microsoft Way Redmond, WA 98052-6399
This message was sent from an unmonitored email address. Please do not reply to this message.

[Privacy](#) | [Legal](#)

PHISHING EMAILS

(Action Required!)
Mail Closure Alert

Hello,

We received a notification from [REDACTED] for Mail Deactivation. Please ignore this message if the request was from you. Your account would be deleted from our system in the next 24 hours.

(Note: All mails in your inbox, spam, draft, and sent items would be deleted, and access to your account would be declined.)

If you wish to cancel this request, do so below:

[Cancel
Request](#)

NB: This request originated from the above mentioned email and reasons may be due to account violation of our usage right.

Mail Administrator.

Reference information
Reference ID: b3325cc0-a9de-4133-b575-e7a9e50db261
Username: [REDACTED]

DISPOSING OF CLIENT DATA



Remember the obligation to take reasonable steps to safeguard client information. This continues after your representation has ended!

Paper files?

Electronic files?

Copy machines?

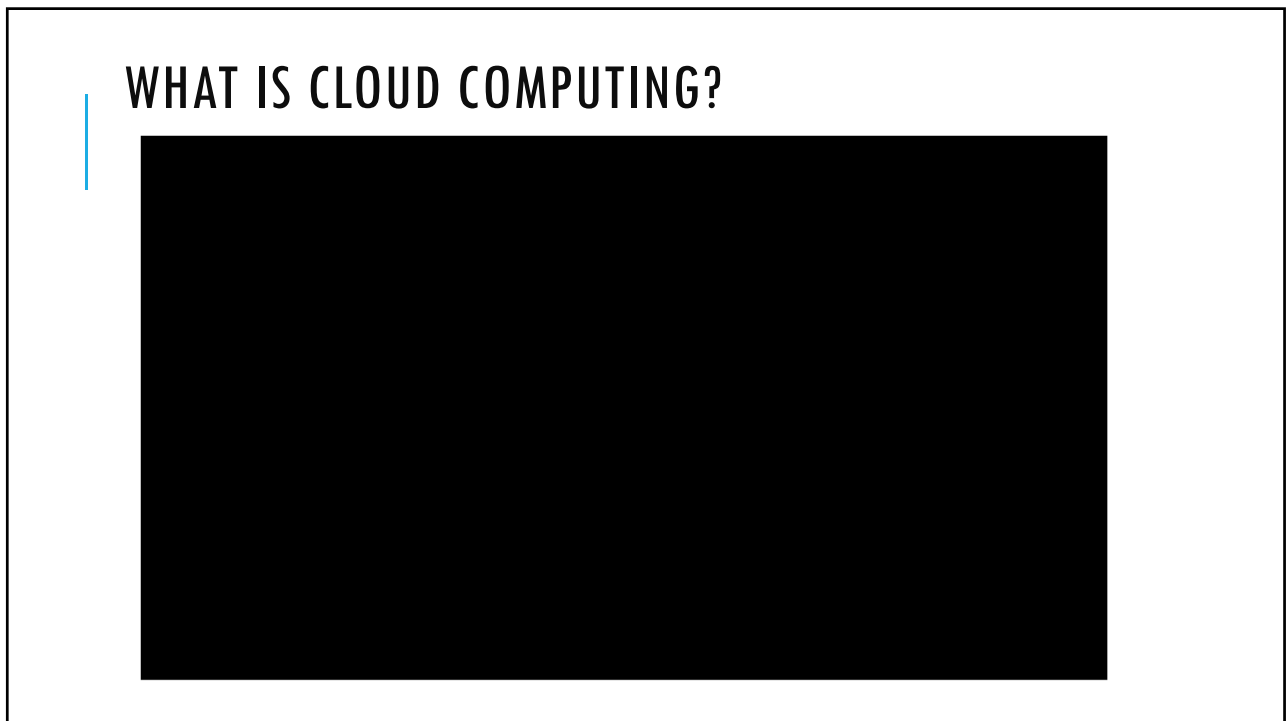
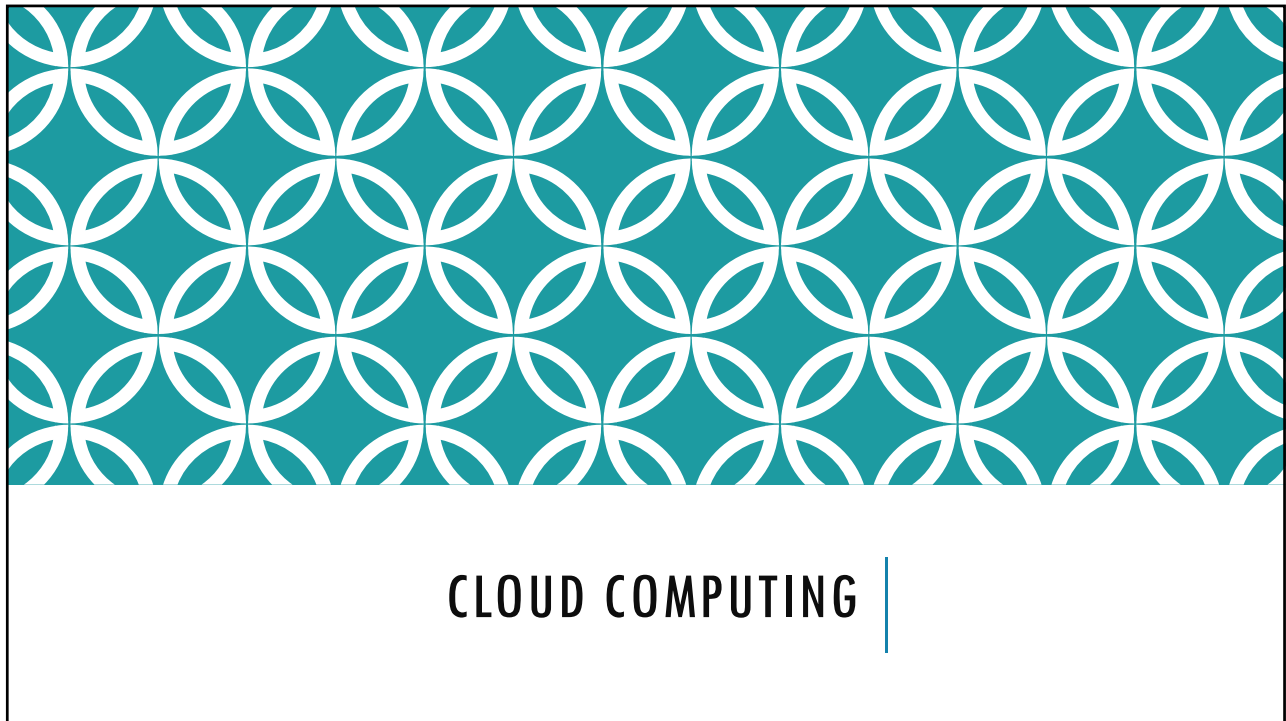
Meta data?

Flash drives?

Hard drives?

 Data wiping software

 Physical destruction

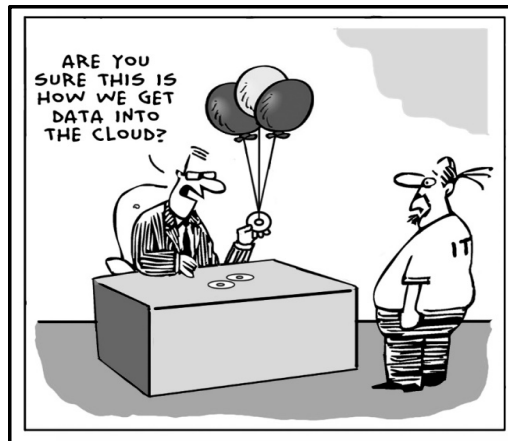


CLOUD COMPUTING

What is it?

"If an attorney uses a Smartphone or an iPhone, or uses web-based electronic mail such as Gmail, Yahoo!, Hotmail or AOL Mail, or uses products such as Google Docs, Microsoft Office 365 or Dropbox, the attorney is using 'cloud computing'. While there are many technical ways to describe cloud computing, perhaps the best description is that cloud computing is merely a 'fancy way of saying stuff's not on your computer.'"

- PA Bar Ethics Opinion 2011-20



ABA: "UNDERSTAND HOW CLIENT INFO. IS TRANSMITTED AND WHERE IT IS STORED"

Ohio Rules of Professional Conduct do not prohibit storing data in the cloud. (OSBA Informal Advisory Op. 2013-03):

- Duties regarding cloud storage are analogous to duties when lawyers use third-party vendors to store paper files off-site.
- "Because technology changes so quickly, overly specific rules would be obsolete as soon as they were issues."

General consensus: cloud computing is ethically acceptable provided an appropriate amount of due diligence is undertaken prior to selecting a provider.

- See supplemental materials for full list of state ethics opinions.

WHERE IS YOUR DATA STORED?



VETTING YOUR CLOUD PROVIDER



Ensure that your cloud provider:

1. Explicitly agrees that it has no ownership or security interest in the data;
2. Has an enforceable obligation to preserve security;
3. Will notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider produces the requested information;
4. Has technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing;
5. Provides the firm with the right to audit the provider's security procedures and to obtain copies of any security audits performed;
6. Will host the firm's data only within a specified geographic area. If the data is hosted outside of the U.S., the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the U.S.;
7. Provides the ability for the law firm, on demand, to get data from the vendor's or third-party data hosting company's servers for the firm's own use or for in-house back-up.

(Copyright © 2013 by the American Bar Association. Reprinted with permission.)

CLOUD COMPUTING & INFORMED CONSENT

“Although not required to do so, a lawyer should inform clients regarding the use of ‘cloud’ storage of all or part of the client’s file. Some clients may have legitimate concerns about the level of security employed by vendors selected by the lawyer.”

- Ohio Ethics Guide: Client File Retention (March 18, 2016)

Rule 1.6, Comment 18: “... A client may require the lawyer to implement special security measures not required by this rule or [may give informed consent to forego security measures](#) that would otherwise be required by this rule.”

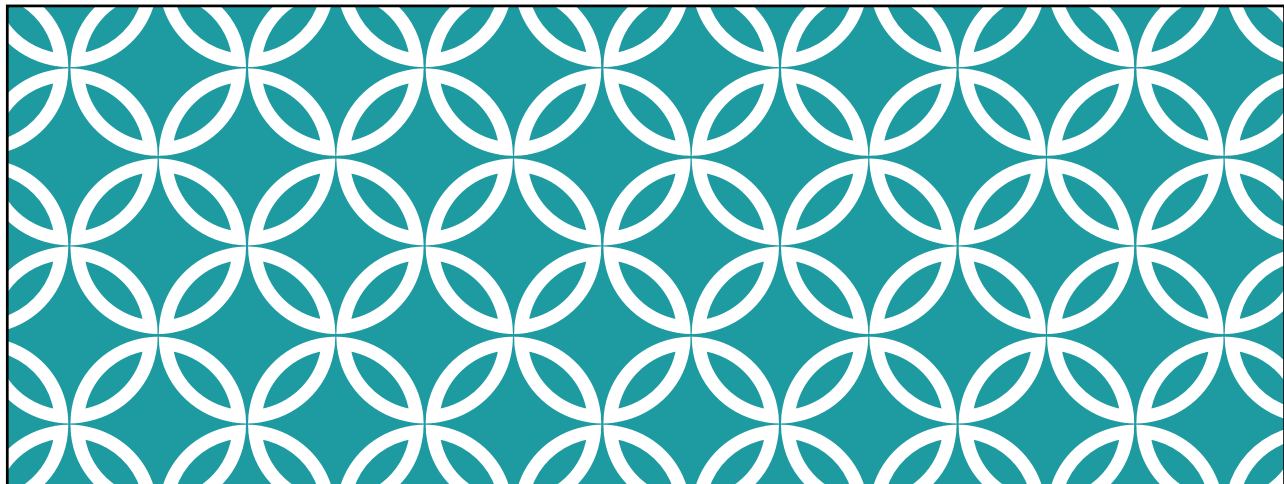
CLOUD COMPUTING TAKEAWAY

You are “working in the cloud” in one form or another

Before you begin storing client information “in the cloud,” review the cloud provider’s security policy and ensure that it complies with the factors set forth by the ABA

Have a discussion with your clients about your cloud provider and obtain their informed consent (as part of your engagement agreement) before you store their data “in the cloud”

Hire an IT consultant, even if only on an “as needed” basis



ELECTRONIC COMMUNICATIONS

ELECTRONIC COMMUNICATIONS

“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.”

Rule 1.6, Comment 19



REASONABLE EXPECTATION OF PRIVACY?

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.

(Rule 1.6, Comment 19)



WHAT ABOUT EMAIL?

In 1999, the ABA concluded that a lawyer did not violate Rule 1.6 by sending information related to the representation of a client by unencrypted email because email afforded a reasonable expectation of privacy.

However, the opinion urged caution when transmitting highly sensitive information.

- See supplemental materials – ABA Formal Opinion 99-413 (1999).

EMAILING CLIENTS ON THEIR WORK DEVICES?

“Clients may not be afforded a ‘reasonable expectation of privacy’ when they use an employer’s computer to send e-mails to their lawyers or receive e-mails from their lawyers. Judicial decisions illustrate the risk that the employer will read these e-mail communications and seek to use them to the employee’s disadvantage.”

(ABA Formal Op. 11-459)

“Unless a lawyer has reason to believe otherwise, a lawyer ordinarily should assume that an employer’s internal policy allows for access to the employee’s e-mails sent to or from a workplace device or system.”

(ABA Formal Op. 11-459)

EMAILING CLIENTS ON THEIR WORK DEVICES?

“Given these risks, a lawyer should ordinarily advise the employee-client about the importance of communicating with the lawyer in a manner that protects the confidentiality of e-mail communications, just as a lawyer should avoid speaking face-to-face with a client about sensitive matters if the conversation might be overheard... In particular, as soon as practical after a client-lawyer relationship is established, a lawyer typically should instruct the employee-client to avoid using a workplace device or system for sensitive or substantive communications, and perhaps for any attorney-client communications, because even seemingly ministerial communications involving matters such as scheduling can have substantive ramifications.”

(ABA Formal Op. 11-459)

A DUTY TO WARN OUR CLIENTS ABOUT E-MAIL?

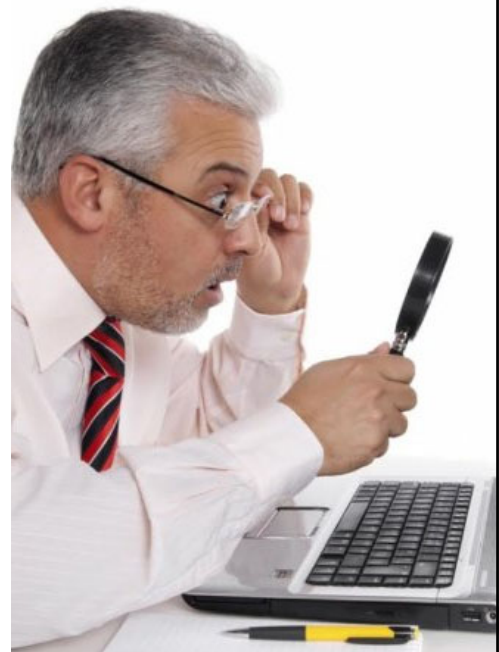
“Clients may be unaware of the possibility that a third party may gain access to their personal correspondence and may fail to take necessary precautions... [which] raises the question of what, if any, steps a lawyer must take to prevent such access by third parties from occurring.”

• ABA Formal Opinion 11-459



CAN THE CLIENT WAIVE THE RISK?

“Protective measures would include the lawyer refraining from sending e-mails to the client’s workplace, as distinct from personal, e-mail address, and cautioning the client against using a business e-mail account or using a personal e-mail account on a workplace computer or device at least for substantive e-mails with counsel...Of course, if the lawyer becomes aware that a client is receiving personal e-mail on a workplace computer or other device owned or controlled by the employer, then a duty arises to caution the client not to do so, and if that caution is not heeded, to cease sending messages even to personal e-mail addresses.”



NEW ABA OPINION ON TECHNOLOGY (5/11/2017)

ABA Formal Op. 477 revisits and updates its earlier opinion in light of the recent “technology amendments” to the ethical rules - “Unlike 1999 where multiple methods of communication were prevalent, today, many lawyers primarily use electronic means to communicate and exchange documents...”

What does this mean for my practice?

- Unencrypted routine email generally remains an acceptable method of communication, but...
- Particularly strong protective measures, like encryption, are warranted in some circumstances
- You should be discussing security safeguards with your clients
- You may need to obtain informed consent from your client to *not* use enhanced security measures
- “Reasonable efforts” might require avoiding electronic communication altogether
- **“Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically.”**

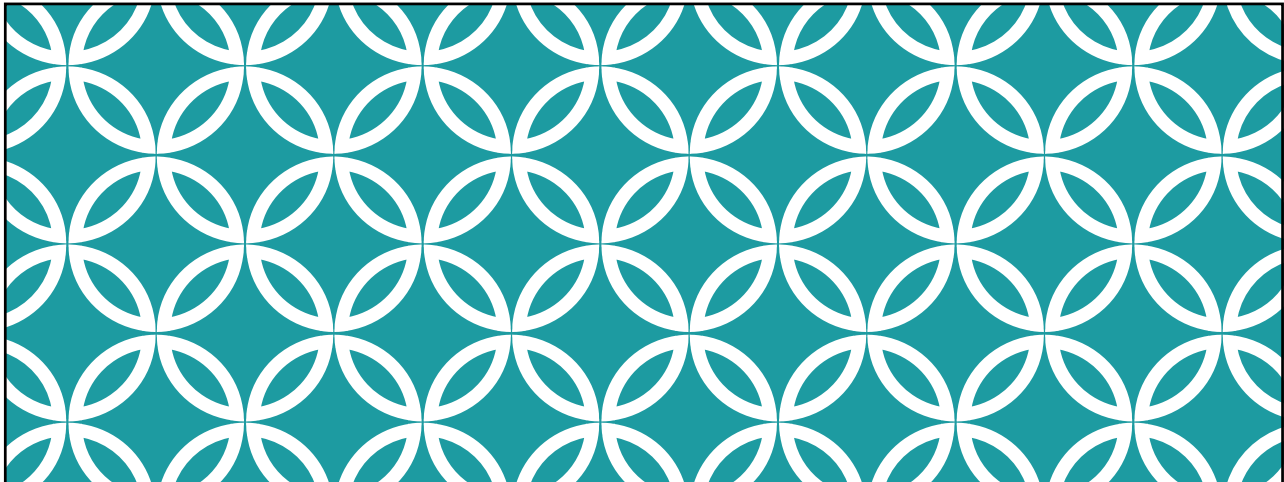
EMAIL TAKEAWAY

Have a discussion with your clients about communicating by email at the outset of your representation

Advise clients in writing (in your engagement agreement) that there are risks associated with email and obtain their informed consent to use this means of communication

Advise clients in writing that emails they send from employer-provided email addresses may not be privileged, and therefore you will not respond

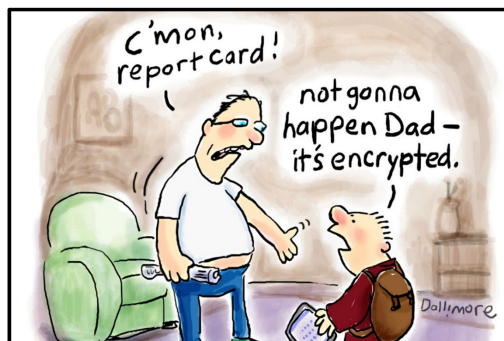
Require that clients set up a private email address to communicate only with you



ENCRYPTION

WHAT IS ENCRYPTION?

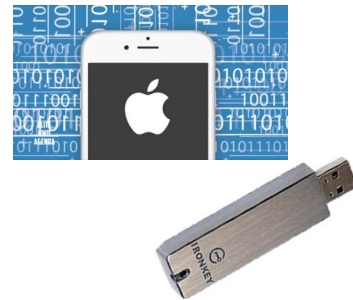
A security measure that protects data in storage (on computers, laptops, smartphones, tablets, and portable devices) and transmitted data (over wired and wireless networks, including email)



ENCRYPTING YOUR “DATA AT REST”

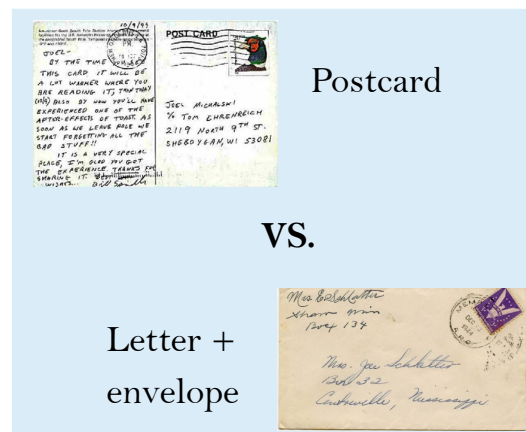
Encrypting mobile devices is especially important because they are easily stolen, lost, etc.

- **iPhones, iPads:** automatic on iOS devices so long as password protected; the device is encrypted while locked by decrypted when unlocked
 - Use a complex password. See materials for instructions.
- **Laptops / tablets:** built-in on current business versions of Windows (BitLocker) & Apple OS X (FileVault)
- **Flash drives:** DataTraveler, BitLocker to Go, IronKey, SanDisk Cruzer



ENCRYPTING YOUR DATA “IN TRANSMISSION”

- Requires a pair of keys (one for sender, one for recipient) – both parties must have program
- Basic encryption of attachments is free on Microsoft Word and Adobe PDF – this *doesn't* encrypt the email itself, just the attachment
- See supplemental materials for instructions



IS ENCRYPTION REQUIRED?

Recall that Rule 1.6 requires that “reasonable efforts” to prevent the inadvertent disclosure of client information.

“In general, considering the present state of technology and email usage, a lawyer may communicate confidential information by email. In some circumstances, however, a lawyer should consider whether the confidentiality of the information will be protected if communicated by email and whether it is prudent to use encrypted email or another form of communication.” (TX Ethics Op. 648 (2015).)

ENCRYPTION IS PROBABLY REQUIRED WHEN...

- communicating highly sensitive or confidential information via email or unencrypted email connections;
- sending an email to or from an account that the email sender or recipient shares with others;
- sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client’s work email account, especially if the email relates to a client’s employment dispute with his employer;



ENCRYPTION IS PROBABLY REQUIRED WHEN...

- sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;
- sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
- sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer's email communication, with or without a warrant.



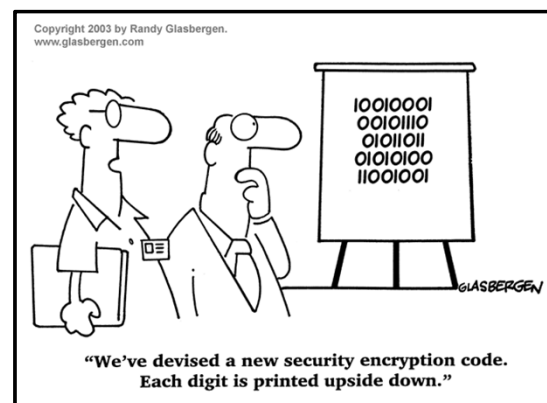
ENCRYPTION TAKEAWAY

Experts are now calling it a “no-brainer.” It is simple, cheap, and readily available.

Encrypting portable devices is a must.

Whether encryption is required in transmitting information electronically probably depends on the sensitivity of the information.

Alternatives to encrypting emails (encrypting attachments) are simple and free.



PUBLIC WI-FI

DANGERS OF PUBLIC WI-FI

Public Wi-Fi that is available at airports, hotels, coffee shops, etc., though convenient, often do not have the necessary security features to protect the data being transmitted

Rule 1.6 requires that we take steps to prevent the unauthorized disclosure of client information. Do we violate that when we use hotel Wi-Fi to email confidential client information?

Hot spots



ETHICS OF PUBLIC WI-FI

“The Committee’s own research – including conferring with computer security experts – causes it to understand that, without appropriate safeguards (such as firewalls, secure username/password combinations, and encryption), data transmitted wirelessly can be intercepted and read with increasing ease. Unfortunately, guidance to attorneys in this area has not kept pace with technology.”

• California Formal Opinion No. 2010-179



ETHICS OF PUBLIC WI-FI

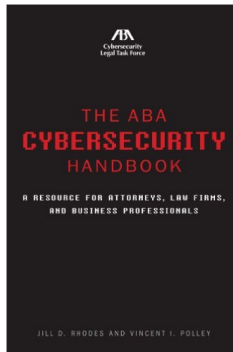


“With regard to the use of a public wireless connection, ...due to the lack of security features provided in most public wireless access locations, Attorney risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on Client’s matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall. Depending on the sensitivity of the matter, Attorney may need to avoid using the public wireless connection entirely or notify Client of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so.”

• California Formal Opinion No. 2010-179

RESOURCES

The ABA Cybersecurity Handbook



ABA Law Practice Division



AMENDMENTS TO THE OHIO RULES OF PROFESSIONAL CONDUCT

The following amendments to the Ohio Rules of Professional Conduct (Prof. Cond. R. 1.0, 1.1, 1.4, 1.6, 1.12, 1.17, 1.18, 4.4, 5.3, 5.5, 7.1, 7.2, 7.3, and 8.5) were adopted by the Supreme Court of Ohio. The history of the amendments is as follows:

September 15, 2014	Initial publication for comment
February 24, 2015	Final adoption by Supreme Court
April 1, 2015	Effective date of amendments

OHIO RULES OF PROFESSIONAL CONDUCT

[Existing language unaffected by the amendments is omitted to conserve space]

RULE 1.0: TERMINOLOGY

As used in these rules:

[Existing language unaffected by the amendments is omitted to conserve space]

(p) “Writing” or “written” denotes a tangible or electronic record of a communication or representation, including handwriting, typewriting, printing, photostating, photography, audio or videorecording, and electronic communications. A “signed” writing includes an electronic sound, symbol, or process attached to or logically associated with a writing and executed or adopted by a person with the intent to sign the writing.

Comment

[Existing language unaffected by the amendments is omitted to conserve space]

[7] Obtaining informed consent will usually require an affirmative response by the client or other person. In general, a lawyer may not assume consent from a client’s or other person’s silence. Consent may be inferred, however, from the conduct of a client or other person who has reasonably adequate information about the matter. A number of rules require that a person’s consent be confirmed in writing. See Rules 1.7(b) and 1.9(a). For a definition of “writing” and “confirmed in writing,” see divisions (p) and (b). Other rules require that a client’s consent be obtained in a writing signed by the client. See, *e.g.*, Rules 1.8(a) and (g). For a definition of “signed,” see division (p).

Screened

[8] This definition applies to situations where screening of a personally disqualified lawyer is permitted to remove imputation of a conflict of interest under Rules 1.10, 1.11, 1.12, or 1.18.

[9] The purpose of screening is to assure the affected parties that confidential information known by the personally disqualified lawyer remains protected. The personally disqualified lawyer should acknowledge the obligation not to communicate with any of the other lawyers in the firm with respect to the matter. Similarly, other lawyers in the firm who are working on the matter should be informed that the screening is in place and that they may not communicate with the personally disqualified lawyer with respect to the matter. Additional screening measures that are appropriate for the particular matter will depend on the circumstances. To implement, reinforce, and remind all affected lawyers of the presence of the screening, it may be appropriate for the firm to undertake such procedures as a written undertaking by the screened lawyer to avoid any communication with other firm personnel and any contact with any firm files or other information, including information in electronic form, relating to the matter, written notice and instructions to all other firm personnel forbidding any communication with the screened lawyer relating to the matter, denial of access by the screened lawyer to firm files or other information, including information in electronic form, relating to the matter, and periodic reminders of the screen to the screened lawyer and all other firm personnel.

[Existing language unaffected by the amendments is omitted to conserve space]

I. CLIENT-LAWYER RELATIONSHIP

RULE 1.1: COMPETENCE

[No amendments to the black-letter rule]

Comment

[Existing language unaffected by the amendments is omitted to conserve space]

Retaining or Contracting with Other Lawyers

[6] Before a lawyer retains or contracts with another lawyer outside the lawyer's own firm to provide or assist in the provision of legal services to a client, the lawyer should ordinarily obtain informed consent from the client and must reasonably believe that the other lawyer's services will contribute to the competent and ethical representation of the client. See also Rule 1.2, 1.4, 1.5(e), 1.6, and 5.5(a). The reasonableness of the decision to retain or contract with another lawyer outside the lawyer's own firm will depend on the circumstances, including the education, experience, and reputation of the nonfirm lawyer, the nature of the services assigned to the nonfirm lawyer, and the legal protections, professional conduct rules, and ethical environments of the jurisdiction in which the services will be performed, particularly relating to

confidential information. The decision to contract with a lawyer for purposes other than the provision of legal services, such to serve as an expert witness, may be governed by other rules. See Rule 1.4 and 1.5.

[7] When lawyers from more than one law firm are providing legal services to the client on a particular matter, the lawyers should ordinarily consult with each other and the client about the scope of their respective representations and the allocation of responsibility between or among them. See Rule 1.2. When making allocations of responsibility in a matter pending before a tribunal, lawyers and parties may have additional obligations that are a matter of law and beyond the scope of these rules.

Maintaining Competence

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

[Existing language unaffected by the amendments is omitted to conserve space]

RULE 1.4: COMMUNICATION

[No amendments to the black-letter rule]

Comment

[Existing language unaffected by the amendments is omitted to conserve space]

[4] A lawyer's regular communication with clients will minimize the occasions on which a client will need to request information concerning the representation. When a client makes a reasonable request for information, however, division (a)(4) requires prompt compliance with the request, or if a prompt response is not feasible, that the lawyer, or a member of the lawyer's staff, acknowledge receipt of the request and advise the client when a response may be expected. A lawyer should promptly respond to or acknowledge client communications.

[Existing language unaffected by the amendments is omitted to conserve space]

RULE 1.6: CONFIDENTIALITY OF INFORMATION

(a) A lawyer shall not reveal information relating to the representation of a client, including information protected by the attorney-client privilege under applicable law, unless the client gives *informed consent*, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by division (b) or required by division (d) of this rule.

(b) A lawyer may reveal information relating to the representation of a client, including information protected by the attorney-client privilege under applicable law, to the extent the lawyer *reasonably believes* necessary for any of the following purposes:

- (1) to prevent reasonably certain death or substantial bodily harm;
- (2) to prevent the commission of a crime by the client or other person;
- (3) to mitigate *substantial* injury to the financial interests or property of another that has resulted from the client's commission of an *illegal* or *fraudulent* act, in furtherance of which the client has used the lawyer's services;
- (4) to secure legal advice about the lawyer's compliance with these rules;
- (5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding, including any disciplinary matter, concerning the lawyer's representation of the client;
- (6) to comply with other law or a court order;
- (7) to detect and resolve conflicts of interest arising from the lawyer's change of employment or from changes in the composition or ownership of a *firm*, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

(c) A lawyer shall make *reasonable* efforts to prevent the inadvertent or unauthorized disclosure of or unauthorized access to information related to the representation of a client.

(d) A lawyer shall reveal information relating to the representation of a client, including information protected by the attorney-client privilege under applicable law, to the extent the lawyer *reasonably believes* necessary to comply with Rule 3.3 or 4.1.

Comment

[Existing language unaffected by the amendments is omitted to conserve space]

Detection of Conflicts of Interest

[13] Division (b)(7) recognizes that lawyers in different firms may need to disclose limited information to each other to detect and resolve conflicts of interest, such as when a lawyer is considering an association with another firm, two or more firms are considering a merger, or a lawyer is considering the purchase of a law practice. See Rule 1.17, Comment [7].

Under these circumstances, lawyers and law firms are permitted to disclose limited information, but only once substantive discussions regarding the new relationship have occurred. Any such disclosure should ordinarily include no more than the identity of the persons and entities involved in a matter, a brief summary of the general issues involved, and information about whether the matter has terminated. Even this limited information should be disclosed only to the extent reasonably necessary to detect and resolve conflicts of interest that might arise from the possible new relationship. Moreover, the disclosure of any information is prohibited if it would compromise the attorney-client privilege or otherwise prejudice the client (*e.g.*, the fact that a corporate client is seeking advice on a corporate takeover that has not been publicly announced; that a person has consulted a lawyer about the possibility of a divorce before the person's intentions are known to the person's spouse; or that a person has consulted a lawyer about a criminal investigation that has not led to a public charge). Under those circumstances, division (a) prohibits disclosure unless the client or former client gives informed consent. A lawyer's fiduciary duty to the lawyer's firm may also govern a lawyer's conduct when exploring an association with another firm and is beyond the scope of these rules.

[14] Any information disclosed pursuant to division (b)(7) may be used or further disclosed only to the extent necessary to detect and resolve conflicts of interest. Division (b)(7) does not restrict the use of information acquired by means independent of any disclosure pursuant to division (b)(7). Division (b)(7) also does not affect the disclosure of information within a law firm when the disclosure is otherwise authorized, such as when a lawyer in a firm discloses information to another lawyer in the same firm to detect and resolve conflicts of interest that could arise in connection with undertaking a new representation. See Comment [5].

[15] A lawyer may be ordered to reveal information relating to the representation of a client by a court or by another tribunal or governmental entity claiming authority pursuant to other law to compel the disclosure. Absent informed consent of the client to do otherwise, the lawyer should assert on behalf of the client all nonfrivolous claims that the order is not authorized by other law or that the information sought is protected against disclosure by the attorney-client privilege or other applicable law. In the event of an adverse ruling, the lawyer must consult with the client about the possibility of appeal to the extent required by Rule 1.4. Unless review is sought, however, division (b)(6) permits the lawyer to comply with the court's order.

[16] Division (b) permits disclosure only to the extent the lawyer reasonably believes the disclosure is necessary to accomplish one of the purposes specified. Where practicable, the lawyer should first seek to persuade the client to take suitable action to obviate the need for disclosure. A disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to accomplish the purpose. If the disclosure will be made in connection with a judicial proceeding, the disclosure should be made in a manner that limits access to the information to the tribunal or other persons having a need to know it and appropriate protective orders or other arrangements should be sought by the lawyer to the fullest extent practicable. Before making a disclosure under division (b)(1), (2), or (3), a lawyer for an organization should ordinarily bring the issue of taking suitable action to higher authority within the organization, including, if warranted by the circumstances, to the highest authority that can act on behalf of the organization as determined by applicable law.

[17] Division (b) permits but does not require the disclosure of information relating to a client's representation to accomplish the purposes specified in divisions (b)(1) through (b)(6). In exercising the discretion conferred by this rule, the lawyer may consider such factors as the nature of the lawyer's relationship with the client and with those who might be injured by the client, the lawyer's own involvement in the transaction, and factors that may extenuate the conduct in question. A lawyer's decision not to disclose as permitted by division (b) does not violate this rule. Disclosure may be required, however, by other rules. Some rules require disclosure only if such disclosure would be permitted by division (b). See Rules 4.1(b), 8.1 and 8.3. Rule 3.3, on the other hand, requires disclosure in some circumstances regardless of whether such disclosure is permitted by this rule.

Acting Competently to Preserve Confidentiality

[18] Division (c) 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 related to the representation of a client does not constitute a violation of division (c) 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 forego 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 or federal laws that govern data privacy or that impose specific 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] and [4].

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

Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws governing data privacy, is beyond the scope of these rules.

Former Client

[20] The duty of confidentiality continues after the client-lawyer relationship has terminated. See Rule 1.9(c)(2). See Rule 1.9(c)(1) for the prohibition against using such information to the disadvantage of the former client.

[Existing language unaffected by the amendments is omitted to conserve space]

RULE 1.12: FORMER JUDGE, ARBITRATOR, MEDIATOR, OR OTHER THIRD-PARTY NEUTRAL

[Existing language unaffected by the amendments is omitted to conserve space]

Comment

[1] This rule generally parallels Rule 1.11. The term “personally and substantially” signifies that a judge who was a member of a multimember court, and thereafter left judicial office to practice law, is not prohibited from representing a client in a matter pending in the court, but in which the former judge did not participate. So also the fact that a former judge exercised administrative responsibility in a court does not prevent the former judge from acting as a lawyer in a matter where the judge had previously exercised remote or incidental administrative responsibility that did not affect the merits. Compare the Comment to Rule 1.11. The term “adjudicative officer” includes such officials as judges pro tempore, magistrates, special masters, hearing officers, and other parajudicial officers, and also lawyers who serve as parttime judges. Part III of the Application section of the Ohio Code of Judicial Conduct provides that a parttime judge shall not “act as a lawyer in any proceeding in which the judge served as a judge or in any other related proceeding.” Although phrased differently from this rule, the provisions correspond in meaning.

[Existing language unaffected by the amendments is omitted to conserve space]

RULE 1.17: SALE OF LAW PRACTICE

[Existing language unaffected by the amendments is omitted to conserve space]

(h) The *written* notice to clients required by division (e) and (f) of this rule shall be provided by regular mail with a certificate of mailing or other comparable proof of mailing. In lieu of providing notice by mail, either the selling lawyer or purchasing lawyer, or both, may personally deliver the notice to a client. In the case of personal delivery, the lawyer providing the notice shall obtain *written* acknowledgement of the delivery from the client.

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.” Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. 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.

Introduction¹

Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers.² In one highly publicized incident, hackers infiltrated the computer networks at some of the country’s most well-known law firms, likely looking for confidential information to exploit through insider trading schemes.³ Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.⁴

In Formal Opinion 477R, this Committee explained a lawyer’s ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet.⁵ This

¹ This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2018. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in individual jurisdictions are controlling.

² See, e.g., Dan Steiner, *Hackers Are Aggressively Targeting Law Firms’ Data* (Aug. 3, 2017), <https://www.cio.com> (explaining that “[f]rom patent disputes to employment contracts, law firms have a lot of exposure to sensitive information. Because of their involvement, confidential information is stored on the enterprise systems that law firms use. . . . This makes them a juicy target for hackers that want to steal consumer information and corporate intelligence.”); See also *Criminal-Seeking-Hacker’ Requests Network Breach for Insider Trading*, Private Industry Notification 160304-01, FBI, CYBER DIVISION (Mar. 4, 2016).

³ Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J. (Mar. 29, 2016), <https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504>.

⁴ Robert S. Mueller, III, *Combatting Threats in the Cyber World Outsmarting Terrorists, Hackers and Spies*, FBI (Mar. 1, 2012), <https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies>.

⁵ ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (2017) (“Securing Communication of Protected Client Information”).

opinion picks up where Opinion 477R left off, and discusses an attorney's ethical obligations when a data breach exposes client confidential information. This opinion focuses on an attorney's ethical obligations after a data breach,⁶ and it addresses only data breaches that involve information relating to the representation of a client. It does not address other laws that may impose post-breach obligations, such as privacy laws or other statutory schemes that law firm data breaches might also implicate. Each statutory scheme may have different post-breach obligations, including different notice triggers and different response obligations. Both the triggers and obligations in those statutory schemes may overlap with the ethical obligations discussed in this opinion. And, as a matter of best practices, attorneys who have experienced a data breach should review all potentially applicable legal response obligations. However, compliance with statutes such as state breach notification laws, HIPAA, or the Gramm-Leach-Bliley Act does not necessarily achieve compliance with ethics obligations. Nor does compliance with lawyer regulatory rules *per se* represent compliance with breach response laws. As a matter of best practices, lawyers who have suffered a data breach should analyze compliance separately under every applicable law or rule.

Compliance with the obligations imposed by the Model Rules of Professional Conduct, as set forth in this opinion, depends on the nature of the cyber incident, the ability of the attorney to know about the facts and circumstances surrounding the cyber incident, and the attorney's roles, level of authority, and responsibility in the law firm's operations.⁷

⁶ The Committee recognizes that lawyers provide legal services to clients under a myriad of organizational structures and circumstances. The Model Rules of Professional Conduct refer to the various structures as a "firm." A "firm" is defined in Rule 1.0(c) as "a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization or the legal department of a corporation or other organization." How a lawyer complies with the obligations discussed in this opinion will vary depending on the size and structure of the firm in which a lawyer is providing client representation and the lawyer's position in the firm. *See* MODEL RULES OF PROF'L CONDUCT R. 5.1 (2018) (Responsibilities of Partners, Managers, and Supervisory Lawyers); MODEL RULES OF PROF'L CONDUCT R. 5.2 (2018) (Responsibility of a Subordinate Lawyers); and MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018) (Responsibility Regarding Nonlawyer Assistance).

⁷ In analyzing how to implement the professional responsibility obligations set forth in this opinion, lawyers may wish to consider obtaining technical advice from cyber experts. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.") *See also, e.g., Cybersecurity Resources*, ABA Task Force on Cybersecurity, <https://www.americanbar.org/groups/cybersecurity/resources.html> (last visited Oct. 5, 2018).

I. Analysis

A. Duty of Competence

Model Rule 1.1 requires that “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”⁸ The scope of this requirement was clarified in 2012, when the ABA recognized the increasing impact of technology on the practice of law and the obligation of lawyers to develop an understanding of that technology. Comment [8] to Rule 1.1 was modified in 2012 to read:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)⁹

In recommending the change to Rule 1.1’s Comment, the ABA Commission on Ethics 20/20 explained:

Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to ‘keep abreast of changes in the law and its practice.’ The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today’s environment without knowing how to use email or create an electronic document.¹⁰

⁸ MODEL RULES OF PROF’L CONDUCT R. 1.1 (2018).

⁹ A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 43 (Art Garwin ed., 2013).

¹⁰ ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_a_mended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer’s substantive duty of competence: “Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase ‘including the benefits and risks associated with relevant technology,’ would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer’s general ethical duty to remain competent.”

In the context of a lawyer's post-breach responsibilities, both Comment [8] to Rule 1.1 and the 20/20 Commission's thinking behind it require lawyers to understand technologies that are being used to deliver legal services to their clients. Once those technologies are understood, a competent lawyer must use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer. A lawyer's competency in this regard may be satisfied either through the lawyer's own study and investigation or by employing or retaining qualified lawyer and nonlawyer assistants.¹¹

1. Obligation to Monitor for a Data Breach

Not every cyber episode experienced by a lawyer is a data breach that triggers the obligations described in this opinion. A data breach for the purposes of this opinion means a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode.

Many cyber events occur daily in lawyers' offices, but they are not a data breach because they do not result in actual compromise of material client confidential information. Other episodes rise to the level of a data breach, either through exfiltration/theft of client confidential information or through ransomware, where no client information is actually accessed or lost, but where the information is blocked and rendered inaccessible until a ransom is paid. Still other compromises involve an attack on a lawyer's systems, destroying the lawyer's infrastructure on which confidential information resides and incapacitating the attorney's ability to use that infrastructure to perform legal services.

Model Rules 5.1 and 5.3 impose upon lawyers the obligation to ensure that the firm has in effect measures giving reasonable assurance that all lawyers and staff in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2], and Model Rule 5.3 Comment [1] state that lawyers with managerial authority within a firm must make reasonable efforts to establish

¹¹ MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2018); *See also* JILL D. RHODES & ROBERT S. LITT, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 124 (2d ed. 2018) [hereinafter ABA CYBERSECURITY HANDBOOK].

internal policies and procedures designed to provide reasonable assurance that all lawyers and staff in the firm will conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2] further states that “such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised.”

Applying this reasoning, and based on lawyers’ obligations (i) to use technology competently to safeguard confidential information against unauthorized access or loss, and (ii) to supervise lawyers and staff, the Committee concludes that lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data¹² and the use of data. Without such a requirement, a lawyer’s recognition of any data breach could be relegated to happenstance --- and the lawyer might not identify whether a breach has occurred,¹³ whether further action is warranted,¹⁴ whether employees are adhering to the law firm’s cybersecurity policies and procedures so that the lawyers and the firm are in compliance with their ethical duties,¹⁵ and how and when the lawyer must take further action under other regulatory and legal provisions.¹⁶ Thus, just as lawyers must safeguard and monitor the security of paper files and actual client property, lawyers utilizing technology have the same obligation to safeguard and monitor the security of electronically stored client property and information.¹⁷

While lawyers must make reasonable efforts to monitor their technology resources to detect a breach, an ethical violation does not necessarily occur if a cyber-intrusion or loss of electronic information is not immediately detected, because cyber criminals might successfully hide their

¹² ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 08-451 (2008).

¹³ Fredric Greene, *Cybersecurity Detective Controls—Monitoring to Identify and Respond to Threats*, ISACA J., Vol. 5, 1025 (2015), available at <https://www.isaca.org/Journal/archives/2015/Volume-5/Pages/cybersecurity-detective-controls.aspx> (noting that “[d]etective controls are a key component of a cybersecurity program in providing visibility into malicious activity, breaches and attacks on an organization’s IT environment.”).

¹⁴ MODEL RULES OF PROF’L CONDUCT R. 1.6(c) (2018); MODEL RULES OF PROF’L CONDUCT R. 1.15 (2018).

¹⁵ See also MODEL RULES OF PROF’L CONDUCT R. 5.1 & 5.3 (2018).

¹⁶ The importance of monitoring to successful cybersecurity efforts is so critical that in 2015, Congress passed the Cybersecurity Information Sharing Act of 2015 (CISA) to authorize companies to monitor and implement defensive measures on their information systems, and to foreclose liability for such monitoring under CISA. AUTOMATED INDICATOR SHARING, <https://www.us-cert.gov/ais> (last visited Oct. 5, 2018); See also National Cyber Security Centre “Ten Steps to Cyber Security” [Step 8: Monitoring] (Aug. 9, 2016), <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>.

¹⁷ ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (2017).

intrusion despite reasonable or even extraordinary efforts by the lawyer. Thus, as is more fully explained below, the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach.

2. Stopping the Breach and Restoring Systems

When a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach. How a lawyer does so in any particular circumstance is beyond the scope of this opinion. As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach.¹⁸ The decision whether to adopt a plan, the content of any plan, and actions taken to train and prepare for implementation of the plan, should be made before a lawyer is swept up in an actual breach. “One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response plans help personnel to minimize loss or theft of information and disruption of services caused by incidents.”¹⁹ While every lawyer’s response plan should be tailored to the lawyer’s or the law firm’s specific practice, as a general matter incident response plans share common features:

The primary goal of any incident response plan is to have a process in place that will allow the firm to promptly respond in a coordinated manner to any type of security incident or cyber intrusion. The incident response process should promptly: identify and evaluate any potential network anomaly or intrusion; assess its nature and scope; determine if any data or information may have been accessed or compromised; quarantine the threat or malware; prevent the exfiltration of information from the firm; eradicate the malware, and restore the integrity of the firm’s network.

Incident response plans should identify the team members and their backups; provide the means to reach team members at any time an intrusion is reported, and

¹⁸ See ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 202 (explaining the utility of large law firms adopting “an incident response plan that details who has ownership of key decisions and the process to follow in the event of an incident.”).

¹⁹ NIST Computer Security Incident Handling Guide, at 6 (2012), <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>.

define the roles of each team member. The plan should outline the steps to be taken at each stage of the process, designate the team member(s) responsible for each of those steps, as well as the team member charged with overall responsibility for the response.²⁰

Whether or not the lawyer impacted by a data breach has an incident response plan in place, after taking prompt action to stop the breach, a competent lawyer must make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer's clients. The lawyer may do so either on her own, if qualified, or through association with experts. This restoration process provides the lawyer with an opportunity to evaluate what occurred and how to prevent a reoccurrence consistent with the obligation under Model Rule 1.6(c) that lawyers "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client."²¹ These reasonable efforts could include (i) restoring the technology systems as practical, (ii) the implementation of new technology or new systems, or (iii) the use of no technology at all if the task does not require it, depending on the circumstances.

3. Determining What Occurred

The Model Rules do not impose greater or different obligations on a lawyer as a result of a breach involving client information, regardless of whether the breach occurs through electronic or physical means. Just as a lawyer would need to assess which paper files were stolen from the lawyer's office, so too lawyers must make reasonable attempts to determine whether electronic files were accessed, and if so, which ones. A competent attorney must make reasonable efforts to determine what occurred during the data breach. A post-breach investigation requires that the lawyer gather sufficient information to ensure the intrusion has been stopped and then, to the extent reasonably possible, evaluate the data lost or accessed. The information gathered in a post-breach investigation is necessary to understand the scope of the intrusion and to allow for accurate disclosure to the client consistent with the lawyer's duty of communication and honesty under

²⁰ Steven M. Puiszis, *Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning*, THE PROF'L LAWYER, Vol. 24, No. 3 (Nov. 2017).

²¹ We discuss Model Rule 1.6(c) further below. But in restoring computer operations, lawyers should consider whether the lawyer's computer systems need to be upgraded or otherwise modified to address vulnerabilities, and further, whether some information is too sensitive to continue to be stored electronically.

Model Rules 1.4 and 8.4(c).²² Again, how a lawyer actually makes this determination is beyond the scope of this opinion. Such protocols may be a part of an incident response plan.

B. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the Rule and the commentary about a lawyer's efforts that are required to preserve the confidentiality of information relating to the representation of a client. Model Rule 1.6(a) requires that "A lawyer shall not reveal information relating to the representation of a client" unless certain circumstances arise.²³ The 2012 modification added a duty in paragraph (c) that: "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."²⁴

Amended Comment [18] explains:

Paragraph (c) 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 (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) 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

²² The rules against dishonesty and deceit may apply, for example, where the lawyer's failure to make an adequate disclosure --- or any disclosure at all --- amounts to deceit by silence. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 4.1 cmt. [1] (2018) ("Misrepresentations can also occur by partially true but misleading statements or omissions that are the equivalent of affirmative false statements.").

²³ MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2018).

²⁴ *Id.* at (c).

- 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).²⁵

As this Committee recognized in ABA Formal Opinion 477R:

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.

As discussed above and in Formal Opinion 477R, an attorney’s competence in preserving a client’s confidentiality is not a strict liability standard and does not require the lawyer to be invulnerable or impenetrable.²⁶ Rather, the obligation is one of reasonable efforts. Rule 1.6 is not violated even if data is lost or accessed if the lawyer has made reasonable efforts to prevent the loss or access.²⁷ As noted above, this obligation includes efforts to monitor for breaches of client confidentiality. The nature and scope of this standard is addressed in the ABA Cybersecurity Handbook:

Although security is relative, a legal standard for “reasonable” security is emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or 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 the measures are effectively implemented, and ensure that they are continually updated in response to new developments.²⁸

²⁵ MODEL RULES OF PROF’L CONDUCT R. 1.6 cmt. [18] (2018). “The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available.” ABA COMMISSION REPORT 105A, *supra* note 9, at 5.

²⁶ ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 122.

²⁷ MODEL RULES OF PROF’L CONDUCT R. 1.6, cmt. [18] (2018) (“The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.”)

²⁸ ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 73.

Finally, Model Rule 1.6 permits a lawyer to reveal information relating to the representation of a client if the disclosure is impliedly authorized in order to carry out the representation. Such disclosures are permitted if the lawyer reasonably believes that disclosure: (1) is impliedly authorized and will advance the interests of the client in the representation, and (2) will not affect a material interest of the client adversely.²⁹ In exercising this discretion to disclose information to law enforcement about the data breach, the lawyer must consider: (i) whether the client would object to the disclosure; (ii) whether the client would be harmed by the disclosure; and (iii) whether reporting the theft would benefit the client by assisting in ending the breach or recovering stolen information. Even then, without consent, the lawyer may disclose only such information as is reasonably necessary to assist in stopping the breach or recovering the stolen information.

C. Lawyer's Obligations to Provide Notice of Data Breach

When a lawyer knows or reasonably should know a data breach has occurred, the lawyer must evaluate notice obligations. Due to record retention requirements of Model Rule 1.15, information compromised by the data breach may belong or relate to the representation of a current client or former client.³⁰ We address each below.

1. Current Client

Communications between a lawyer and current client are addressed generally in Model Rule 1.4. Rule 1.4(a)(3) provides that a lawyer must “keep the client reasonably informed about the status of the matter.” Rule 1.4(b) provides: “A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.” Under these provisions, an obligation exists for a lawyer to communicate with current clients about a data breach.³¹

²⁹ ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 01-421(2001) (disclosures to insurer in bills when lawyer representing insured).

³⁰ This opinion addresses only obligations to clients and former clients. Data breach, as used in this opinion, is limited to client confidential information. We do not address ethical duties, if any, to third parties.

³¹ Relying on Rule 1.4 generally, the New York State Bar Committee on Professional Ethics concluded that a lawyer must notify affected clients of information lost through an online data storage provider. N.Y. State Bar Ass'n Op. 842 (2010) (Question 10: “If the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients' confidential information,

Our conclusion here is consistent with ABA Formal Ethics Opinion 95-398 where this Committee said that notice must be given to clients if a breach of confidentiality was committed by or through a third-party computer vendor or other service provider. There, the Committee concluded notice to the client of the breach may be required under 1.4(b) for a “serious breach.”³² The Committee advised:

Where the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Rule 1.4(b).³³

A data breach under this opinion involves the misappropriation, destruction or compromise of client confidential information, or a situation where a lawyer's ability to perform the legal services for which the lawyer was hired is significantly impaired by the event. Each of these scenarios is one where a client's interests have a reasonable possibility of being negatively impacted. When a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information a lawyer has a duty to notify the client of the breach. As noted in ABA Formal Opinion 95-398, a data breach requires notice to the client because such notice is an integral part of keeping a “client reasonably informed about the status of the matter” and the lawyer should provide information as would be “reasonably necessary to permit the client to make informed decisions regarding the representation” within the meaning of Model Rule 1.4.³⁴

The strong client protections mandated by Model Rule 1.1, 1.6, 5.1 and 5.3, particularly as they were amended in 2012 to account for risks associated with the use of technology, would be compromised if a lawyer who experiences a data breach that impacts client confidential information is permitted to hide those events from their clients. And in view of the duties imposed by these other Model Rules, Model Rule 1.4's requirement to keep clients “reasonably informed about the status” of a matter would ring hollow if a data breach was somehow excepted from this responsibility to communicate.

notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated.”) (*citations omitted*).

³² ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-398 (1995).

³³ *Id.*

³⁴ MODEL RULES OF PROF'L CONDUCT R. 1.4(b) (2018).

Model Rule 1.15(a) provides that a lawyer shall hold “property” of clients “in connection with a representation separate from the lawyer’s own property.” Funds must be kept in a separate account, and “[o]ther property shall be identified as such and appropriately safeguarded.” Model Rule 1.15(a) also provides that, “Complete records of such account funds and other property shall be kept by the lawyer” Comment [1] to Model Rule 1.15 states:

A lawyer should hold property of others with the care required of a professional fiduciary. Securities should be kept in a safe deposit box, except when some other form of safekeeping is warranted by special circumstances. All property that is the property of clients or third persons, including prospective clients, must be kept separate from the lawyer’s business and personal property.

An open question exists whether Model Rule 1.15’s reference to “property” includes information stored in electronic form. Comment [1] uses as examples “securities” and “property” that should be kept separate from the lawyer’s “business and personal property.” That language suggests Rule 1.15 is limited to tangible property which can be physically segregated. On the other hand, many courts have moved to electronic filing and law firms routinely use email and electronic document formats to image or transfer information. Reading Rule 1.15’s safeguarding obligation to apply to hard copy client files but not electronic client files is not a reasonable reading of the Rule.

Jurisdictions that have addressed the issue are in agreement. For example, Arizona Ethics Opinion 07-02 concluded that client files may be maintained in electronic form, with client consent, but that lawyers must take reasonable precautions to safeguard the data under the duty imposed in Rule 1.15. The District of Columbia Formal Ethics Opinion 357 concluded that, “Lawyers who maintain client records solely in electronic form should take reasonable steps (1) to ensure the continued availability of the electronic records in an accessible form during the period for which they must be retained and (2) to guard against the risk of unauthorized disclosure of client information.”

The Committee has engaged in considerable discussion over whether Model Rule 1.15 and, taken together, the technology amendments to Rules 1.1, 1.6, and 5.3 impliedly impose an obligation on a lawyer to notify a current client of a data breach. We do not have to decide that question in the absence of concrete facts. We reiterate, however, the obligation to inform the client does exist under Model Rule 1.4.

2. Former Client

Model Rule 1.9(c) requires that “A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter . . . reveal information relating to the representation except as these Rules would permit or require with respect to a client.”³⁵ When electronic “information relating to the representation” of a former client is subject to unauthorized access, disclosure, or destruction, the Model Rules provide no direct guidance on a lawyer’s obligation to notify the former client. Rule 1.9(c) provides that a lawyer “shall not . . . reveal” the former client’s information. It does not describe what steps, if any, a lawyer should take if such information is revealed. The Committee is unwilling to require notice to a former client as a matter of legal ethics in the absence of a black letter provision requiring such notice.³⁶

Nevertheless, we note that clients can make an informed waiver of the protections in Rule 1.9.³⁷ We also note that Rule 1.16(d) directs that lawyers should return “papers and property” to clients at the conclusion of the representation, which has commonly been understood to include the client’s file, in whatever form it is held. Rule 1.16(d) also has been interpreted as permitting lawyers to establish appropriate data destruction policies to avoid retaining client files and property indefinitely.³⁸ Therefore, as a matter of best practices, lawyers are encouraged to reach agreement with clients before conclusion, or at the termination, of the relationship about how to handle the client’s electronic information that is in the lawyer’s possession.

Absent an agreement with the former client lawyers are encouraged to adopt and follow a paper and electronic document retention schedule, which meets all applicable laws and rules, to reduce the amount of information relating to the representation of former clients that the lawyers retain. In addition, lawyers should recognize that in the event of a data breach involving former client information, data privacy laws, common law duties of care, or contractual arrangements with

³⁵ MODEL RULES OF PROF’L CONDUCT R. 1.9(c)(2) (2018).

³⁶ See *Discipline of Feland*, 2012 ND 174, ¶ 19, 820 N.W.2d 672 (Rejecting respondent’s argument that the court should engraft an additional element of proof in a disciplinary charge because “such a result would go beyond the clear language of the rule and constitute amendatory rulemaking within an ongoing disciplinary proceeding.”).

³⁷ See MODEL RULES OF PROF’L CONDUCT R. 1.9, cmt. [9] (2018).

³⁸ See ABA Ethics Search Materials on Client File Retention, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/piles_of_files_2008.pdf (last visited Oct.15, 2018).

the former client relating to records retention, may mandate notice to former clients of a data breach. A prudent lawyer will consider such issues in evaluating the response to the data breach in relation to former clients.³⁹

3. Breach Notification Requirements

The nature and extent of the lawyer's communication will depend on the type of breach that occurs and the nature of the data compromised by the breach. Unlike the "safe harbor" provisions of Comment [18] to Model Rule 1.6, if a post-breach obligation to notify is triggered, a lawyer must make the disclosure irrespective of what type of security efforts were implemented prior to the breach. For example, no notification is required if the lawyer's office file server was subject to a ransomware attack but no information relating to the representation of a client was inaccessible for any material amount of time, or was not accessed by or disclosed to unauthorized persons. Conversely, disclosure will be required if material client information was actually or reasonably suspected to have been accessed, disclosed or lost in a breach.

The disclosure must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything. In a data breach scenario, the minimum disclosure required to all affected clients under Rule 1.4 is that there has been unauthorized access to or disclosure of their information, or that unauthorized access or disclosure is reasonably suspected of having occurred. Lawyers must advise clients of the known or reasonably ascertainable extent to which client information was accessed or disclosed. If the lawyer has made reasonable efforts to ascertain the extent of information affected by the breach but cannot do so, the client must be advised of that fact.

In addition, and as a matter of best practices, a lawyer also should inform the client of the lawyer's plan to respond to the data breach, from efforts to recover information (if feasible) to steps being taken to increase data security.

The Committee concludes that lawyers have a continuing duty to keep clients reasonably apprised of material developments in post-breach investigations affecting the clients'

³⁹ Cf. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018), at 8-10 (discussing obligations regarding client files lost or destroyed during disasters like hurricanes, floods, tornadoes, and fires).

information.⁴⁰ Again, specific advice on the nature and extent of follow up communications cannot be provided in this opinion due to the infinite number of variable scenarios.

If personally identifiable information of clients or others is compromised as a result of a data breach, the lawyer should evaluate the lawyer's obligations under state and federal law. All fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have statutory breach notification laws.⁴¹ Those statutes require that private or governmental entities notify individuals of breaches involving loss or disclosure of personally identifiable information.⁴² Most breach notification laws specify who must comply with the law, define "personal information," define what constitutes a breach, and provide requirements for notice.⁴³ Many federal and state agencies also have confidentiality and breach notification requirements.⁴⁴ These regulatory schemes have the potential to cover individuals who meet particular statutory notice triggers, irrespective of the individual's relationship with the lawyer. Thus, beyond a Rule 1.4 obligation, lawyers should evaluate whether they must provide a statutory or regulatory data breach notification to clients or others based upon the nature of the information in the lawyer's possession that was accessed by an unauthorized user.⁴⁵

III. Conclusion

Even lawyers who, (i) under Model Rule 1.6(c), make "reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," (ii) under Model Rule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data

⁴⁰ State Bar of Mich. Op. RI-09 (1991).

⁴¹ National Conference of State Legislatures, *Security Breach Notification Laws* (Sept. 29, 2018), <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

⁴² *Id.*

⁴³ *Id.*

⁴⁴ ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 65.

⁴⁵ Given the broad scope of statutory duties to notify, lawyers would be well served to actively manage the amount of confidential and or personally identifiable information they store beyond any ethical, statutory, or other legal obligation to do so. Lawyers should implement, and follow, a document retention policy that comports with Model Rule 1.15 and evaluate ways to limit receipt, possession and/or retention of confidential or personally identifiable information during or after an engagement.

breach under Model Rule 1.4 in sufficient detail to keep clients “reasonably informed” and with an explanation “to the extent necessary to permit the client to make informed decisions regarding the representation.”

AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

321 N. Clark Street, Chicago, Illinois 60654-4714 Telephone (312) 988-5328

CHAIR: Barbara S. Gillers, New York, NY ■ John M. Barkett, Miami, FL ■ Wendy Wen Yun Chang, Los Angeles, CA ■ Hon. Daniel J. Crothers, Bismarck, ND ■ Keith R. Fisher, Arlington, VA ■ Douglas R. Richmond, Chicago, IL ■ Michael H. Rubin, Baton Rouge, LA ■ Lynda Shely, Scottsdale, AZ ■ Elizabeth C. Tarbert, Tallahassee, FL. ■ Allison Wood, Chicago, IL

CENTER FOR PROFESSIONAL RESPONSIBILITY: Dennis A. Rendleman, Ethics Counsel

©2018 by the American Bar Association. All rights reserved.

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 internet 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.

I. Introduction

In Formal Opinion 99-413 this Committee addressed a lawyer's confidentiality obligations for email communications with clients. While the basic obligations of confidentiality remain applicable today, the role and risks of technology in the practice of law have evolved since 1999 prompting the need to update Opinion 99-413.

Formal Opinion 99-413 concluded: "Lawyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure. It therefore follows that its use is consistent with the duty under Rule 1.6 to use reasonable means to maintain the confidentiality of information relating to a client's representation."¹

Unlike 1999 where multiple methods of communication were prevalent, today, many lawyers primarily use electronic means to communicate and exchange documents with clients, other lawyers, and even with other persons who are assisting a lawyer in delivering legal services to clients.²

Since 1999, those providing legal services now regularly use a variety of devices to create, transmit and store confidential communications, including desktop, laptop and notebook

*The opinion below is a revision of, and replaces Formal Opinion 477 as issued by the Committee May 11, 2017. This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2016. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

1. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413, at 11 (1999).

2. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008); ABA COMMISSION ON ETHICS 20/20 REPORT TO THE HOUSE OF DELEGATES (2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_resolution_and_report_outsourcing_posting.authcheckdam.pdf.

computers, tablet devices, smartphones, and cloud resource and storage locations. Each device and each storage location offer an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicate a lawyer's ethical duties.³

In 2012 the ABA adopted "technology amendments" to the Model Rules, including updating the Comments to Rule 1.1 on lawyer technological competency and adding paragraph (c) and a new Comment to Rule 1.6, addressing a lawyer's obligation to take reasonable measures to prevent inadvertent or unauthorized disclosure of information relating to the representation.

At the same time, the term "cybersecurity" has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the internet. Cybersecurity recognizes a post-Opinion 99-413 world where law enforcement discusses hacking and data loss in terms of "when," and not "if."⁴ Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.⁵

The Model Rules do not impose greater or different duties of confidentiality based upon the method by which a lawyer communicates with a client. But how a lawyer should comply with the core duty of confidentiality in an ever-changing technological world requires some reflection.

Against this backdrop we describe the "technology amendments" made to the Model Rules in 2012, identify some of the technology risks lawyers face, and discuss factors other than the Model Rules of Professional Conduct that lawyers should consider when using electronic means to communicate regarding client matters.

II. Duty of Competence

Since 1983, Model Rule 1.1 has read: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."⁶ The scope of this requirement was

3. See JILL D. RHODES & VINCENT I. POLLEY, *THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS* 7 (2013) [hereinafter *ABA CYBERSECURITY HANDBOOK*].

4. "Cybersecurity" is defined as "measures taken to protect a computer or computer system (as on the internet) against unauthorized access or attack." CYBERSECURITY, MERRIAM WEBSTER, <http://www.merriam-webster.com/dictionary/cybersecurity> (last visited Sept. 10, 2016). In 2012 the ABA created the Cybersecurity Legal Task Force to help lawyers grapple with the legal challenges created by cyberspace. In 2013 the Task Force published *The ABA Cybersecurity Handbook: A Resource For Attorneys, Law Firms, and Business Professionals*.

5. Bradford A. Bleier, Unit Chief to the Cyber National Security Section in the FBI's Cyber Division, indicated that "[l]aw firms have tremendous concentrations of really critical private information, and breaking into a firm's computer system is a really optimal way to obtain economic and personal security information." Ed Finkel, *Cyberspace Under Siege*, A.B.A. J., Nov. 1, 2010.

6. A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 37-44 (Art Garwin ed., 2013).

clarified in 2012 when the ABA recognized the increasing impact of technology on the practice of law and the duty of lawyers to develop an understanding of that technology. Thus, Comment [8] to Rule 1.1 was modified to read:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)⁷

Regarding the change to Rule 1.1's Comment, the ABA Commission on Ethics 20/20 explained:

Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to “keep abreast of changes in the law and its practice.” The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document.⁸

III. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the rule and the commentary about what efforts are required to preserve the confidentiality of information relating to the representation. Model Rule 1.6(a) requires that “A lawyer shall not reveal information relating to the representation of a client” unless certain circumstances arise.⁹ The 2012 modification added a new duty in paragraph (c) that: “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.”¹⁰

7. *Id.* at 43.

8. ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer's substantive duty of competence: “Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase ‘including the benefits and risks associated with relevant technology,’ would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent.”

9. MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2016).

10. *Id.* at (c).

Amended Comment [18] explains:

Paragraph (c) 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 (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

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.¹¹

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

. . . 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.¹²

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

- the sensitivity of the information,

11. The 20/20 Commission's report emphasized that lawyers are not the guarantors of data safety. It wrote: "[t]o be clear, paragraph (c) does not mean that a lawyer engages in professional misconduct any time a client's confidences are subject to unauthorized access or disclosed inadvertently or without authority. A sentence in Comment [16] makes this point explicitly. The reality is that disclosures can occur even if lawyers take all reasonable precautions. The Commission, however, believes that it is important to state in the black letter of Model Rule 1.6 that lawyers have a duty to take reasonable precautions, even if those precautions will not guarantee the protection of confidential information under all circumstances."

12. ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 48-49.

- 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).¹³

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 the technological landscape of Opinion 99-413, and due to the reasonable expectations of privacy available to email communications at the time, unencrypted email posed no greater risk of interception or disclosure than other non-electronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic security measures.¹⁴ Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication.

However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable.

13. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2016). "The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available." ABA COMMISSION REPORT 105A, *supra* note 8, at 5.

14. See item 3 below.

While it is beyond the scope of an ethics opinion to specify the reasonable steps that lawyers should take under any given set of facts, we offer the following considerations as guidance:

1. Understand the Nature of the Threat.

Understanding the nature of the threat includes consideration of the sensitivity of a client's information and whether the client's matter is a higher risk for cyber intrusion. Client matters involving proprietary information in highly sensitive industries such as industrial designs, mergers and acquisitions or trade secrets, and industries like healthcare, banking, defense or education, may present a higher risk of data theft.¹⁵ "Reasonable efforts" in higher risk scenarios generally means that greater effort is warranted.

2. Understand How Client Confidential Information is Transmitted and Where It Is Stored.

A lawyer should understand how their firm's electronic communications are created, where client data resides, and what avenues exist to access that information. Understanding these processes will assist a lawyer in managing the risk of inadvertent or unauthorized disclosure of client-related information. Every access point is a potential entry point for a data loss or disclosure. The lawyer's task is complicated in a world where multiple devices may be used to communicate with or about a client and then store those communications. Each access point, and each device, should be evaluated for security compliance.

3. Understand and Use Reasonable Electronic Security Measures.

Model Rule 1.6(c) requires a lawyer to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. As Comment [18] makes clear, what is deemed to be "reasonable" may vary, depending on the facts and circumstances of each case. Electronic disclosure of, or access to, client communications can occur in different forms ranging from a direct intrusion into a law firm's systems to theft or interception of information during the transmission process. Making reasonable efforts to protect against unauthorized disclosure in client communications thus includes analysis of security measures applied to both disclosure and access to a law firm's technology system and transmissions.

A lawyer should understand and use electronic security measures to safeguard client communications and information. A lawyer has a variety of options to safeguard communications including, for example, using secure internet access methods to communicate, access and store client information (such as through secure Wi-Fi, the use of a Virtual Private Network, or another secure internet portal), using unique complex

15. See, e.g., Noah Garner, *The Most Prominent Cyber Threats Faced by High-Target Industries*, TREND-MICRO (Jan. 25, 2016), <http://blog.trendmicro.com/the-most-prominent-cyber-threats-faced-by-high-target-industries/>.

passwords, changed periodically, implementing firewalls and anti-Malware/Anti-Spyware/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software. Each of these measures is routinely accessible and reasonably affordable or free. Lawyers may consider refusing access to firm systems to devices failing to comply with these basic methods. It also may be reasonable to use commonly available methods to remotely disable lost or stolen devices, and to destroy the data contained on those devices, especially if encryption is not also being used.

Other available tools include encryption of data that is physically stored on a device and multi-factor authentication to access firm systems.

In the electronic world, “delete” usually does not mean information is permanently deleted, and “deleted” data may be subject to recovery. Therefore, a lawyer should consider whether certain data should *ever* be stored in an unencrypted environment, or electronically transmitted at all.

4. Determine How Electronic Communications About Clients Matters Should Be Protected.

Different communications require different levels of protection. At the beginning of the client-lawyer relationship, the lawyer and client should discuss what levels of security will be necessary for each electronic communication about client matters. Communications to third parties containing protected client information requires analysis to determine what degree of protection is appropriate. In situations where the communication (and any attachments) are sensitive or warrant extra security, additional electronic protection may be required. For example, if client information is of sufficient sensitivity, a lawyer should encrypt the transmission and determine how to do so to sufficiently protect it,¹⁶ and consider the use of password protection for any attachments. Alternatively, lawyers can consider the use of a well vetted and secure third-party cloud based file storage system to exchange documents normally attached to emails.

Thus, routine communications sent electronically are those communications that do not contain information warranting additional security measures beyond basic methods. However, in some circumstances, a client’s lack of technological sophistication or the limitations of technology available to the client may require alternative non-electronic forms of communication altogether.

16. See Cal. Formal Op. 2010-179 (2010); ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 121. Indeed, certain laws and regulations require encryption in certain situations. *Id.* at 58-59.

A lawyer also should be cautious in communicating with a client if the client uses computers or other devices subject to the access or control of a third party.¹⁷ If so, the attorney-client privilege and confidentiality of communications and attached documents may be waived. Therefore, the lawyer should warn the client about the risk of sending or receiving electronic communications using a computer or other device, or email account, to which a third party has, or may gain, access.¹⁸

5. Label Client Confidential Information.

Lawyers should follow the better practice of marking privileged and confidential client communications as “privileged and confidential” in order to alert anyone to whom the communication was inadvertently disclosed that the communication is intended to be privileged and confidential. This can also consist of something as simple as appending a message or “disclaimer” to client emails, where such a disclaimer is accurate and appropriate for the communication.¹⁹

Model Rule 4.4(b) obligates a lawyer who “knows or reasonably should know” that he has received an inadvertently sent “document or electronically stored information relating to the representation of the lawyer’s client” to promptly notify the sending lawyer. A clear and conspicuous appropriately used disclaimer may affect whether a recipient lawyer’s duty under Model Rule 4.4(b) for inadvertently transmitted communications is satisfied.

17. ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 11-459, Duty to Protect the Confidentiality of E-mail Communications with One’s Client (2011). Formal Op. 11-459 was issued prior to the 2012 amendments to Rule 1.6. These amendments added new Rule 1.6(c), which provides that lawyers “shall” make reasonable efforts to prevent the unauthorized or inadvertent access to client information. *See, e.g.*, Scott v. Beth Israel Med. Center, Inc., Civ. A. No. 3:04-CV-139-RJC-DCK, 847 N.Y.S.2d 436 (Sup. Ct. 2007); Mason v. ILS Tech., LLC, 2008 WL 731557, 2008 BL 298576 (W.D.N.C. 2008); Holmes v. Petrovich Dev Co., LLC, 191 Cal. App. 4th 1047 (2011) (employee communications with lawyer over company owned computer not privileged); Bingham v. BayCare Health Sys., 2016 WL 3917513, 2016 BL 233476 (M.D. Fla. July 20, 2016) (collecting cases on privilege waiver for privileged emails sent or received through an employer’s email server).

18. Some state bar ethics opinions have explored the circumstances under which email communications should be afforded special security protections. *See, e.g.*, Tex. Prof’l Ethics Comm. Op. 648 (2015) that identified six situations in which a lawyer should consider whether to encrypt or use some other type of security precaution:

- communicating highly sensitive or confidential information via email or unencrypted email connections;
- sending an email to or from an account that the email sender or recipient shares with others;
- sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client’s work email account, especially if the email relates to a client’s employment dispute with his employer...;
- sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;
- sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
- sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer’s email communication, with or without a warrant.

19. *See* Veteran Med. Prods. v. Bionix Dev. Corp., Case No. 1:05-cv-655, 2008 WL 696546 at *8, 2008 BL 51876 at *8 (W.D. Mich. Mar. 13, 2008) (email disclaimer that read “this email and any files transmitted with are confidential and are intended solely for the use of the individual or entity to whom they are addressed” with nondisclosure constitutes a reasonable effort to maintain the secrecy of its business plan).

6. Train Lawyers and Nonlawyer Assistants in Technology and Information Security.

Model Rule 5.1 provides that 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. Model Rule 5.1 also provides that lawyers having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct. In addition, Rule 5.3 requires lawyers who are responsible for managing and supervising nonlawyer assistants to take reasonable steps to reasonably assure that the conduct of such assistants is compatible with the ethical duties of the lawyer. These requirements are as applicable to electronic practices as they are to comparable office procedures.

In the context of electronic communications, lawyers must establish policies and procedures, and periodically train employees, subordinates and others assisting in the delivery of legal services, in the use of reasonably secure methods of electronic communications with clients. Lawyers also must instruct and supervise on reasonable measures for access to and storage of those communications. Once processes are established, supervising lawyers must follow up to ensure these policies are being implemented and partners and lawyers with comparable managerial authority must periodically reassess and update these policies. This is no different than the other obligations for supervision of office practices and procedures to protect client information.

7. Conduct Due Diligence on Vendors Providing Communication Technology.

Consistent with Model Rule 1.6(c), Model Rule 5.3 imposes a duty on lawyers with direct supervisory authority over a nonlawyer to make “reasonable efforts to ensure that” the nonlawyer’s “conduct is compatible with the professional obligations of the lawyer.”

In ABA Formal Opinion 08-451, this Committee analyzed Model Rule 5.3 and a lawyer’s obligation when outsourcing legal and nonlegal services. That opinion identified several issues a lawyer should consider when selecting the outsource vendor, to meet the lawyer’s due diligence and duty of supervision. Those factors also apply in the analysis of vendor selection in the context of electronic communications. Such factors may include:

- reference checks and vendor credentials;
- vendor’s security policies and protocols;
- vendor’s hiring practices;
- the use of confidentiality agreements;
- vendor’s conflicts check system to screen for adversity; and

- the availability and accessibility of a legal forum for legal relief for violations of the vendor agreement.

Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.²⁰

Since the issuance of Formal Opinion 08-451, Comment [3] to Model Rule 5.3 was added to address outsourcing, including “using an Internet-based service to store client information.” Comment [3] provides that the “reasonable efforts” required by Model Rule 5.3 to ensure that the nonlawyer’s services are provided in a manner that is compatible with the lawyer’s professional obligations “will depend upon the circumstances.” Comment [3] contains suggested factors that might be taken into account:

- the education, experience, and reputation of the nonlawyer;
- the nature of the services involved;
- the terms of any arrangements concerning the protection of client information; and
- the legal and ethical environments of the jurisdictions in which the services will be performed particularly with regard to confidentiality.

Comment [3] further provides that when retaining or directing a nonlawyer outside of the firm, lawyers should communicate “directions appropriate under the circumstances to give reasonable assurance that the nonlawyer’s conduct is compatible with the professional obligations of the lawyer.”²¹ If the client has not directed the selection of the outside nonlawyer vendor, the lawyer has the responsibility to monitor how those services are being performed.²²

Even after a lawyer examines these various considerations and is satisfied that the security employed is sufficient to comply with the duty of confidentiality, the lawyer must periodically reassess these factors to confirm that the lawyer’s actions continue to comply with the ethical obligations and have not been rendered inadequate by changes in circumstances or technology.

20. MODEL RULES OF PROF’L CONDUCT R. 1.1 cmts. [2] & [8] (2016).

21. The ABA’s catalog of state bar ethics opinions applying the rules of professional conduct to cloud storage arrangements involving client information can be found at: http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.

22. By contrast, where a client directs the selection of a particular nonlawyer service provider outside the firm, “the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer.” MODEL RULES OF PROF’L CONDUCT R. 5.3 cmt. [4] (2016). The concept of monitoring recognizes that although it may not be possible to “directly supervise” a client directed nonlawyer outside the firm performing services in connection with a matter, a lawyer must nevertheless remain aware of how the nonlawyer services are being performed. ABA COMMISSION ON ETHICS 20/20 REPORT 105C, at 12 (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105c_filed_may_2012.auth_checkdam.pdf.

IV. Duty to Communicate

Communications between a lawyer and client generally are addressed in Rule 1.4. When the lawyer reasonably believes that highly sensitive confidential client information is being transmitted so that extra measures to protect the email transmission are warranted, the lawyer should inform the client about the risks involved.²³ The lawyer and client then should decide whether another mode of transmission, such as high level encryption or personal delivery is warranted. Similarly, a lawyer should consult with the client as to how to appropriately and safely use technology in their communication, in compliance with other laws that might be applicable to the client. Whether a lawyer is using methods and practices to comply with administrative, statutory, or international legal standards is beyond the scope of this opinion.

A client may insist or require that the lawyer undertake certain forms of communication. As explained in Comment [19] to Model Rule 1.6, “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.”

V. Conclusion

Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make “reasonable efforts” to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.

A lawyer generally may transmit information relating to the representation of a client over the internet 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.

AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

321 N. Clark Street, Chicago, Illinois 60654-4714 Telephone (312) 988-5328

CHAIR: Myles V. Lynk, Tempe, AZ ■ John M. Barkett, Miami, FL ■ Arthur D. Burger, Washington, DC ■ Wendy Wen Yun Chang, Los Angeles, CA ■ Robert A. Creamer, Cambridge, MA ■ Hon. Daniel J. Crothers, Bismarck, ND ■ Keith R. Fisher, Arlington, VA ■ Douglas R. Richmond, Chicago, IL ■ Hope Cahill Todd, Washington, DC ■ Allison Wood, Chicago, IL

CENTER FOR PROFESSIONAL RESPONSIBILITY: Dennis A. Rendleman, Ethics Counsel; Mary McDermott, Associate Ethics Counsel

©2017 by the American Bar Association. All rights reserved.

23. MODEL RULES OF PROF'L CONDUCT R. 1.4(a)(1) & (4) (2016).



The Data Protection Act

In 2017, 61 percent of small businesses experienced a cyberattack.

Small- to medium-sized businesses spent an average of \$1 million because of damage from cyberattacks in 2017.

An average data breach of a small- to medium-sized business involves 9,000 individual records.



Source: "2017 State of Cybersecurity in Small & Medium-Sized Businesses" by Ponemon Institute

The Data Protection Act is the first piece of legislation introduced as a result of Ohio Attorney General Mike DeWine's CyberOhio Initiative. Gov. John Kasich signed the act, Senate Bill 220, into law in August 2018. The law encourages businesses to voluntarily adopt strong cybersecurity practices to protect consumer data.

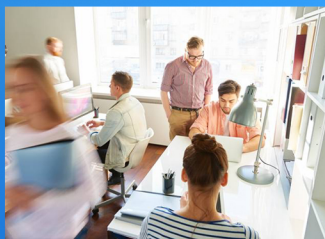
The Data Protection Act specifies industry-recognized security frameworks for Ohio businesses to incorporate into their cybersecurity policies. Effective protections save customers from the expense, embarrassment, and harm caused by having their personal information compromised. The act does not create a minimum cybersecurity standard

and is intended to be an incentive for businesses to achieve a higher level of cybersecurity through voluntary action. If a business has a cybersecurity program that meets one of the act's requirements, it is eligible to use the affirmative defense in the event of a lawsuit from the result of a data breach.



Affirmative defense

The purpose of the act is to provide an affirmative defense to a lawsuit that alleges a data breach was caused by a business' failure to implement reasonable information-security controls. *(An affirmative defense allows a defendant to introduce evidence, that if found credible, can negate civil liability, even if the allegations are true.)*



Flexible programs

Under this act, a cybersecurity program is scalable to each business based on:

- Size
- Complexity
- Nature
- Cost
- Resources

Supported security frameworks

The cybersecurity frameworks incorporated into the act:

- National Institute of Standards and Technology (NIST)
- Federal Risk and Authorization Management Program (FedRAMP)
- Center for Internet Security (CIS) Controls
- International Organization for Standardization (ISO) 27000
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm–Leach–Bliley Act (GLBA)
- Federal Information Security Management Act (FISMA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Payment Card Industry Data Security Standard (PCI DSS)

Launched in 2016, the goal of CyberOhio is to help foster a legal, technical, and collaborative cybersecurity environment to help Ohio businesses thrive. In addition to promoting legislation, other parts of the initiative include training opportunities for businesses, development of cybersecurity workforce personnel, and expansion of the Ohio Attorney General's Identity Theft Unit.



MIKE DEWINE
OHIO ATTORNEY GENERAL

www.OhioAttorneyGeneral.gov

For more information, contact **CyberOhio@OhioAttorneyGeneral.gov** or call **800-282-0515**.



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

**ETHICAL OBLIGATIONS FOR ATTORNEYS USING CLOUD COMPUTING/
SOFTWARE AS A SERVICE WHILE FULFILLING THE DUTIES OF
CONFIDENTIALITY AND PRESERVATION OF CLIENT PROPERTY**

FORMAL OPINION 2011-200

I. Introduction and Summary

If an attorney uses a Smartphone or an iPhone, or uses web-based electronic mail (e-mail) such as Gmail, Yahoo!, Hotmail or AOL Mail, or uses products such as Google Docs, Microsoft Office 365 or Dropbox, the attorney is using “cloud computing.” While there are many technical ways to describe cloud computing, perhaps the best description is that cloud computing is merely “a fancy way of saying stuff’s not on your computer.”¹

From a more technical perspective, “cloud computing” encompasses several similar types of services under different names and brands, including: web-based e-mail, online data storage, software-as-a-service (“SaaS”), platform-as-a-service (“PaaS”), infrastructure-as-a-service (“IaaS”), Amazon Elastic Cloud Compute (“Amazon EC2”), and Google Docs.

This opinion places all such software and services under the “cloud computing” label, as each raises essentially the same ethical issues. In particular, the central question posed by “cloud computing” may be summarized as follows:

May an attorney ethically store confidential client material in “the cloud”?

In response to this question, this Committee concludes:

Yes. 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 such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks.

In recent years, technological advances have occurred that have dramatically changed the way attorneys and law firms store, retrieve and access client information. Many law firms view these

¹ Quinn Norton, “Byte Rights,” *Maximum PC*, September 2010, at 12.

technological advances as an opportunity to reduce costs, improve efficiency and provide better client service. Perhaps no area has seen greater changes than “cloud computing,” which refers to software and related services that store information on a remote computer, *i.e.*, a computer or server that is not located at the law office’s physical location. Rather, the information is stored on another company’s server, or many servers, possibly all over the world, and the user’s computer becomes just a way of accessing the information.²

The advent of “cloud computing,” as well as the use of electronic devices such as cell phones that take advantage of cloud services, has raised serious questions concerning the manner in which lawyers and law firms handle client information, and has been the subject of numerous ethical inquiries in Pennsylvania and throughout the country. The American Bar Association Commission on Ethics 20/20 has suggested changes to the Model Rules of Professional Conduct designed to remind lawyers of the need to safeguard client confidentiality when engaging in “cloud computing.”

Recent “cloud” data breaches from multiple companies, causing millions of dollars in penalties and consumer redress, have increased concerns about data security for cloud services. The Federal Trade Commission (“FTC”) has received complaints that inadequate cloud security is placing consumer data at risk, and it is currently studying the security of “cloud computing” and the efficacy of increased regulation. Moreover, the Federal Bureau of Investigations (“FBI”) warned law firms in 2010 that they were being specifically targeted by hackers who have designs on accessing the firms’ databases.

This Committee has also considered the client confidentiality implications for electronic document transmission and storage in Formal Opinions 2009-100 (“Metadata”) and 2010-200 (“Virtual Law Offices”), and an informal Opinion directly addressing “cloud computing.” Because of the importance of “cloud computing” to attorneys – and the potential impact that this technological advance may have on the practice of law – this Committee believes that it is appropriate to issue this Formal Opinion to provide guidance to Pennsylvania attorneys concerning their ethical obligations when utilizing “cloud computing.”

This Opinion also includes a section discussing the specific implications of web-based electronic mail (e-mail). With regard to web-based email, *i.e.*, products such as Gmail, AOL Mail, Yahoo! and Hotmail, the Committee concludes that attorneys may use e-mail but that, when circumstances require, attorneys must take additional precautions to assure the confidentiality of client information transmitted electronically.

II. Background

For lawyers, “cloud computing” may be desirable because it can provide costs savings and increased efficiency in handling voluminous data. Better still, cloud service is elastic, and users can have as much or as little of a service as they want at any given time. The service is sold on demand, typically by the minute, hour or other increment. Thus, for example, with “cloud computing,” an attorney can simplify document management and control costs.

² *Id.*

The benefits of using “cloud computing” may include:

- Reduced infrastructure and management;
- Cost identification and effectiveness;
- Improved work production;
- Quick, efficient communication;
- Reduction in routine tasks, enabling staff to elevate work level;
- Constant service;
- Ease of use;
- Mobility;
- Immediate access to updates; and
- Possible enhanced security.

Because “cloud computing” refers to “offsite” storage of client data, much of the control over that data and its security is left with the service provider. Further, data may be stored in other jurisdictions that have different laws and procedures concerning access to or destruction of electronic data. Lawyers using cloud services must therefore be aware of potential risks and take appropriate precautions to prevent compromising client confidentiality, *i.e.*, attorneys must take great care to assure that any data stored offsite remains confidential and not accessible to anyone other than those persons authorized by their firms. They must also assure that the jurisdictions in which the data are physical stored do not have laws or rules that would permit a breach of confidentiality in violation of the Rules of Professional Conduct.

III. Discussion

A. Prior Pennsylvania Opinions

In Formal Opinion 2009-100, this Committee concluded that a transmitting attorney has a duty of reasonable care to remove unwanted metadata from electronic documents before sending them to an adverse or third party. Metadata is hidden information contained in an electronic document that is not ordinarily visible to the reader. The Committee also concluded, *inter alia*, that a receiving lawyer has a duty pursuant to RPC 4.4(b) to notify the transmitting lawyer if an inadvertent metadata disclosure occurs.

Formal Opinion 2010-200 advised that an attorney with a virtual law office “is under the same obligation to maintain client confidentiality as is the attorney in a traditional physical office.” Virtual law offices generally are law offices that do not have traditional brick and mortar facilities. Instead, client communications and file access exist entirely online. This Committee also concluded that attorneys practicing in a virtual law office need not take additional precautions beyond those utilized by traditional law offices to ensure confidentiality, because virtual law firms and many brick-and-mortar firms use electronic filing systems and incur the same or similar risks endemic to accessing electronic files remotely.

Informal Opinion 2010-060 on “cloud computing” stated that an attorney may ethically allow client confidential material to be stored in “the cloud” provided the attorney makes reasonable efforts to protect confidential electronic communications and information. Reasonable efforts

discussed include regularly backing up data, installing firewalls, and avoiding inadvertent disclosures.

B. Pennsylvania Rules of Professional Conduct

An attorney using “cloud computing” is under the same obligation to maintain client confidentiality as is the attorney who uses offline documents management. While no Pennsylvania Rule of Profession Conduct specifically addresses “cloud computing,” the following rules, *inter alia*, are implicated:

Rule 1.0 (“Terminology”);
Rule 1.1 (“Competence”);
Rule 1.4 (“Communication”);
Rule 1.6 (“Confidentiality of Information”);
Rule 1.15 (“Safekeeping Property”); and
Rule 5.3 (“Responsibilities Regarding Nonlawyer Assistants”).

Rule 1.1 (“Competence”) states:

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

Comment [5] (“Thoroughness and Preparation”) of Rule 1.1 provides further guidance about an attorney’s obligations to clients that extend beyond legal skills:

Competent handling of particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. ...

Competency is affected by the manner in which an attorney chooses to represent his or her client, or, as Comment [5] to Rule 1.1 succinctly puts it, an attorney’s “methods and procedures.” Part of a lawyer’s responsibility of competency is to take reasonable steps to ensure that client data and information is maintained, organized and kept confidential when required. A lawyer has latitude in choosing how or where to store files and use software that may best accomplish these goals. However, it is important that he or she is aware that some methods, like “cloud computing,” require suitable measures to protect confidential electronic communications and information. The risk of security breaches and even the complete loss of data in “cloud computing” is magnified because the security of any stored data is with the service provider. For example, in 2011, the syndicated children’s show “Zodiac Island” lost an entire season’s worth of episodes when a fired employee for the show’s data hosting service accessed the show’s content without authorization and wiped it out.³

³ Eriq Gardner, “Hacker Erased a Season’s Worth of ‘Zodiac Island’,” *Yahoo! TV* (March 31, 2011), available at http://tv.yahoo.com/news/article/tv-news.en.reuters.com/tv-news.en.reuters.com-20110331-us_zodiac

Rule 1.15 (“Safekeeping Property”) requires that client property should be “appropriately safeguarded.”⁴ Client property generally includes files, information and documents, including those existing electronically. Appropriate safeguards will vary depending on the nature and sensitivity of the property. Rule 1.15 provides in relevant part:

(b) A lawyer shall hold all Rule 1.15 Funds and property separate from the lawyer’s own property. Such property shall be identified and appropriately safeguarded.

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) The duty not to reveal information relating to representation of a client continues after the client-lawyer relationship has terminated.

Comment [2] of Rule 1.6 explains the importance and some of the foundation underlying the confidential relationship that lawyers must afford to a client. It is vital for the promotion of trust, justice and social welfare that a client can reasonably believe that his or her personal information or information related to a case is kept private and protected. Comment [2] explains the nature of the confidential attorney-client relationship:

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. See Rule 1.0(e) for the definition of informed consent. 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. ...

Also relevant is Rule 1.0(e) defining the requisite “Informed Consent”:

“Informed consent” denotes the consent by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct.

Rule 1.4 directs a lawyer to promptly inform the client of any decision with respect to which the client’s informed consent is required. While it is not necessary to communicate every minute

⁴ In previous Opinions, this Committee has noted that the intent of Rule 1.15 does not extend to the entirety of client files, information and documents, including those existing electronically. In light of the expansion of technology as a basis for storing client data, it would appear that the strictures of diligence required of counsel under Rule 1.15 are, at a minimum, analogous to the “cloud.”

detail of a client's representation, "adequate information" should be provided to the client so that the client understands the nature of the representation and "material risks" inherent in an attorney's methods. So for example, if an attorney intends to use "cloud computing" to manage a client's confidential information or data, it may be necessary, depending on the scope of representation and the sensitivity of the data involved, to inform the client of the nature of the attorney's use of "cloud computing" and the advantages as well as the risks endemic to online storage and transmission.

Absent a client's informed consent, as stated in Rule 1.6(a), confidential client information cannot be disclosed unless either it is "impliedly authorized" for the representation or enumerated among the limited exceptions in Rule 1.6(b) or Rule 1.6(c).⁵ This may mean that a third party vendor, as with "cloud computing," could be "impliedly authorized" to handle client data provided that the information remains confidential, is kept secure, and any disclosure is confined only to necessary personnel. It also means that various safeguards should be in place so that an attorney can be reasonably certain to protect any information that is transmitted, stored, accessed, or otherwise processed through cloud services. Comment [24] to Rule 1.6(a) further clarifies an attorney's duties and obligations:

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.

An attorney utilizing "cloud computing" will likely encounter circumstances that require unique considerations to secure client confidentiality. For example, because a server used by a "cloud computing" provider may physically be kept in another country, an attorney must ensure that the data in the server is protected by privacy laws that reasonably mirror those of the United States. Also, there may be situations in which the provider's ability to protect the information is compromised, whether through hacking, internal impropriety, technical failures, bankruptcy, or other circumstances. While some of these situations may also affect attorneys who use offline

⁵ The exceptions covered in Rule 1.6(b) and (c) are not implicated in "cloud computing." Generally, they cover compliance with Rule 3.3 ("Candor Toward the Tribunal"), the prevention of serious bodily harm, criminal and fraudulent acts, proceedings concerning the lawyer's representation of the client, legal advice sought for Rule compliance, and the sale of a law practice.

storage, an attorney using “cloud computing” services may need to take special steps to satisfy his or her obligation under Rules 1.0, 1.6 and 1.15.⁶

Rule 5.3 (“Responsibilities Regarding Nonlawyer Assistants”) 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.

At its essence, “cloud computing” can be seen as an online form of outsourcing subject to Rule 5.1 and Rule 5.3 governing the supervision of those who are associated with an attorney. Therefore, a lawyer must ensure that tasks are delegated to competent people and organizations. This means that any service provider who handles client information needs to be able to limit authorized access to the data to only necessary personnel, ensure that the information is backed up, reasonably available to the attorney, and reasonably safe from unauthorized intrusion.

It is also important that the vendor understands, embraces, and is obligated to conform to the professional responsibilities required of lawyers, including a specific agreement to comply with all ethical guidelines, as outlined below. Attorneys may also need a written service agreement that can be enforced on the provider to protect the client’s interests. In some circumstances, a client may need to be advised of the outsourcing or use of a service provider and the identification of the provider. A lawyer may also need an agreement or written disclosure with the client to outline the nature of the cloud services used, and its impact upon the client’s matter.

C. Obligations of Reasonable Care for Pennsylvania/Factors to Consider

⁶ Advisable steps for an attorney to take reasonable care to meet his or her obligations for Professional Conduct are outlined below.

In the context of “cloud computing,” an attorney must take reasonable care to make sure that the conduct of the cloud computing service provider conforms to the rules to which the attorney himself is subject. Because the operation is outside of an attorney’s direct control, some of the steps taken to ensure reasonable care are different from those applicable to traditional information storage.

While the measures necessary to protect confidential information will vary based upon the technology and infrastructure of each office – and this Committee acknowledges that the advances in technology make it difficult, if not impossible to provide specific standards that will apply to every attorney – there are common procedures and safeguards that attorneys should employ.

These various safeguards also apply to traditional law offices. 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. However, since cloud services are under the provider’s control, using “the cloud” to store data electronically could have unwanted consequences, such as interruptions in service or data loss. There are numerous examples of these types of events. Amazon EC2 has experienced outages in the past few years, leaving a portion of users without service for hours at a time. Google has also had multiple service outages, as have other providers. Digital Railroad, a photo archiving service, collapsed financially and simply shut down. These types of risks should alert anyone contemplating using cloud services to select a suitable provider, take reasonable precautions to back up data and ensure its accessibility when the user needs it.

Thus, the standard of reasonable care for “cloud computing” may include:

- Backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted;
- Installing a firewall to limit access to the firm’s network;
- Limiting information that is provided to others to what is required, needed, or requested;
- Avoiding inadvertent disclosure of information;
- Verifying the identity of individuals to whom the attorney provides confidential information;
- Refusing to disclose confidential information to unauthorized individuals (including family members and friends) without client permission;
- Protecting electronic records containing confidential data, including backups, by encrypting the confidential data;
- Implementing electronic audit trail procedures to monitor who is accessing the data;

- Creating plans to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data;
- Ensuring the provider:
 - explicitly agrees that it has no ownership or security interest in the data;
 - has an enforceable obligation to preserve security;
 - will notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider produces the requested information;
 - has technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing;
 - includes in its “Terms of Service” or “Service Level Agreement” an agreement about how confidential client information will be handled;
 - provides the firm with right to audit the provider’s security procedures and to obtain copies of any security audits performed;
 - will host the firm’s data only within a specified geographic area. If by agreement, the data are hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and Pennsylvania;
 - provides a method of retrieving data if the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity; and,
 - provides the ability for the law firm to get data “off” of the vendor’s or third party data hosting company’s servers for the firm’s own use or in-house backup offline.
- Investigating the provider’s:
 - security measures, policies and recovery methods;
 - system for backing up data;
 - security of data centers and whether the storage is in multiple centers;
 - safeguards against disasters, including different server locations;
 - history, including how long the provider has been in business;
 - funding and stability;
 - policies for data retrieval upon termination of the relationship and any related charges; and,
 - process to comply with data that is subject to a litigation hold.
- Determining whether:
 - data is in non-proprietary format;
 - the Service Level Agreement clearly states that the attorney owns the data;
 - there is a 3rd party audit of security; and,
 - there is an uptime guarantee and whether failure results in service credits.

- Employees of the firm who use the SaaS must receive training on and are required to abide by all end-user security measures, including, but not limited to, the creation of strong passwords and the regular replacement of passwords.
- Protecting the ability to represent the client reliably by ensuring that a copy of digital data is stored onsite.⁷
- Having an alternate way to connect to the internet, since cloud service is accessed through the internet.

The terms and conditions under which the “cloud computing” services are offered, *i.e.*, Service Level Agreements (“SLAs”), may also present obstacles to reasonable care efforts. Most SLAs are essentially “take it or leave it,”⁸ and often users, including lawyers, do not read the terms closely or at all. As a result, compliance with ethical mandates can be difficult. However, new competition in the “cloud computing” field is now causing vendors to consider altering terms. This can help attorneys meet their ethical obligations by facilitating an agreement with a vendor that adequately safeguards security and reliability.⁹

Additional responsibilities flow from actual breaches of data. At least forty-five states, including Pennsylvania, currently have data breach notification laws and a federal law is expected. Pennsylvania’s notification law, 73 P.S. § 2303 (2011) (“Notification of Breach”), states:

(a) GENERAL RULE. -- An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4 or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.

(b) ENCRYPTED INFORMATION. -- An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.

⁷ This is recommended even though many vendors will claim that it is not necessary.

⁸ Larger providers can be especially rigid with SLAs, since standardized agreements help providers to reduce costs.

⁹ One caveat in an increasing field of vendors is that some upstart providers may not have staying power. Attorneys are well advised to consider the stability of any company that may handle sensitive information and the ramifications for the data in the event of bankruptcy, disruption in service or potential data breaches.

(c) **VENDOR NOTIFICATION.** -- A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.

A June, 2010, Pew survey highlighted concerns about security for “cloud computing.” In the survey, a number of the nearly 900 internet experts surveyed agreed that it “presents security problems and further exposes private information,” and some experts even predicted that “the cloud” will eventually have a massive breach from cyber-attacks.¹⁰ Incident response plans should be in place before attorneys move to “the cloud”, and the plans need to be reviewed annually. Lawyers may need to consider that at least some data may be too important to risk inclusion in cloud services.

One alternative to increase security measures against data breaches could be “private clouds.” Private clouds are not hosted on the Internet, and give users completely internal security and control. Therefore, outsourcing rules do not apply to private clouds. Reasonable care standards still apply, however, as private clouds do not have impenetrable security. Another consideration might be hybrid clouds, which combine standard and private cloud functions.

D. Web-based E-mail

Web-based email (“webmail”) is a common way to communicate for individuals and businesses alike. Examples of webmail include AOL Mail, Hotmail, Gmail, and Yahoo! Mail. These services transmit and store e-mails and other files entirely online and, like other forms of “cloud computing,” are accessed through an internet browser. While pervasive, webmail carries with it risks that attorneys should be aware of and mitigate in order to stay in compliance with their ethical obligations. As with all other cloud services, reasonable care in transmitting and storing client information through webmail is appropriate.

In 1999, The ABA Standing Commission on Ethics and Professional Responsibility issued Formal Opinion No. 99-413, discussed in further detail above, and concluded that using unencrypted email is permissible. Generally, concerns about e-mail security are increasing, particularly unencrypted e-mail. Whether an attorney’s obligations should include the safeguard of encrypting emails is a matter of debate. An article entitled, “Legal Ethics in the Cloud: Avoiding the Storms,” explains:

Respected security professionals for years have compared e-mail to postcards or postcards written in pencil. Encryption is being increasingly required in areas like banking and health care. New laws in Nevada and Massachusetts (which apply to attorneys as well as others) require defined personal information to be encrypted when it is electronically transmitted. As the use of encryption grows in areas like

¹⁰ Janna Quitney Anderson & Lee Rainie, The Future of Cloud Computing. Pew Internet & American Life Project, June 11, 2010, <http://www.pewinternet.org/Reports/2010/The-future-of-cloud-computing/Main-Findings.aspx?view=all>

these, it will become difficult for attorneys to demonstrate that confidential client data needs lesser protection.¹¹

The article also provides a list of nine potential e-mail risk areas, including: confidentiality, authenticity, integrity, misdirection or forwarding, permanence (wanted e-mail may become lost and unwanted e-mail may remain accessible even if deleted), and malware. The article further provides guidance for protecting e-mail by stating:

In addition to complying with any legal requirements that apply, the most prudent approach to the ethical duty of protecting confidentiality is to have an express understanding with clients about the nature of communications that will be (and will not be) sent by e-mail and whether or not encryption and other security measures will be utilized.

It has now reached the point (or at least is reaching it) where most attorneys should have encryption available for use in appropriate circumstances.¹²

Compounding the general security concerns for e-mail is that users increasingly access webmail using unsecure or vulnerable methods such as cell phones or laptops with public wireless internet connections. Reasonable precautions are necessary to minimize the risk of unauthorized access to sensitive client information when using these devices and services, possibly including precautions such as encryption and strong password protection in the event of lost or stolen devices, or hacking.

The Committee further notes that this issue was addressed by the District of Columbia Bar in Opinion 281 (Feb. 18, 1998) (“Transmission of Confidential Information by Electronic Mail”), which concluded that, “In most circumstances, transmission of confidential information by unencrypted electronic mail does not per se violate the confidentiality rules of the legal profession. However, individual circumstances may require greater means of security.”

The Committee concluded, and this Committee agrees, that the use of unencrypted electronic mail is not, by itself, a violation of the Rules of Professional Conduct, in particular Rule 1.6 (“Confidentiality of Information”).

Thus, we hold that the mere use of electronic communication is not a violation of Rule 1.6 absent special factors. We recognize that as to any confidential communication, the sensitivity of the contents of the communication and/or the circumstances of the transmission may, in specific instances, dictate higher levels of security. Thus, it may be necessary in certain circumstances to use extraordinary means to protect client confidences. To give an obvious example, a lawyer representing an associate in a dispute with the associate’s law firm could very easily violate Rule 1.6 by sending a fax concerning the dispute to the law firm’s mail room if that message contained client confidential

¹¹ David G. Ries, Esquire, “Legal Ethics in the Cloud: Avoiding the Storms,” course handbook, *Cloud Computing 2011: Cut Through the Fluff & Tackle the Critical Stuff* (June 2011) (internal citations omitted).

¹² *Id.*

information. It is reasonable to suppose that employees of the firm, other lawyer employed at the firm, indeed firm management, could very well inadvertently see such a fax and learn of its contents concerning the associate's dispute with the law firm. Thus, what may ordinarily be permissible—the transmission of confidential information by facsimile—may not be permissible in a particularly factual context.

By the same analysis, what may ordinarily be permissible – the use of unencrypted electronic transmission – may not be acceptable in the context of a particularly heightened degree of concern or in a particular set of facts. But with that exception, we find that a lawyer takes reasonable steps to protect his client's confidence when he uses unencrypted electronically transmitted messages.

E. Opinions From Other Ethics Committees

Other Ethics Committees have reached conclusions similar in substance to those in this Opinion. Generally, the consensus is that, while “cloud computing” is permissible, lawyers should proceed with caution because they have an ethical duty to protect sensitive client data. In service to that essential duty, and in order to meet the standard of reasonable care, other Committees have determined that attorneys must (1) include terms in any agreement with the provider that require the provider to preserve the confidentiality and security of the data, and (2) be knowledgeable about how providers will handle the data entrusted to them. Some Committees have also raised ethical concerns regarding confidentiality issues with third-party access or general electronic transmission (*e.g.*, web-based email) and these conclusions are consistent with opinions about emergent emergent “cloud computing” technologies.

The American Bar Association Standing Committee on Ethics and Professional Responsibility has not yet issued a formal opinion on “cloud computing.” However, the ABA Commission on Ethics 20/20 Working Group on the Implications of New Technologies, published an “Issues Paper Concerning Client Confidentiality and Lawyers’ Use of Technology” (Sept. 20, 2010) and considered some of the concerns and ethical implications of using “the cloud.” The Working Group found that potential confidentiality problems involved with “cloud computing” include:

- Storage in countries with less legal protection for data;
- Unclear policies regarding data ownership;
- Failure to adequately back up data;
- Unclear policies for data breach notice;
- Insufficient encryption;
- Unclear data destruction policies;
- Bankruptcy;
- Protocol for a change of cloud providers;
- Disgruntled/dishonest insiders;
- Hackers;
- Technical failures;
- Server crashes;
- Viruses;

- Data corruption;
- Data destruction;
- Business interruption (*e.g.*, weather, accident, terrorism); and,
- Absolute loss (*i.e.*, natural or man-made disasters that destroy everything).

Id. The Working Group also stated, “[f]orms of technology other than ‘cloud computing’ can produce just as many confidentiality-related concerns, such as when laptops, flash drives, and smart phones are lost or stolen.” *Id.* Among the precautions the Commission is considering recommending are:

- Physical protection for devices (*e.g.*, laptops) or methods for remotely deleting data from lost or stolen devices;
- Strong passwords;
- Purging data from replaced devices (*e.g.*, computers, smart phones, and copiers with scanners);
- Safeguards against malware (*e.g.*, virus and spyware protection);
- Firewalls to prevent unauthorized access;
- Frequent backups of data;
- Updating to operating systems with the latest security protections;
- Configuring software and network settings to minimize security risks;
- Encrypting sensitive information;
- Identifying or eliminating metadata from electronic documents; and
- Avoiding public Wi-Fi when transmitting confidential information (*e.g.*, sending an email to a client).

Id. Additionally, the ABA Commission on Ethics 20/20 has drafted a proposal to amend, *inter alia*, Model Rule 1.0 (“Terminology”), Model Rule 1.1 (“Competence”), and Model Rule 1.6 (“Duty of Confidentiality”) to account for confidentiality concerns with the use of technology, in particular confidential information stored in an electronic format. Among the proposed amendments (insertions underlined, deletions ~~struck through~~):

Rule 1.1 (“Competence”) Comment [6] (“Maintaining Competence”): “To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.”

Rule 1.6(c) (“Duty of Confidentiality”): “A lawyer shall make reasonable efforts to prevent the inadvertent disclosure of, or unauthorized access to, information relating to the representation of a client.”

Rule 1.6 (“Duty of Confidentiality”) Comment [16] (“Acting Competently to Preserve Confidentiality”): “Paragraph (c) requires a ~~A~~ lawyer ~~must to~~ act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons or entities who are participating in the representation of the client or who are subject to the lawyer’s supervision or monitoring. See Rules 1.1, 5.1, and 5.3. Factors to

be considered in determining the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, and the cost of employing additional safeguards. 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.

In Formal Opinion No. 99-413 (March 10, 1999), the ABA Standing Committee on Ethics and Professional Responsibility determined that using e-mail for professional correspondence is acceptable. Ultimately, it concluded that unencrypted e-mail poses no greater risks than other communication modes commonly relied upon. As the Committee reasoned, "The risk of unauthorized interception and disclosure exists in every medium of communication, including e-mail. It is not, however, reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible, especially when unauthorized interception or dissemination of the information is a violation of the law." *Id.*

Also relevant is ABA Formal Opinion 08-451 (August 5, 2008), which concluded that the ABA Model Rules generally allow for outsourcing of legal and non-legal support services if the outsourcing attorney ensures compliance with competency, confidentiality, and supervision. The Committee stated that an attorney has a supervisory obligation to ensure compliance with professional ethics even if the attorney's affiliation with the other lawyer or nonlawyer is indirect. An attorney is therefore obligated to ensure that any service provider complies with confidentiality standards. The Committee advised attorneys to utilize written confidentiality agreements and to verify that the provider does not also work for an adversary.

The Alabama State Bar Office of General Council Disciplinary Commission issued Ethics Opinion 2010-02, concluding that an attorney must exercise reasonable care in storing client files, which includes becoming knowledgeable about a provider's storage and security and ensuring that the provider will abide by a confidentiality agreement. Lawyers should stay on top of emerging technology to ensure security is safeguarded. Attorneys may also need to back up electronic data to protect against technical or physical impairment, and install firewalls and intrusion detection software.

State Bar of Arizona Ethics Opinion 09-04 (Dec. 2009) stated that an attorney should take reasonable precautions to protect the security and confidentiality of data, precautions which are satisfied when data is accessible exclusively through a Secure Sockets Layer ("SSL") encrypted connection and at least one other password was used to protect each document on the system. The Opinion further stated, "It is important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult experts in the field." *Id.* Also, lawyers should ensure reasonable protection through a periodic review of security as new technologies emerge.

The California State Bar Standing Committee on Professional Responsibility and Conduct concluded in its Formal Opinion 2010-179 that an attorney using public wireless connections to conduct research and send e-mails should use precautions, such as personal firewalls and encrypting files and transmissions, or else risk violating his or her confidentiality and competence obligations. Some highly sensitive matters may necessitate discussing the use of

public wireless connections with the client or in the alternative avoiding their use altogether. Appropriately secure personal connections meet a lawyer's professional obligations. Ultimately, the Committee found that attorneys should (1) use technology in conjunction with appropriate measures to protect client confidentiality, (2) tailor such measures to each unique type of technology, and (3) stay abreast of technological advances to ensure those measures remain sufficient.

The Florida Bar Standing Committee on Professional Ethics, in Opinion 06-1 (April 10, 2006), concluded that lawyers may utilize electronic filing provided that attorneys "take reasonable precautions to ensure confidentiality of client information, particularly if the lawyer relies on third parties to convert and store paper documents to electronic records." *Id.*

Illinois State Bar Association Ethics Opinion 10-01 (July 2009) stated that "[a] law firm's use of an off-site network administrator to assist in the operation of its law practice will not violate the Illinois Rules of Professional Conduct regarding the confidentiality of client information if the law firm makes reasonable efforts to ensure the protection of confidential client information."¹³

The Maine Board of Overseers of the Bar Professional Ethics Commission adopted Opinion 194 (June 30, 2008) in which it stated that attorneys may use third-party electronic back-up and transcription services so long as appropriate safeguards are taken, including "reasonable efforts to prevent the disclosure of confidential information," and at minimum an agreement with the vendor that contains "a legally enforceable obligation to maintain the confidentiality of the client data involved." *Id.*

Of note, the Maine Ethics Commission, in a footnote, suggests in Opinion 194 that the federal Health Insurance Portability and Accountability Act ("HIPAA") Privacy and Security Rule 45 C.F.R. Subpart 164.314(a)(2) provide a good medical field example of contract requirements between medical professionals and third party service providers ("business associates") that handle confidential patient information. SLAs that reflect these or similar requirements may be advisable for lawyers who use cloud services.

45 C.F.R. Subpart 164.314(a)(2)(i) states:

The contract between a covered entity and a business associate must provide that the business associate will:

(A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;

¹³ Mark Mathewson, *New ISBA Ethics Opinion Re: Confidentiality and Third-Party Tech Vendors*, Illinois Lawyer Now, July 24, 2009, available at <http://www.illinoislawyernow.com/2009/07/24/new-isba-ethics-opinion-re-confidentiality-and-third-party-tech-vendors/>

- (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;
- (C) Report to the covered entity any security incident of which it becomes aware;
- (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

Massachusetts Bar Association Ethics Opinion 05-04 (March 3, 2005) addressed ethical concerns surrounding a computer support vendor's access to a firm's computers containing confidential client information. The committee concluded that a lawyer may provide a third-party vendor with access to confidential client information to support and maintain a firm's software. Clients have "impliedly authorized" lawyers to make confidential information accessible to vendors "pursuant to Rule 1.6(a) in order to permit the firm to provide representation to its clients." *Id.* Lawyers must "make reasonable efforts to ensure" a vendor's conduct comports with professional obligations. *Id.*

The State Bar of Nevada Standing Committee on Ethics and Professional Responsibility issued Formal Opinion No. 33 (Feb. 9, 2006) in which it stated, "an attorney may use an outside agency to store confidential information in electronic form, and on hardware located outside an attorney's direct supervision and control, so long as the attorney observed the usual obligations applicable to such arrangements for third party storage services." *Id.* Providers should, as part of the service agreement, safeguard confidentiality and prevent unauthorized access to data. The Committee determined that an attorney does not violate ethical standards by using third-party storage, even if a breach occurs, so long as he or she acts competently and reasonably in protecting information.

The New Jersey State Bar Association Advisory Committee on Professional Ethics issued Opinion 701 (April 2006) in which it concluded that, when using electronic filing systems, attorneys must safeguard client confidentiality by exercising "sound professional judgment" and reasonable care against unauthorized access, employing reasonably available technology. *Id.* Attorneys should obligate outside vendors, through "contract, professional standards, or otherwise," to safeguard confidential information. *Id.* The Committee recognized that Internet service providers often have better security than a firm would, so information is not necessarily safer when it is stored on a firm's local server. The Committee also noted that a strict guarantee of invulnerability is impossible in any method of file maintenance, even in paper document filing, since a burglar could conceivably break into a file room or a thief could steal mail.

The New York State Bar Association Committee on Professional Ethics concluded in Opinion 842 (Sept. 10, 2010) that the reasonable care standard for confidentiality should be maintained for online data storage and a lawyer is required to stay abreast of technology advances to ensure protection. Reasonable care may include: (1) obligating the provider to preserve confidentiality and security and to notify the attorney if served with process to produce client information, (2) making sure the provider has adequate security measures, policies, and recoverability methods,

and (3) guarding against “reasonably foreseeable” data infiltration by using available technology. *Id.*

The North Carolina State Bar Ethics Committee has addressed the issue of “cloud computing” directly, and this Opinion adopts in large part the recommendations of this Committee. Proposed Formal Opinion 6 (April 21, 2011) concluded that “a law firm may use SaaS¹⁴ if reasonable care is taken effectively to minimize the risks to the disclosure of confidential information and to the security of client information and client files.” *Id.* The Committee reasoned that North Carolina Rules of Professional Conduct do not require a specific mode of protection for client information or prohibit using vendors who may handle confidential information, but they do require reasonable care in determining the best method of representation while preserving client data integrity. Further, the Committee determined that lawyers “must protect against security weaknesses unique to the Internet, particularly ‘end-user’ vulnerabilities found in the lawyer’s own law office.” *Id.*

The Committee’s minimum requirements for reasonable care in Proposed Formal Opinion 6 included:¹⁵

- An agreement on how confidential client information will be handled in keeping with the lawyer’s professional responsibilities must be included in the SaaS vendor’s Terms of Service or Service Level Agreement, or in a separate agreement that states that the employees at the vendor’s data center are agents of the law firm and have a fiduciary responsibility to protect confidential client information and client property;
- The agreement with the vendor must specify that firm’s data will be hosted only within a specified geographic area. If by agreement the data is hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and the state of North Carolina;
- If the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity, the law firm must have a method for retrieving the data, the data must be available in a non-proprietary format that is compatible with other firm software or the firm must have access to the vendor’s software or source code, and data hosted by the vendor or third party data hosting company must be destroyed or returned promptly;

¹⁴ SaaS, as stated above, stands for Software-as-a-Service and is a type of “cloud computing.”

¹⁵ The Committee emphasized that these are minimum requirements, and, because risks constantly evolve, “due diligence and perpetual education as to the security risks of SaaS are required.” Consequently, lawyers may need security consultants to assess whether additional measures are necessary.

- The law firm must be able get data “off” the vendor’s or third party data hosting company’s servers for lawyers’ own use or in-house backup offline; and,
- Employees of the firm who use SaaS should receive training on and be required to abide by end-user security measures including, but not limited to, the creation of strong passwords and the regular replacement of passwords.

In Opinion 99-03 (June 21, 1999), the **State Bar Association of North Dakota** Ethics Committee determined that attorneys are permitted to use online data backup services protected by confidential passwords. Two separate confidentiality issues that the Committee identified are, (1) transmission of data over the internet, and (2) the storage of electronic data. The Committee concluded that the transmission of data and the use of online data backup services are permissible provided that lawyers ensure adequate security, including limiting access only to authorized personnel and requiring passwords.

Vermont Bar Association Advisory Ethics Opinion 2003-03 concluded that lawyers can use third-party vendors as consultants for confidential client data-base recovery if the vendor fully understands and embraces the clearly communicated confidentiality rules. Lawyers should determine whether contractors have sufficient safety measures to protect information. A significant breach obligates a lawyer to disclose the breach to the client.

Virginia State Bar Ethics Counsel Legal Ethics Opinion 1818 (Sept. 30, 2005) stated that lawyers using third party technical assistance and support for electronic storage should adhere to Virginia Rule of Professional Conduct 1.6(b)(6)¹⁶, requiring “due care” in selecting the service provider and keeping the information confidential. *Id.*

These opinions have offered compelling rationales for concluding that using vendors for software, service, and information transmission and storage is permissible so long as attorneys meet the existing reasonable care standard under the applicable Rules of Professional Conduct, and are flexible in contemplating the steps that are required for reasonable care as technology changes.

IV. Conclusion

The use of “cloud computing,” and electronic devices such as cell phones that take advantage of cloud services, is a growing trend in many industries, including law. Firms may be eager to capitalize on cloud services in an effort to promote mobility, flexibility, organization and efficiency, reduce costs, and enable lawyers to focus more on legal, rather than technical and

¹⁶ Virginia Rule of Professional Conduct 1.6(b) states in relevant part:

To the extent a lawyer reasonably believes necessary, the lawyer may reveal:

(6) information to an outside agency necessary for statistical, bookkeeping, accounting, data processing, printing, or other similar office management purposes, provided the lawyer exercises due care in the selection of the agency, advises the agency that the information must be kept confidential and reasonably believes that the information will be kept confidential.

administrative, issues. However, lawyers must be conscientious about maintaining traditional confidentiality, competence, and supervisory standards.

This Committee concludes that the Pennsylvania Rules of Professional Conduct require attorneys to make reasonable efforts to meet their obligations to ensure client confidentiality, and confirm that any third-party service provider is likewise obligated.

Accordingly, as outlined above, this Committee concludes that, under the Pennsylvania Rules of Professional Conduct an attorney may store confidential material in “the cloud.” Because the need to maintain confidentiality is crucial to the attorney-client relationship, attorneys using “cloud” software or services must take appropriate measures to protect confidential electronic communications and information. In addition, attorneys may use email but must, under appropriate circumstances, take additional precautions to assure client confidentiality.

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.

July 25, 2013

Re: Request for Informal Advisory Opinion

Dear _____:

You have requested the opinion of the Ohio State Bar Association Professionalism Committee on whether your law firm may use a third-party vendor to store client data in “the cloud.” As you describe it, your firm currently backs up its computer files, including client documents and data, on a server located on site. You are considering a third-party vendor that is offering a program that would use “a major software provider to securely store your data off site,” which your law firm would be able to access via the Internet. You indicate that the data would be encrypted before it left the law firm and would remain encrypted at the offsite data center, located in Atlanta.

The Committee’s opinion is that storing client data in “the cloud” is a permutation on traditional ways of storing client data, and requires lawyers to follow the ethics rules that apply to client information in whatever form. With due regard for these rules and related Ohio ethics opinions, the Committee advises that the Ohio Rules of Professional Conduct do not prohibit storing client data in “the cloud.”

Applicable Rules of Professional Conduct:

Your request for an opinion requires consideration of the following provision of the Ohio Rules of Professional Conduct (“ORPC” or “Rules”):

- 1.1 (lawyer shall provide competent representation);
- 1.4(a)(2) (lawyer shall reasonably consult with client about means by which client’s objectives are to be accomplished);
- 1.6(a) (lawyer shall preserve confidentiality of information relating to the representation, subject to certain limited exceptions);
- 1.15(a) (lawyer shall safeguard client property);
- 5.3(a)-(b) (with respect to a non-lawyer employed by, retained by or associated with a lawyer, lawyer shall make reasonable efforts to ensure that the non-lawyer’s conduct is compatible with lawyer’s professional obligations).

Opinion:

The “cloud” is “merely ‘a fancy way of saying stuff’s not on your [own] computer.’” Formal Op. 2011-200, 1 (Pa. Bar Ass’n. Comm. on Legal Ethics & Prof’l Respon. 2011). More formally, cloud storage is the use of “internet-based computing in which large groups of remote servers are networked so as to allow ... centralized data storage.” Andrew L. Askew, *iEthics: How Cloud Computing has Impacted the Rules of Professional Conduct*, 88 N. Dak. L. Rev. 453, 457 (2012).

Due to “recent advances in ... technology, the ways attorneys are able to perform and deliver legal services have drastically changed.” Askew, *supra* at 466. The applicable Ohio Rules of Professional Conduct, however, are adaptable to address new technologies. Regarding cloud storage, the key rules are those relating to competent representation, communicating with the client, preserving client confidentiality, safeguarding the client’s property and supervising non-lawyers that provide support services. The obligations expressed in these rules operate as they traditionally have for older data storage methods. *See, e.g.*, Adv. Op. 99-2 (Ohio Bd. of Comm’rs on Grievances & Disc. Apr. 9, 1999) (communicating by e-mail was not contemplated in 1970, when former disciplinary rule on confidentiality was adopted by Ohio Supreme Court, but “nevertheless, the rule applies” to e-mail).

The issues and ethical duties regarding cloud storage are analogous to the ones that apply when lawyers opt to use a vendor to store their paper files offsite rather than in their own offices. The analogy to paper files can help lawyers as they exercise their professional judgment in adopting specific practices that address new storage technologies such as “the cloud.” That process of exercising individual judgment would not be assisted by overly-detailed regulatory input from this Committee. As one state bar ethics committee noted, a lawyer “has always been under a duty to make reasonable judgments when protecting client property and information. *Specific practices regarding protection of client property and information have always been left up to individual lawyers’ judgment, and that same approach applies to the use of online data storage,*” subject as always to the relevant conduct rules. Adv. Op. 2215, 2 (Wash. St. Bar Rules of Prof’l Cond. Comm. 2012) (emphasis added).

This approach – applying existing principles to new technological advances while refraining from mandating specific practices – is a practical one. Because technology changes so quickly, overly-specific rules would become obsolete as soon as they were issued. *See* Ethics Op. 2010-6 (Vt. Bar Prof’l Respon. Section 2010) (dynamism of cloud computing makes it unwise to establish “specific conditions precedent” to use). For example, rules about exactly what security measures are required in order to protect client data stored in the cloud would be superseded quickly by technological advances.¹

¹ The American Bar Association’s recent promulgation through the Commission on Ethics 20/20 of rule changes and new comments for the Model Rules of Professional Conduct (“MRPC”) is in line with this approach. The Commission on Ethics 20/20 proposed and the ABA House of Delegates adopted minor changes to existing rules rather than specific regulations aimed at specific new technologies. *See e.g.*, revised cmt. [8] to MRPC 1.1 (lawyer should keep

Against that background, there are four main issues to consider in applying the Ohio Rules of Professional Conduct to cloud storage of client data: competently selecting an appropriate vendor; preserving confidentiality and safeguarding the client's data; supervising cloud storage vendors; and communicating with the client

1. *Competently selecting an appropriate vendor for cloud storage*

The duty of competence under ORPC 1.1 requires a lawyer to exercise the "legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation." In Ohio Advisory Opinion 2009-6 (Aug. 14, 2009), the Ohio Board of Commissioners on Grievances and Discipline ("Board") opined that a lawyer who selects a vendor for *any* type of support services that are provided outside the lawyer's firm must exercise "due diligence as to the qualifications and reputation of those to whom services are outsourced," and also as to whether the outside vendor will itself provide the requested services competently and diligently. *Id.* at 6.²

Knowing the qualifications, reputation and longevity of your cloud storage vendor is necessary. But in addition, just as you would review and assess the terms of a contract for off-site storage of your clients' paper files in a brick-and-mortar facility, so you must read and under-

up with changes in law and its practice, "including the benefits and risks associated with relevant technology") (emphasis added); new cmt. [3] to MRPC 5.3 (lawyer may use outside non-lawyers to assist in rendering legal services; "[e]xamples include ... using an Internet-based service to store client information."; extent of lawyer's obligation to ensure that non-lawyers provide services in a manner compatible with lawyer's professional obligations "will depend upon the circumstances.") (emphasis added).

Ohio has not yet adopted any of the revised provisions of the Model Rules. See Univ. of Akron Miller-Becker Ctr. for Prof'l Respon., *Navigating the Practice of Law in the Wake of Ethics 20/20 - Globalization, New Technologies, and What It Means to be a Lawyer in these Uncertain Times* (Apr. 4-5, 2013), available at <http://tinyurl.com/lblj6q8> (examining Ethics 20/20's final work and its impact in Ohio and elsewhere); Frank E. Quirk, *Lawyer Ethics for the 21st Century*, 19-21 Ohio Lawyer (Jan. - Feb. 2013) (discussing Ethics 20/20, including possible future impact on ORPC).

² Lawyers can call on many resources to assist in selecting a vendor. See, e.g., John Edwards, *How to Pick the Best Cloud*, Law Technology News (June 11, 2013), available at <http://tinyurl.com/k77w2sg>; Nicole Black & Matt Spiegel, *Breaking Down Cloud Computing*, ABA Section of Litigation (Feb. 7, 2013), available at <http://tinyurl.com/ksaeww8>; Am. Bar Ass'n, *Moving Your Law Practice to the Cloud Safely and Ethically* (Jan. 14, 2013), available at <http://tinyurl.com/kr3s2xw>; Am. Bar Ass'n, *Evaluating Cloud-Computing Providers* (YourABA June 2012), available at <http://tinyurl.com/l7b9wfh>. See generally, Nick Pournader, *Embracing Technology's 'Cloudy' Frontier*, Law Practice Today (webzine of ABA Law Practice Management Section) (Oct. 2010), available at <http://tinyurl.com/k54f3gh>.

stand the agreement you enter into with an online data storage service – sometimes called a “Service Level Agreement.”³ Some commonly-occurring issues include:

- What safeguards does the vendor have to prevent confidentiality breaches?
- Does the agreement create a legally enforceable obligation on the vendor’s part to safeguard the confidentiality of the data?
- Do the terms of the agreement purport to give “ownership” of the data to the vendor, or is the data merely subject to the vendor’s license?⁴
- How may the vendor respond to government or judicial attempts to obtain disclosure of your client data?
- What is the vendor’s policy regarding returning your client data at the termination of its relationship with your firm?
- What plans and procedures does the vendor have in case of natural disaster, electric power interruption or other catastrophic events?
- Where is the server located (particularly if the vendor itself does not actually host the data, and uses a data center located elsewhere)? Is the relationship subject to international law?

2. *Preserving confidentiality and safeguarding client property*

Under ORPC 1.6(a), a lawyer “shall not reveal information relating to the representation of a client,” with only limited exceptions. As recommended by the Commission on Ethics 20/20, the ABA House of Delegates added Model Rule 1.6(c) in August 2012, requiring a lawyer to make “reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.” The Ohio Supreme Court has not considered or adopted that change. Yet the language of the new Model Rule only makes explicit a duty that is already implicit in Ohio’s current Rule 1.6(a). That duty is to maintain the confidentiality of all client data relating to the representation, irrespective of the form of that data, and to carry out that duty with due regard for the form that the data is in.

³ See Sharon D. Nelson & John W. Simek, *Have Attorneys Read the iCloud Terms and Conditions?*, Slaw (Canadian online legal magazine) (Jan. 30, 2012), *available at* <http://tinyurl.com/m425p3j> (discussing Apple iCloud terms and conditions of use and expressing doubt that attorneys have read them).

⁴ See § 2, below. A Service Level Agreement or terms of service that provide that the vendor “owns” the data would violate ORPC 1.15(a), which requires that client property “be identified as such” and “appropriately safeguarded.”

For instance, in Advisory Opinion 99-2 (Apr. 9, 1999), the Board said that communicating with clients by e-mail was covered by the confidentiality rule in the former Code of Professional Responsibility, which “establishes a broad duty to preserve confidences and secrets that applies to all methods of communication. The duty extends to communications by electronic methods just as it extends to other forms of communication used by an attorney.” *Id.* at 3. Significantly, the Board ruled that it was not necessary to encrypt e-mail communications with clients, despite the possibility that such communications might be electronically intercepted. Such a risk was not unique to e-mail in the Board’s view, and did not call for extraordinary methods of protection:

Every method of communication carries with it a risk of interception. Mail can be intercepted. Telephone messages can also be intercepted. Land-based telephones may be wiretapped, eavesdropping may occur by listening through a receiver of a telephone extension, or too loud voices may be overheard by others. Yet, these forms of communication are considered reasonable under the rule. To summarize, additional security measures, such as scrambling devices or encoding methods, have not traditionally been required under [the confidentiality rule] for other forms of communication frequently used by attorneys, even though the communication may be susceptible of interception.

Id. at 9-10.

Rather, the Board emphasized that “an attorney must use his or her professional judgment to determine the appropriate method of each attorney-client communication,” and that client preference or particular specialized circumstances may call for taking additional measures to ensure confidentiality. *Id.* at 10-11.

In the same way, storing client data in the cloud involves yielding exclusive control over the information and puts it in the hands of a third party, just as storing a client’s paper files off-site does. And similar to storing a client’s paper files off-site, cloud storage raises the risk that “a third party could illegally gain access to ... confidential client data.” Formal Ethics Op. 2010-02, 14 (Ala. Disc. Comm. 2010). “[J]ust as with traditional storage and retention of client files, a lawyer cannot guarantee that client confidentiality will never be breached, whether by an employee or some other third-party.” *Id.* at 15. Therefore, a lawyer’s duty under the ORPC to preserve the confidentiality of cloud-stored client data is to exercise competence (1) in selecting an appropriate vendor, (2) in staying abreast of technology issues that have an impact on client data storage and (3) in considering whether any special circumstances call for extra protection for particularly sensitive client information or for refraining from using the cloud to store such particularly sensitive data.

In the context of cloud storage, the requirement under ORPC 1.15(a) that client property “be identified as such and appropriately safeguarded” is a corollary to the duty to preserve the confidentiality of information related to the representation. A client’s information and documents in whatever form can be construed as its “property” when in the lawyer’s possession. Safeguarding such property includes reasonably ensuring that the vendor has systems in place to

protect client data from destruction, loss or unavailability. In addition, terms of service that provide or suggest that the cloud storage vendor acquires an ownership interest in the electronic data on its servers would violate the duty to keep client property “identified as such.”

3. *Supervising cloud vendors*

Rule 5.3(a) of the ORPC requires that law firms make reasonable efforts to have policies and procedures in place that give reasonable assurance that the conduct of a non-lawyer employed by the lawyer is “compatible with the professional obligations of the lawyer.” And under Rule 5.3(b), individual lawyers who have supervisory authority over non-lawyers must likewise make reasonable efforts to ensure that the non-lawyer’s conduct is compatible with the lawyers’ own professional obligations.

In its Advisory Opinion 2009-6, *supra*, the Board explained how these duties apply when lawyers outsource non-legal “support services,” defined to encompass all varieties of “ministerial” services that are non-legal in nature. *Id.* at 3. The Board emphasized that while Rule 5.3’s supervisory duties apply to lawyers when they outsource to support-service vendors, “the *extent* of supervision for outsourced services is a matter of professional judgment for an Ohio lawyer,” subject to the requirement that lawyers exercise that judgment with the diligence due under the Rules – particularly as to the vendor’s qualifications, competence and ability to protect confidentiality. *Id.* at 8 (emphasis added).

Storing client data in “the cloud” is almost by definition a service that lawyers will outsource, and cloud-storage vendors provide the kind of “ministerial” non-legal support services that are contemplated under the Board’s Advisory Opinion 2009-6. Therefore, under Rule 5.3(a)-(b), lawyers who contract with a cloud-storage vendor must make reasonable efforts to ensure that the vendor’s conduct is compatible with the lawyer’s own professional obligations. While the extent of supervision needed is a matter of professional judgment for the lawyer, the lawyer must exercise due diligence in ascertaining whether the vendor will be capable of conduct consistent with the lawyer’s own obligations.

4. *Communicating with the client*

Rule 1.4(a)(2) requires a lawyer to “reasonably consult with the client” about how the client’s objectives are to be accomplished. We do not conclude that storing client data in “the cloud” always requires prior client consultation, because we interpret the language “reasonably consult” as indicating that the lawyer must use judgment in order to determine if the circumstances call for consultation. Our opinion on this point is in line with ethics authorities in other jurisdictions that have considered the question. *See, e.g.*, Formal Op. 2011-200, 5-6 (Pa. Bar Ass’n Comm. on Legal Ethics & Prof’l Respon. 2011) (not necessary to “communicate every minute detail” of representation, but it may at times be necessary to inform client of lawyer’s use of cloud computing, depending on scope of representation and sensitivity of data involved); Adv. Op. 2012-13/4 (N.H. Bar Ass’n Ethics Comm. 2012) (where highly sensitive data involved, “may become necessary” to inform client and obtain consent for lawyer’s use of cloud computing). In exercising judgment about whether to consult with the client about storing client data in “the cloud,” the lawyer should consider, among other things, the sensitivity of the client’s data.

5. Ethics opinions from other jurisdictions regarding cloud storage

Our conclusion that cloud storage is permissible under the ORPC is echoed by ethics authorities in other jurisdictions. To date, at least 14 states have issued ethics opinions regarding or related to cloud data storage. All have concluded that their respective lawyer conduct rules permit lawyers to store client data in the cloud, with due regard for their state ethics rules, usually their states' versions of ORPC 1.1, 1.6, 1.15 and 5.3.⁵

Conclusion:

Storing client data in “the cloud” can provide benefits to lawyers and clients by facilitating access to client data, increasing efficiency and reducing the cost of legal services. The Ohio Rules of Professional Conduct do not prohibit cloud storage, provided that lawyers follow the ethics rules that apply to client information in whatever form and are guided by applicable Ohio ethics opinions.

Sincerely,

Professionalism Committee
OHIO STATE BAR ASSOCIATION

Note: Advisory Opinions of the Ohio State Bar Association Professionalism Committee are informal, non-binding opinions in response to prospective or hypothetical questions regarding the application of the Supreme Court Rules for the Government of the Judiciary, the Rules of Professional Conduct, the Code of Judicial Conduct, and the Attorney's Oath of Office.

⁵ The ABA has summarized and charted the opinions on cloud ethics issues via the ABA's Law Practice Management Section's Legal Technology Resource Center. See Am. Bar Ass'n, *Cloud Ethics Opinions Around the U.S.*, available at <http://tinyurl.com/733gyr8>.

Quick Reference	Opinion Summaries		
Jurisdiction	Permitted?	Standard?	Specific Requirements or Recommendations*
ALABAMA Opinion 2010-02	Yes	Reasonable Care	<ul style="list-style-type: none"> • Know how provider handles storage/security of data. • Reasonably ensure confidentiality agreement is followed. • Stay abreast of best practices regarding data safeguards.
ARIZONA** Opinion 09-04	Yes	Reasonable Care	<ul style="list-style-type: none"> • "Reasonable security precautions," including password protection, encryption, etc. • Develop or consult someone with competence in online computer security. • Periodically review security measures.
CALIFORNIA Opinion 2010-179	Yes	Reasonable Care	<ul style="list-style-type: none"> • Evaluate the nature of the technology, available security precautions, and limitations on third-party access. • Consult an expert if lawyer's technology expertise is lacking. • Weigh the sensitivity of the data, the impact of disclosure on the client, the urgency of the situation, and the client's instructions.
CONNECTICUT Informal Opinion 2013-07	Yes	Reasonable Care	<ul style="list-style-type: none"> • Lawyers ownership and access to the data must not be hindered. • Security policies and processes should segregate the lawyer's data to prevent unauthorized access to the data, including by the cloud service provider. • Ensure provider has enforceable obligation to preserve confidentiality

FLORIDA
Opinion 12-3

Yes

Reasonable
Care

and security, and will provide notice if served with process.

- Investigate provider's security measures
- Guard against reasonably foreseeable attempts to infiltrate data.
- Ensure unfettered access to your data when it is needed, including removing it upon termination of the service.
- Determine the degree of protection afforded to the data residing within the cloud service.

IOWA
Opinion 11-01

Yes

Reasonable
Care

- Ensure firm technology in general meets professional responsibility constraints.
- Review provider's terms of service and/or service level agreements.
- Review provider's technology, specifically focusing on security and backup.
- Review (and periodically revisit) terms of service, restrictions on access to data, data portability, and vendor's security practices.

MAINE
Opinion 207

Yes

Reasonable
Care

- Follow clients' express instructions regarding use of cloud technology to store or transmit data.
- For particularly sensitive client information, obtain client approval before storing/transmitting via the internet.
- Have a basic understanding of technology and stay abreast of changes, including privacy laws and regulations.
- Consider obtaining client's informed consent

MASSACHUSETTS
Opinion 12-03

Yes

Reasonable
Care

NEW HAMPSHIRE
Opinion #2012-13/4

Yes

Reasonable Care

when storing highly confidential information.

- Delete data from the cloud and return it to the client at the conclusion of representation or when the file must no longer be preserved.
- Make a reasonable effort to ensure cloud providers understand and act in a manner compatible with a lawyer's professional responsibilities.

NEW JERSEY**
Opinion 701

Yes

Reasonable Care

- Vendor must have an enforceable obligation to preserve confidentiality and security.
- Use available technology to guard against foreseeable attempts to infiltrate data..

NEW YORK
Opinion 842

Yes

Reasonable Care

- Vendor must have an enforceable obligation to preserve confidentiality and security, and should notify lawyer if served with process for client data.
- Use available technology to guard against foreseeable attempts to infiltrate data.
- Investigate vendor security practices and periodically review to be sure they remain up-to-date.
- Investigate any potential security breaches or lapses by vendor to ensure client data was not compromised.

NEVADA
Opinion 33

Yes

Reasonable Care

- Chose a vendor that can be reasonably relied upon to keep client information confidential.
- Instruct and require the vendor to keep client information confidential.

NORTH

- Review terms and policies, and if necessary re-negotiate, to ensure they're consistent with ethical obligations.

CAROLINA
2011 Formal Ethics
Opinion 6

Yes

Reasonable
Care

- Evaluate vendor's security measures and backup strategy.
- Ensure data can be retrieved if vendor shuts down or lawyer wishes to cancel service.

OHIO
Informal Advisory
Opinion 2013-03

Yes

Reasonable
Care

- Competently select appropriate vendor.
- Preserve confidentiality and safeguard client property.
- Provide reasonable supervision of cloud vendor.
- Communicate with the client as appropriate.

OREGON
Opinion 2011-188

Yes

Reasonable
Care

- Ensure service agreement requires vendor to preserve confidentiality and security.
- Require notice in the event that lawyer's data is accessed by a non-authorized party.
- Ensure adequate backup.
- Re-evaluate precautionary steps periodically in light of advances in technology.

PENNSYLVANIA
Opinion 2011-200

Yes

Reasonable
Care

- Exercise reasonable care to ensure materials stored in the cloud remain confidential.
- Employ reasonable safeguards to protect data from breach, data loss, and other risk.
- See full opinion for 15 point list of possible safeguards.
- Take reasonable precautions to ensure client data is secure and accessible.

VERMONT
Opinion 2010-6

Yes

Reasonable
Care

- Consider whether certain types of data (e.g. wills) must be retained in original paper format.
- Discuss appropriateness of cloud storage with

VIRGINIA
Legal Ethics
Opinion 1872

Yes

Reasonable
Care

client if data is especially sensitive (e.g. trade secrets).

- Exercise care in selection of the vendor.
- Have a reasonable expectation the vendor will keep data confidential and inaccessible.
- Instruct the vendor to preserve the confidentiality of information.

WASHINGTON**
Advisory Opinion
2215

Yes

Reasonable
Care

- Conduct a due diligence investigation of any potential provider.
- Stay abreast of changes in technology.
- Review providers security procedures periodically.

WISCONSIN
Opinion EF-15-01

Yes

Reasonable
Care

- Consider the sensitivity of the data, the impact of the disclosure, the client's circumstances and instructions
- Consult an expert if lawyer's technology expertise is lacking.
- Understand/know the experience and reputation of the service provider and the terms of their agreement.

* Note that in most opinions, the specific steps or factors listed are intended as non-binding recommendations or suggestions. Best practices may evolve depending on the sensitivity of the data or changes in the technology.

** These opinions address issues which aren't directly labeled cloud computing or software as a service, but which share similar technology (e.g.. online backup and file storage).

Quick Reference

Opinion Summaries

Jurisdiction

Summary of Opinion

ALABAMA
 Opinion 2010-02

The Alabama Disciplinary Commission examined cloud computing specifically within the context of storing and producing client files. In that context, the Commission recognized certain benefits of cloud computing, including "the lawyer's increased access to client data" and the possibility that it may also "allow clients greater access to their own files over the internet." That said, the Commission recognized the "confidentiality issues that arise with the use of 'cloud computing,'" specifically that "[c]lient confidences and secrets are no longer under the direct control of the lawyer or his law firm."

After reviewing other opinions from both Arizona and Nevada, the Commission eventually concluded "that a lawyer may use "cloud computing" or third-party providers to store client data provided that the attorney exercises reasonable care in doing so." The Commission defined reasonable care as requiring the lawyer to:

- Learn how the provider would handle the storage and security of the data;
- Reasonably ensure that the provider abides by a confidentiality agreement in handling the data;
- Stay abreast of appropriate safeguards that should be employed by both the lawyer and the third-party.

In the event that a breach of confidentiality occurs, "the focus of the inquiry will be whether the lawyer acted reasonably in selecting the method of storage and/or the third party provider."

Finally, with regard to client files generally, the Commission emphasized that the the format the lawyer uses to store client documents must allow the lawyer "to reproduce the documents in their original paper format," and that the lawyer "must abide by the client's decision in whether to produce the file in its electronic format ... or in its original paper format."

ARIZONA
 Opinion 09-04

The State Bar of Arizona's Ethics Committee reviewed a query from an Arizona lawyer interested in using "an encrypted online file storage and retrieval system for clients in which all documents are converted to password-protected PDF format and stored in online folders with unique, randomly-generated alpha-numeric names and passwords."

In an earlier 2005 opinion, Arizona's Committee had already approved electronic storage of client files where the lawyer or law firm takes "competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence." The opinion stated that there were a "panoply of electronic and other measures ... available to assist an attorney" in this regard, and that specific reasonable precautions included "firewalls, password protection schemes, encryption, anti-virus measures, etc."

The opinion concluded that the "proposed online client file system appears to meet the requirements" outlined by the rules and the earlier ethics opinion, but did stress that "technology advances may make certain protective measures obsolete over time" and therefore "lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients' documents and information."

Recognizing that a technology-by-technology analysis "would likely become obsolete" in a short amount of time, the State Bar of California's Standing Committee on Professional Responsibility and Conduct instead issued an opinion that "sets forth the general analysis that an attorney should undertake when considering use of a particular form of technology."

CALIFORNIA
Opinion 2010-179

The Committee stated that "transmission of information through a third party reasonably necessary for purposes of the representation should not be deemed to have destroyed the confidentiality of the information," but that the "manner in which an attorney acts to safeguard confidential information is governed by the duty of competence." Examining the issue of competence, the Committee declares that "the duty of competence includes taking appropriate steps to ensure both that secrets and privileged information of a client remain confidential and that the attorney's handling of such information does not result in a waiver of any privileges or protections."

The Committee next examines several factors that an attorney should consider before using a given type of technology. These include:

- The nature of the technology in relation to more traditional counterparts (i.e. e-mail versus mail).
- Reasonable precautions possible to improve the security of a given technology.
- Limitations on who can monitor the use of technology and disclose activity.
- The lawyer's own level of technological competence, and whether it's necessary to consult with an expert.
- Legal ramifications to third parties for intercepting or otherwise interfering with electronic information.
- The sensitivity of the data.
- Impact of possible disclosure on the client.
- Urgency of the situation.
- Client instructions.

Summing up the opinion, the Committee states that a lawyer must take the appropriate steps to ensure that technology use "does not subject confidential client information to an undue risk of unauthorized disclosure" and must "monitor the efficacy of such steps" on an ongoing basis.

Addressing the question of "whether it is permissible under the Rules of Professional Responsibility for a lawyer to use cloud computing in the practice of law," the Connecticut Bar Association's Professional Ethics Committee found that "Lawyers who use cloud computing have a duty to understand its potential impact on their obligations under applicable law and under the Rules of Professional Responsibility."

The opinion noted that "Lawyers' remote storage of data is not a new phenomenon; lawyers have been using off-site storage providers for many years, and the issues remain the same whether tangible records are stored in a 'brick-and-mortar' warehouse or intangible data is stored on third party servers." Recognizing the new ABA Model Rule 1.1 comment that lawyers should "keep abreast of changes in the law and practice, including the benefits and risks associated with relevant technology, the Committee concluded that "[i]n order to determine whether use of a particular technology or hiring a particular service provider is consistent or compliant with the lawyer's professional obligations, a lawyer must engage in due diligence."

CONNECTICUT
Informal Opinion
2013-07

The Committee discussed several rules to be considered when engaged in this due diligence. They include:

- Rule 1.6(a) - the prohibition against revealing confidential information of a client
- Rule 1.15 - which requires that property of clients and third persons which the lawyer receives should be 'appropriately safeguarded.'
- Rule 5.3 - which addresses a lawyer's duties regarding nonlawyers employed or retained by / associated with a lawyer

This reference to Rule 5.3 seems to be the most important consideration for the Committee. In concluding its opinion, the Committee states that "the lawyer outsourcing cloud computing tasks...must exercise reasonable efforts to select a cloud service provider who...is able to limit authorized access to the data, ensure that the data is preserved...reasonably available to the lawyer, and reasonably safe from unauthorized intrusion."

The Professional Ethics Committee of the Florida Bar examined the issues surrounding lawyers' use of cloud computing because it "raises ethics concerns of confidentiality, competence, and proper supervision of nonlawyers."

FLORIDA Opinion 12-3

After identifying that confidentiality was the primary concern, the Committee stated that lawyers have an obligation "To maintain as confidential all information that relates to a client's representation, regardless of the source," and that obligation extends to ensuring the "confidentiality of information ... maintained by nonlawyers under the lawyer's supervision, including nonlawyers that are third parties used by the lawyer in the provision of legal services." Added to a lawyers obligation to remain current on developments in technology that affect the practice of law, the Committee concludes that lawyers using cloud technology "have an ethical obligation to understand the technology they are using and how it potentially impacts confidentiality of information relating to client matters, so that the lawyers may take appropriate steps to comply with their ethical obligations."

After a review of comparable ethics opinions from other state and local bars, the Committee determined that it agreed with their general finding: cloud computing is permissible "as long as the lawyer adequately addresses the potential risks associated with it."

The Committee goes on to favorably cite the New York State Bar Ethics Opinion 842 with regard to specific due diligence steps, and likewise notes Iowa's Ethics Opinion 11-01 which lists appropriate considerations including using secure passwords, encrypting where possible, and more.

Finally, the Committee adds an additional note that lawyers should "consider whether the lawyer should use the outside service provider or use additional security in specific matters in which the lawyer has proprietary client information or has other particularly sensitive information."

The Iowa State Bar Association's Ethics Committee evaluated the broad question of whether a lawyer or law firm may use cloud computing or Software as a Service (SaaS). The Committee chose to take a "reasonable and flexible approach to guide a lawyer's use of ever-changing technology" that "places on the lawyer the obligation to perform due diligence to assess the degree of protection that will be needed and to act accordingly."

The opinion stressed that lawyers wishing to use SaaS "must ensure that there is unfettered access to the data when it is needed" and that lawyers must also "determine the nature and degree of protection that will be afforded the data while residing elsewhere."

IOWA Opinion 11-01

In describing these two key requirements, the opinion explores a number of questions that lawyers may need to ask before using such a service, including questions about the legitimacy of the provider, the location where data will be stored, the ability to remove data from the service, and so forth. In terms of data protection, the opinion stresses the need to perform due diligence regarding password protection, access to data, and the ability to encrypt data used in such a service.

The opinion concludes by noting that performing due diligence "can be complex and requires specialized knowledge and skill," but allows that lawyers may discharge their ethical duties "by relying on the due diligence services of independent companies, bar associations or other similar organizations or through its own qualified employees."

MAINE
Opinion 207

In earlier Opinion 194, the Maine State Bar Association's Professional Ethics Commission conducted a limited review of confidential firm data held electronically and potentially handled by third-party vendors and technicians. Though not directly addressing the cloud, the opinion covered enough common issues that it was previously included in this comparison chart.

In January 2013, the Commission revisited the matter to "remove any uncertainty ... by squarely and formally addressing the issue" of cloud computing and storage. Overall, the Commission determined that use of such technology was permissible if "safeguards are in place to ensure that the attorney's use of this technology does not result in the violation of any of the attorney's obligations under the various Maine Rules of Professional Conduct."

As part of its review, the Commission noted that a number of rules were implicated by the use of cloud technology including 1.1, 1.3, 1.4, 1.6, 1.15, 1.16, 1.17, and 5.3. Yet at the same time, the Commission notes that the "overriding ethical constraints on counsel" have not changed with the evolution of technology; rather, the steps lawyers must take to satisfy those constraints have changed.

The Commission notes several internal policies and procedures that lawyers should consider to satisfy their obligations generally under the Rules, including backing up firm data, protecting the firm's network with a firewall, limiting information provided to third parties, and much more. The full list of suggested policies runs to 10 items and draws heavily on Pennsylvania Formal Opinion 2011-200.

In addition to these general suggestions regarding firm's technology, the Commission suggests that firm's should also carefully review the terms of service or SLA with providers and ensure adequate recognition of the lawyers' professional responsibilities. In addition, lawyers should ensure data will be accessible if the service is terminated and that data will be destroyed at the request of the firm. Finally, lawyers should review the provider's security and backup policies.

The Commission goes on to provide some specific guidance regarding how a lawyer may evaluate the provider's technology and terms, including determining ownership of data, the provider's ability to withstand infiltration attempts, and so on.

While the opinion includes several lengthy lists of suggested policies and steps to meet ethical obligations, the Commission is clear that the "dynamic nature of the technology make it impossible to list criteria that apply to all situations for all time" and thus adopts the view articulated by the North Carolina Ethics Committee that lawyers must stay educated "on computer technology as it changes and as it is challenged by and reacts to additional indirect factors such as third party hackers or technical failures."

In this opinion, the Massachusetts Bar Association examined cloud computing in the context of a lawyer who wished to synchronize his files, including confidential client files, between multiple computers using a solution like Google Docs. The MBA recognized that other options were available and drafted the opinion to generally address storage of data in "Internet based storage solutions."

Reviewing past opinions that dealt with electronic data and the duty to preserve confidentiality, the MBA Committee concluded that the "the use of an Internet based storage provider to store confidential client information would not violate Massachusetts Rule of Professional Conduct 1.6(a) in ordinary circumstances *as long as* Lawyer undertakes reasonable efforts to ensure that the provider's data privacy policies, practices and procedures are compatible with Lawyer's professional obligations." [Emphasis in the original.]

The MBA Committee goes on to list several examples of "reasonable efforts," including examining the provider's written policies and procedures regarding confidential data, ensuring that those terms prohibit unauthorized access to data, ensuring that the lawyer will have reasonable access to and control over

MASSACHUSETTS
Opinion 12-03

the data, examining the provider's security practices (e.g. encryption, password protection) and service history, and periodically revisiting these topics to ensure continued acceptability.

The Committee also stresses that a lawyer "remains bound to follow an express instruction from his client that the client's confidential information not be stored or transmitted by means of the Internet" and also that a lawyer "should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first seeking and obtaining the client's express consent to do so."

Finally, the Committee concludes by stating that ultimate responsibility for determining whether to use a cloud computing solution resides with the lawyer, who must make the determination "based on the criteria set forth in this opinion, the information that he is reasonably able to obtain regarding the relative security of the various alternatives that are available, and his own sound professional judgment."

Recognizing that technology has become pervasive in the practice, and that cloud computing in particular "is already a part of many devices" including smartphones and web-based email, New Hampshire sets out to explore the "effect on the lawyer's professional responsibilities."

The opinion focuses on four specific rules: Rule 1.1 Competence, Rule 1.6 Confidentiality, Rule 1.15 Safekeeping Property, and Rule 5.3 Responsibilities Regarding Nonlawyer Assistants. Beginning with Rule 1.1, the opinion notes that recent changes to the comments of ABA Model Rule 1.1 specifically reference the need to "keep abreast of changes in the law and its practice, including the benefits or risks associated with relevant technology." As a result, the opinion stresses that a competent lawyer wishing to use the cloud must understand and guard against the risks inherent to it, and must stay abreast of changes in the technology, privacy laws, and applicable regulations.

On Rule 1.6, the opinion again looks at recent changes to the ABA Model Rules, particularly the factors relating to the reasonableness of a lawyer's efforts to keep information confidential. As the relative sensitivity of the information is among those factors, and because not all information is alike, New Hampshire states that "consent of the client to use cloud computing may be necessary" where information is highly sensitive.

On Rule 1.15, the opinion discusses the need to safeguard the client's property--including the client file. Where the contents of that file are stored in the cloud, the lawyer must "take reasonable steps to ensure that the electronic data stored in the cloud is secure and available while representing a client," and that the data can be deleted from the cloud and returned to the client "after representation is concluded or when the lawyer decides to no longer preserve the file."

Finally on Rule 5.3, New Hampshire identifies cloud computing as a form of outsourcing and notes that this requires the lawyer to "make reasonable efforts to ensure that the provider understands and is capable of complying with its obligation to act in a matter compatible with the lawyer's own professional responsibilities." The opinion goes on to stress that this applies as well to any intermediaries the attorney may employ in selecting a provider - e.g. technology consultants or support staff.

While New Hampshire is clear that its opinion addresses a lawyer's obligations and not the technical requirements of the cloud providers, it does conclude with a list of issues which an attorney must address before using the cloud. These include checking the provider's reputation, assessing their security measures, and reviewing the terms of service among other factors.

The opinion from New Jersey's Advisory Committee on Professional Ethics does not focus on cloud-computing specifically, but on the more general topic of storing client files in digital format (e.g. PDF). The committee notes that per an earlier opinion (Opinion 692), certain types of documents are considered

**NEW
HAMPSHIRE**
Opinion 2012-13/4

NEW JERSEY Opinion 701

"property of the client" and therefore "cannot be preserved...merely by digitizing them in electronic form."

The Committee states, however, that "there is nothing in the RPCs that mandates a particular medium of archiving" for other common document types typically included in the client file, such as correspondence, pleadings, memoranda and briefs. Indeed, the Committee states that the lawyer's "paramount consideration is the ability to represent the client competently, and given the advances of technology, a lawyer's ability to discharge those duties may very well be enhanced by having client documents available in electronic form." The Committee goes on to state that putting client documents online through a secure website "has the potential of enhancing communications between lawyer and client, and promotes the values embraced in RPC 1.4."

The Committee does acknowledge that electronic document storage presents some risk of unauthorized access, and emphasizes that a lawyer's obligation to maintain client confidentiality "requires that the attorney take reasonable affirmative steps to guard against the risk of inadvertent disclosure." Reasonable care in this case "does not mean that the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all unauthorized access." When a lawyer entrusts confidential data to an outside party, however, the "touchstone" for reasonable care requires that "(1) the lawyer has entrusted such documents to an outside provider under circumstances in which there is an enforceable obligation to preserve confidentiality and security, and (2) use is made of available technology to guard against reasonably foreseeable attempts to infiltrate the data."

The New York State Bar Association's Committee on Professional Ethics examined the question of whether a lawyer could store client's confidential information online without violating professional responsibility rules, and if so, what steps the lawyer should take to ensure the data remains secure.

The Committee stresses that a lawyer's duty to maintain client confidentiality includes an affirmative duty to exercise reasonable care in protecting confidential data. This includes exercising reasonable care to prevent inadvertent disclosure by attorney's staff, but does not mean "that the lawyer guarantees that the information is secure from *any* unauthorized access." The Committee notes that "the exercise of reasonable care may differ from one case to the next" based on the sensitivity of the data.

NEW YORK Opinion 842

Using online data storage to backup (i.e. preserve) client data is deemed ethically permissible where the lawyer has exercised reasonable care "to ensure that the system is secure and that client confidentiality will be maintained." The Committee suggests that this might include ensuring that the vendor has an enforceable obligation to preserve confidentiality and security and will notify the lawyer if served with process requiring production of client data, investigating the vendor's security and backup procedures, and using available technology to guard against reasonably foreseeable attempts to infiltrate it.

The Committee also writes that lawyers "should periodically reconfirm that the vendor's security measures remain effective in light of advances in technology." If the vendor's methods are insufficient or if the lawyer learns of any breaches affecting the vendor, the lawyer must investigate to be sure his or her clients' data wasn't compromised and if necessary discontinue use of the vendor's service. Lawyers should also stay abreast of general developments in technology insofar as they impact the transmission or storage of electronic files.

The State Bar of Nevada's Standing Committee on Ethics and Professional Responsibility examined whether a lawyer violated their professional responsibility rules "by storing confidential client information and/or communications, without client consent, in an electronic format on a server or other device that is not exclusively in the lawyer's control."

NEVADA
Opinion 33

The Committee provided that a lawyer "must act competently to safeguard against inadvertent or unauthorized disclosure of confidential client information" by taking "reasonable precautions." The Committee likened the storage of data online to the storage of paper documents in a third-party warehouse, and stated that this was permissible "so long as the attorney observes the usual obligations applicable to such arrangements." This would include, for example, choosing a vendor that "can be reasonably relied upon to maintain the confidentiality" of client data.

The opinion also noted that client consent isn't necessary, but that a client "may give informed consent to a means of protection that might otherwise be considered insufficient."

The North Carolina State Bar's Ethics Committee examined two broad questions in its opinion on cloud computing: first, may a lawyer use cloud computing or software as a service, and second, what measures should a lawyer consider when evaluating a vendor or seeking to reduce the risks associated with the cloud?

On the first subject, the Committee's answer is straightforward: yes, lawyers may use the cloud, "provided steps are taken to minimize the risk of inadvertent or unauthorized disclosure of confidential client information and to protect client property." In taking these steps, the lawyer should apply "the same diligence and competency to manag[ing] the risks of SaaS that the lawyer is required to apply when representing clients."

On the broader question of the appropriate measures a lawyer should take, the Committee begins by stating that it "does not set forth specific security requirements because mandatory security measures would create a false sense of security in an environment where the risks are continually changing." Rather, the Committee urges lawyers to exercise due diligence and educate themselves regularly about the subject.

The Committee does recommend several security measures, however, which includes reviewing applicable terms and policies, and if necessary, negotiating terms regarding how confidential data will be handled. The Committee also suggests that the lawyer have a method of retrieving data if they leave the service or the vendor goes out of business, that the lawyer review the vendor's backup strategy, and finally that the lawyer evaluate the vendor's overall security measures.

The OSBA Informal Advisory Opinion examines a question of "whether [a] law firm may use a third-party vendor to store client data 'in the cloud.'" While acknowledging that previous opinions and rules have traditionally examined "older data storage methods," the Professional Committee writes that the "issues and ethical duties regarding cloud storage are analogous to the ones that apply when lawyers opt to use a vendor to store their paper files offsite rather than in their own offices."

Thus, the Committee opts to take a "practical" approach by "applying existing principles to new technological advances while refraining from mandating specific practices." More specifically, the Committee notes that rules about specific security measures would be superseded quickly by technological advances.

The Committee addresses the matter in four areas. First, it states that lawyers must "exercise 'due diligence as to the qualifications and reputation of those to whom services are outsourced,' and also as to whether the outside vendor will itself provide the requested services competently and diligently." The Committee specifically suggests a Service Level Agreement and offers some guidance on the types of questions that vendors should be asked.

Next, the Committee looks at confidentiality and states that lawyers have a "duty...to maintain the confidentiality of all client data relating to the representation, irrespective of the form of that data, and to carry out that duty with due regard for the form that the data is in." To preserve the

**NORTH
CAROLINA**
2011 Formal Ethics
Opinion 6

OHIO
Informal Advisory
Opinion 2013-03

confidentiality, a lawyer must exercise competence "(1) in selecting an appropriate vendor, (2) in staying abreast of technology issues that have an impact on client data storage and (3) in considering whether any special circumstances call for extra protection for particularly sensitive client information or for refraining from using the cloud to store such particularly sensitive data." The Committee notes that terms of service that provide or suggest that the vendor has an ownership interest in the data "would violate the duty to keep client property 'identified as such'."

Third, the Committee looks at supervision of cloud vendors and states that putting data in the cloud "is almost by definition a service that lawyers will out-source," thus "lawyers who contract with a cloud-storage vendor must make reasonable efforts to ensure that the vendor's conduct is compatible with the lawyer's own professional obligations." On the fourth and final issue, the Committee states that lawyers should use judgment to determine if the circumstances require consultation with the client regarding the use of cloud computing. That might arise where the data is of a particularly sensitive nature.

The Oregon Committee found that a lawyer "may store client materials on a third-party server as long as Lawyer complies with the duties of competence and confidentiality to reasonably keep the client's information secure within a given situation." That compliance requires "reasonable steps" to ensure that the storage company will secure the client data and preserve its confidentiality.

The Committee stated that in some circumstances it may be sufficient for the vendor to be compliant with "industry standards relating to confidentiality and security," but only where those standards "meet the minimum requirements imposed on the Lawyer by the Oregon RPCs.

As examples of these requirements, the Committee suggests that lawyers should ensure that "the service agreement requires the vendor to preserve the confidentiality and security of the materials," and that the vendor notify the lawyer if there's any non authorized third-party access to the lawyer's files. The opinion also suggests that lawyers should "investigate how the vendor backs up and stores its data and metadata."

Finally, the Committee notes that the reasonableness of the lawyer's protective measures will be judged based on the technology available at the time of disclosure. In other words, the "vendor's protective measures may become less secure or obsolete over time" and therefore the lawyer must reevaluate the measures periodically.

The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility begins its opinion by recognizing that advances in technology, including the cloud, offer opportunities to "reduce costs, improve efficiency and provide better client service." There's also a genuine risk of data breach, particularly given a recent FBI warning that law firms are "being specifically targeted by hackers who have designs on accessing the firms' databases."

Noting that an earlier informal opinion (2010-060) had found that a lawyer may "ethically allow client confidential material to be stored in 'the cloud' provided the attorney makes reasonable efforts to protect confidential electronic communications and information," the Committee dedicates most of this formal opinion to addressing the nature of those "reasonable" efforts.

The Committee provides a 15 point list of possible steps a firm "may" take in exercising reasonable care with cloud computing. Several of these steps are routine elements of preserving client confidentiality (e.g. "[r]efusing to disclose confidential information to unauthorized individuals (including family members and friends) without client permission"), but others focus on specific technology issues:

- Backing up firm data and maintaining onsite copies;
- Using encryption to protect confidential data, including backups;

OREGON Opinion 2011-188

PENNSYLVANIA

Opinion 2011-200

- Developing a plan to address security breaches, including possible notifications to clients;
- Evaluating the vendor regarding data ownership, security precautions, the location of data centers, data portability, and more;
- Providing training to firm staff that will use the cloud tool, including instruction on password best practices;
- Having an backup internet connection.

Pennsylvania attorneys should review the *full list* published in the opinion.

The opinion goes on to stress that "some data may be too important to risk inclusion in cloud services," and also notes that most states have data breach notification laws that lawyers should be familiar with and adhere to in the event that a data breach occurs.

The opinion also addresses the question of web-based email, which the Pennsylvania Committee lists as a type of cloud computing. It suggests that attorneys take reasonable precautions "to minimize the risk of unauthorized access to sensitive client information" when using webmail, possibly including specific steps like "encryption and strong password protection"--especially when the data is of a particularly sensitive nature.

The Vermont Bar Association's Professional Responsibility Section addressed the "propriety of use by attorneys and law firms of Software as a Service ("SaaS") which is also known as Cloud Computing." In its analysis, it looked at storing client data in the cloud, possible data types that should not be stored online, as well as specific Cloud uses such as web-based email, calendaring, and remote document synchronization.

A significant portion of the Section's analysis is focused on reviewing other recent cloud computing ethics opinions from other jurisdictions, including North Carolina, California, and New York. Drawing upon these opinions and its own analysis, the Section "agrees with the consensus view" that lawyers are obligated to provide "competent representation" while "maintaining confidentiality of client information, and protecting client property in their possession." In choosing whether to use new technologies, including the cloud, lawyers must exercise their due diligence. The Section provides a list of steps a lawyer may take, though it stresses that is not providing a formal "checklist of factors a lawyer must examine."

This loose list of factors includes reviewing the vendor's security, checking for limitations on access to or protection of data, reviewing terms of service, examining vendor confidentiality policies, weighing the sensitivity of data placed in the cloud, reviewing other regulatory obligations, and requiring notice if a third party accesses or requests access to data.

In addition to those factors, the Section adds that a lawyer may consider giving notice to the client when using the cloud to store client's data, and may want to look to expert third parties to review the vendor's security and access systems. Finally, the Section stresses that lawyers should take "reasonable measures to stay apprised of current developments regarding SaaS systems and the benefits and risks they present."

Virginia Legal Ethics Opinion 1872 examines a variety of ethical issues associated with virtual law offices, including the use of cloud computing. This summary focuses specifically on the elements of the opinion dealing with cloud computing, but readers are encouraged to view the full text of the opinion to understand the context.

The opinion begins by stating that lawyers "must always act competently to protect the confidentiality of client information, regardless of how that information is stored/transmitted," but notes that the task may be more challenging when the information is being "transmitted and/or stored

VERMONT
Opinion 2010-6

VIRGINIA
Legal Ethics
Opinion 1872

electronically through third-party software and storage providers."

The opinion notes that the duty is not to "absolutely guarantee that a brief of confidentiality cannot occur," only to "act with reasonable care to protect information relating to the representation of a client."

Specifically, lawyers are instructed to carefully select vendors, instruct the vendor to preserve confidentiality, and to have a reasonable expectation that the vendor will in fact keep data confidential and inaccessible. To do that, lawyers must "examine the third party provider's use of technology and terms of service" and, if they're unable to make an assessment on their own, "consult with someone qualified to make that determination."

In Advisory Opinion 2215, the Washington State Bar Association's Rules of Professional Conduct Committee examined lawyers' ethical obligations relating "to the use of online data storage managed by third party vendors to store confidential client documents." The opinion focused specifically on data storage rather than the broader category of cloud computing, but addressed many issues common to both platforms.

In its analysis, the Committee noted that such an arrangement places "confidential client information ... outside of the direct control of the lawyer" and thus raises some concern. In particular, the Committee notes lawyers' obligations to preserve confidentiality under RPC 1.6 and to protect client property under RPC 1.15A.

Acknowledging that specific guidelines regarding security are impossible "because the technology is changing too rapidly," and also noting that it's "impractical to expect every lawyer who uses such services to be able to understand the technology sufficiently in order to evaluate a particular service provider's systems," the Committee nonetheless suggested that a lawyer must conduct a due diligence investigation of the provider and "cannot rely on lack of technological sophistication to excuse the failure to do so."

The Committee offered several steps to conduct such a due diligence investigation, including familiarizing oneself with the risks of online data storage, evaluating the provider's history, comparing terms with other providers, ensuring notice of any non-authorized access to lawyer's data, and generally ensuring that data is secured and backed up.

Finally, the Committee also noted that under RPC 1.1 a lawyer has a duty to stay abreast of changes in the law and its practice, and that necessarily includes staying informed about the risks associated with the technology the lawyer employs in his or her practice. As technology evolves, the lawyer must also "monitor and regularly review the security measures of the provider" he or she uses for online data storage.

Wisconsin Formal Ethics Opinion EF-15-01 (Ethical Obligations of Attorneys Using Cloud Computing), issued by the State Bar of Wisconsin's Professional Ethics Committee, notes that increased lawyer accessibility to cloud-based platforms and services comes with a direct loss of control over client information but that lawyers can use cloud computing services if the lawyer uses reasonable efforts to adequately address the potential risks associated with it. "To be reasonable," the opinion states, "the lawyer's efforts must be commensurate with the risks presented." The opinion acknowledges that lawyers cannot guard against every conceivable danger when using cloud-based services, but lists numerous factors to consider when assessing the risk of using cloud-based services in their practices:

- The information's sensitivity
- The client's instructions and circumstances
- The possible effect that inadvertent disclosure or unauthorized interception could pose to a client or third party

WASHINGTON
Advisory Opinion
2215

WISCONSIN
Opinion EF-15-01

- The attorney's ability to assess the technology's level of security
- The likelihood of disclosure if additional safeguards are not employed
- The cost of employing additional safeguards
- The difficulty of implementing the safeguards
- The extent to which the safeguards adversely affect the lawyer's ability to represent clients
- The need for increased accessibility and the urgency of the situation
- The experience and reputation of the service provider
- The terms of the agreement with the service provider
- The legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality

The opinion also states that in determining what efforts are reasonable to address the cloud-computing risk, lawyers should understand a number of computer security concepts:

- Firewalls
- Virus and spyware programs
- Operating system updates
- Strong passwords and multifactor identification
- Encryption for stored information
- Dangers of using public wi-fi
- Risks of file-sharing sites
- Options for using a virtual private network (VPN)
- The importance of regularly backing up data

5 May 1999. Thanks to PK.

Source: <http://www.abanet.org/cpr/fo99-413.html>

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion No. 99-413

March 10, 1999

Protecting the Confidentiality of Unencrypted E-Mail

A lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct (1998) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint. The same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail. A lawyer should consult with the client and follow her instructions, however, as to the mode of transmitting highly sensitive information relating to the client's representation.

The Committee addresses in this opinion the obligations of lawyers under the Model Rules of Professional Conduct (1998) when using unencrypted electronic mail to communicate with clients or others about client matters. The Committee (1) analyzes the general standards that lawyers must follow under the Model Rules in protecting "confidential client information"¹ from inadvertent disclosure; (2) compares the risk of interception of unencrypted e-mail with the risk of interception of other forms of communication; and (3) reviews the various forms of e-mail transmission, the associated risks of unauthorized disclosure, and the laws affecting unauthorized interception and disclosure of electronic communications.

The Committee believes that e-mail communications, including those sent unencrypted over the Internet, pose no greater risk of interception or disclosure than other modes of communication commonly relied upon as having a reasonable expectation of privacy. The level of legal protection accorded e-mail transmissions, like that accorded other modes of electronic communication, also supports the reasonableness of an expectation of privacy for unencrypted e-mail transmissions. The risk of unauthorized interception and disclosure exists in every medium of communication, including e-mail. It is not, however, reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible, especially when unauthorized interception or dissemination of the information is a violation of law.²

The Committee concludes, based upon current technology and law as we are informed of it, that a lawyer sending confidential client information by unencrypted e-mail does not violate Model Rule 1.6(a) in choosing that mode to communicate. This is principally because there is a reasonable expectation of privacy in its use.

The conclusions reached in this opinion do not, however, diminish a lawyer's obligation to consider with her client the sensitivity of the communication, the costs of its disclosure, and the relative security of the contemplated medium of communication. Particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters. Those measures might include the avoidance of e-

mail,³ just as they would warrant the avoidance of the telephone, fax, and mail. See Model Rule 1.1 and 1.4(b). The lawyer must, of course, abide by the client's wishes regarding the means of transmitting client information. See Model Rule 1.2(a).

A. Lawyers' Duties Under Model Rule 1.6

The prohibition in Model Rule 1.6(a) against revealing confidential client information absent client consent after consultation imposes a duty on a lawyer to take reasonable steps in the circumstances to protect such information against unauthorized use or disclosure.⁴ Reasonable steps include choosing a means of communication in which the lawyer has a reasonable expectation of privacy.⁵ In order to comply with the duty of confidentiality under Model Rule 1.6, a lawyer's expectation of privacy in a communication medium need not be absolute; it must merely be reasonable.

It uniformly is accepted that a lawyer's reliance on land-line telephone, fax machine, and mail to communicate with clients does not violate the duty of confidentiality because in the use of each medium, the lawyer is presumed to have a reasonable expectation of privacy.⁶ The Committee now considers whether a lawyer's expectation of privacy is any less reasonable when she communicates by e-mail.

B. Communications Alternatives To E-Mail

In order to understand what level of risk may exist without destroying the reasonable expectation of privacy, this Section evaluates the risks inherent in the use of alternative means of communication in which lawyers nonetheless are presumed to have such an expectation. These include ordinary U.S. mail; land-line, cordless, and cellular telephones; and facsimile transmissions.

1. U.S. and Commercial Mail

It uniformly is agreed that lawyers have a reasonable expectation of privacy in communications made by mail (both U.S. Postal Service and commercial). This is despite risks that letters may be lost, stolen or misplaced at several points between sender and recipient. Further, like telephone companies, Internet service providers (ISPs), and on-line service providers (OSPs), mail services often reserve the right to inspect the contents of any letters or packages handled by the service. Like e-mail, U.S. and commercial mail can be intercepted and disseminated illegally. But, unlike unencrypted e-mail, letters are sealed and therefore arguably more secure than e-mail.⁷

2. Land-Line Telephones

It is undisputed that a lawyer has a reasonable expectation of privacy in the use of a telephone.⁸

For this reason, the protection against unreasonable search and seizure guaranteed by the Fourth Amendment applies to telephone conversations.⁹ It also is recognized widely that the attorney-client privilege applies to conversations over the telephone as long as the other elements of the privilege are present.¹⁰ However, this expectation of privacy in communications by telephone must be considered in light of the substantial risk of interception and disclosure inherent in its use. Tapping a telephone line does not require great technical sophistication or equipment, nor is the know-how difficult to obtain.¹¹

Multiple extensions provide opportunities for eavesdropping without the knowledge of the speakers. Technical errors by the phone company may result in third parties listening to private conversations. Lastly, phone companies are permitted by law to monitor phone calls under limited conditions.

Despite this lack of absolute security in the medium, using a telephone is considered to be consistent with the duty to take reasonable precautions to maintain confidentiality.¹²

3. Cordless and Cellular Phones

Authority is divided as to whether users have a reasonable expectation of privacy in conversations made over cordless and cellular phones.¹³ Some court decisions reached the conclusion that there is no reasonable expectation of privacy in cordless phones in part because of the absence, at the time, of federal law equivalent to that which protects traditional telephone communications.¹⁴ After the 1994 amendment to the Wiretap Statute, which extended the same legal protections afforded regular telephone communications to cordless phone conversations,¹⁵ at least one ethics opinion addressed the advisability of using cordless phones to communicate with clients and concluded that their use does not violate the duty of confidentiality.¹⁶

The nature of cordless and cellular phone technology exposes it to certain risks that are absent from e-mail communication. E-mail messages are not "broadcast" over public airwaves.¹⁷ Cordless phones, by contrast, rely on FM and AM radio waves to broadcast signals to the phone's base unit, which feeds the signals into land-based phone lines. Therefore, in addition to the risks inherent in the use of a regular telephone, cordless phones also are subject to risks of interception due to their broadcast on radio signals that may be picked up by mass-marketed devices such as radios, baby monitors, and other cordless phones within range.¹⁸ Further, the intercepted signals of cordless and analog cellular telephones are in an instantly comprehensible form (oral speech), unlike the digital format of e-mail communications.

Similarly, cellular phones transmit radio signals to a local base station that feeds the signals into land-based phone lines. The broadcast area from the phone to the station is larger than that of a cordless phone, and receivers and scanners within range may intercept and overhear the conversation. Although the Committee does not here express an opinion regarding the use of cellular or cordless telephone, it notes that the concerns about the expectation of privacy in the use of cordless and cellular telephones do not apply to e-mail transmitted over land-based phone lines.¹⁹

4. Facsimile

Authority specifically stating that the use of fax machines is consistent with the duty of confidentiality is absent, perhaps because, according to some commentators, courts assume the conclusion to be self-evident.²⁰ Nonetheless, there are significant risks of interception and disclosure in the use of fax machines. Misdirection may result merely by entering one of ten digits incorrectly. Further, unlike e-mail, faxes often are in the hands of one or more intermediaries before reaching their intended recipient, including, for example, secretaries, runners, and mailroom employees. In light of these risks, prudent lawyers faxing highly sensitive information should take heightened measures to preserve the communication's confidentiality.

C. Characteristics Of E-Mail Systems

The reasonableness of a lawyer's use of any medium to communicate with or about clients depends both on the objective level of security it affords and the existence of laws intended to protect the privacy of the information communicated. We here examine the four most common types of e-mail and compare the risks inherent in their use with those of alternative means of communication, including the telephone (regular, cordless and cellular), fax, and mail.

Like many earlier technologies, "e-mail" has become a generic term that presently encompasses a variety of systems allowing communication among computer users. Because the security of these e-mail systems is not uniform, the Committee here evaluates separately the degree of privacy afforded by each. As set forth below, we conclude that a lawyer has a reasonable expectation of privacy in such use.

1. "Direct" E-Mail²¹

Lawyers may e-mail their clients directly (and vice versa) by programming their computer's modem to dial their client's. The modem simply converts the content of the e-mail into digital information that is carried on land-based phone lines to the recipient's modem, where it is reassembled back into the message. This is virtually indistinguishable from the process of sending a fax: a fax machine dials the number of the recipient fax machine and digitally transmits information to it through land-based phone lines. Because the information travels in digital form, tapping a telephone line to intercept an e-mail message would require more effort and technical sophistication than would eavesdropping on a telephone conversation by telephone tap.

Based on the difficulty of intercepting direct e-mail, several state bar ethics opinions and many commentators recognize a reasonable expectation of privacy in this form of e-mail.²² Further, in two recent federal court decisions, the attorney-client and work-product privileges were considered applicable to e-mail communications.²³ The Committee agrees that there is a reasonable expectation of privacy in this mode of communication.

2. "Private System" E-Mail

A "private system" includes typical internal corporate e-mail systems and so-called "extranet" networks in which one internal system directly dials another private system. The only relevant distinction between "private system" and "direct" e-mail is the greater risk of misdirected e-mails in a private system. Messages mistakenly may be sent throughout a law firm or to unintended recipients within the client's organization. However, all members of a firm owe a duty of confidentiality to each of the firm's clients.²⁴ Further, unintended disclosures to individuals within a client's private e-mail network are unlikely to be harmful to the client.

The reliance of "private system" e-mail on land-based phone lines and its non-use of any publicly accessible network renders this system as secure as direct e-mail, regular phone calls, and faxes. As a result, there is a widespread consensus that confidentiality is not threatened by its use,²⁵ and the Committee concurs.

3. On-line Service Providers

E-mail also may be provided by third-party on-line service providers or "OSPs."²⁶ Users typically are provided a password-protected mailbox from which they may send and retrieve e-mail.

There are two features of this system that distinguish it from direct and private-system e-mail. First, user mailboxes, although private, exist in a public forum consisting of other fee-paying users. The added risk caused by the existence of other public users on the same network is that misdirected e-mails may be sent to unknown users. Unlike users of private system e-mail networks who, as agents of their employers, owe a duty of confidentiality to them and, in the case of a law firm, to all firm clients, the inadvertent user owes no similar duties.²⁷ The risk of misdirection is, however, no different from that which exists when sending a fax. Further, the misdirection of an e-mail to another OSP can be avoided with reasonable care.²⁸

The second distinctive feature of e-mail administered by an OSP is that the relative security and confidentiality of user e-mail largely depends on the adequacy of the particular OSP's security measures meant to limit external access and its formal policy regarding the confidentiality of user e-mail. Together, they will determine whether a user has a reasonable expectation of privacy in this type of e-mail.

The denial of external access ordinarily is ensured by the use of password-protected mailboxes or encryption²⁹. The threat to confidentiality caused by the potential inspection of users' e-mail by OSP system administrators who must access the e-mail for administrative and compliance purposes is overcome by the adoption of a formal policy that narrowly restricts the bases on which system administrators³⁰ and OSP agents^{31 32} are permitted to examine user e-mail.

Moreover, federal law imposes limits on the ability of OSP administrators to inspect user e-mail, irrespective of the OSP's formal policy. Inspection is limited by the ECPA to purposes "necessary to the rendition of services" or to the protection of "rights or property."³³ Further, even if an OSP administrator lawfully inspects user e-mail within the narrow limits defined by the ECPA, the disclosure of those communications for purposes other than those provided by the statute is prohibited.³⁴

Accordingly, the Committee concludes that lawyers have a reasonable expectation of privacy when communicating by e-mail maintained by an OSP, a conclusion that also has been reached by at least one case as well as state bar ethics committees and commentators.³⁵

4. Internet E-Mail

E-mail may be sent over the Internet between service users without interposition of OSPs. Internet e-mail typically uses land-based phone lines and a number of intermediate computers randomly selected to travel from sender to recipient. The intermediate computers consist of various Internet service providers or "routers" that maintain software designed to help the message reach its final destination.

Because Internet e-mail typically travels through land-based phone lines, the only points of unique vulnerability consist of the third party-owned Internet services providers or "ISPs," each capable of copying messages passing through its network. Confidentiality may be compromised by (1) the ISP's legal, though qualified, right to monitor e-mail passing through or temporarily stored in its network, and (2) the illegal interception of e-mail by ISPs or "hackers."³⁶

The ISPs' qualified inspection rights are identical to those of OSPs.³⁷ The same limits described above therefore apply to ISPs. In addition, the provider of an electronic communications service may by law conduct random monitoring only for mechanical or service quality control checks.³⁸

The second threat to confidentiality is the illegal interception of e-mail, either by ISPs exceeding their qualified monitoring rights or making unauthorized disclosures, or by third party hackers who use ISPs as a means of intercepting e-mail. Although it is difficult to quantify precisely the frequency of either practice, the interception or disclosure of e-mail in transit or in storage (whether passing through an ISP or in any other medium) is a crime and also may result in civil liability.³⁹

In addition to criminalization, practical constraints on the ability of third parties and ISPs to capture and read Internet e-mail lead to the conclusion that the user of Internet e-mail has a reasonable expectation of privacy. An enormous volume of data travelling at an extremely high rate passes through ISPs every hour. Further, during the passage of Internet e-mail between sender and recipient, the message ordinarily is split into fragments or "packets" of information. Therefore, only parts of individual messages customarily

pass through ISPs, limiting the extent of any potential disclosure. Because the specific route taken by each e-mail message through the labyrinth of phone lines and ISPs is random, it would be very difficult consistently to intercept more than a segment of a message by the same author.

Together, these characteristics of Internet e-mail further support the Committee's conclusion that an expectation of privacy in this medium of communication is reasonable. The fact that ISP administrators or hackers are capable of intercepting Internet e-mail - albeit with great difficulty and in violation of federal law - should not render the expectation of privacy in this medium any the less reasonable, just as the risk of illegal telephone taps does not erode the reasonable expectation of privacy in a telephone call.⁴⁰

CONCLUSION

Lawyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure. It therefore follows that its use is consistent with the duty under Rule 1.6 to use reasonable means to maintain the confidentiality of information relating to a client's representation.

Although earlier state bar ethics opinions on the use of Internet e-mail tended to find a violation of the state analogues of Rule 1.6 because of the susceptibility to interception by unauthorized persons and, therefore, required express client consent to the use of e-mail, more recent opinions reflecting lawyers' greater understanding of the technology involved approve the use of unencrypted Internet e-mail without express client consent.

Even so, when the lawyer reasonably believes that confidential client information being transmitted is so highly sensitive that extraordinary measures to protect the transmission are warranted, the lawyer should consult the client as to whether another mode of transmission, such as special messenger delivery, is warranted. The lawyer then must follow the client's instructions as to the mode of transmission. See Model Rule 1.2(a).

ENDNOTES

1 As used in this opinion, "confidential client information" denotes "information relating to the representation of a client" under Model Rule 1.6(a), which states:

(a) a lawyer shall not reveal information relating to representation of a client unless a client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation.

2 The Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986), amended the Federal Wiretap Statute of 1968 by extending its scope to include "electronic communications." 18 U.S.C.A. (2510, et seq. (1998) (the "ECPA"). The ECPA now commonly refers to the amended statute in its entirety. The ECPA provides criminal and civil penalties for the unauthorized interception or disclosure of any wire, oral, or electronic communication. 18 U.S.C.A. (2511.

3 Options other than abandoning e-mail include using encryption or seeking client consent after apprising the client of the risks and consequences of disclosure.

4 See also RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS (112 cmt. d (Proposed Official Draft 1998), which provides that confidential client information must be "acquired, stored, retrieved, and transmitted under systems and controls that are reasonably designed and managed to maintain confidentiality."

5 Whether a lawyer or a client has a reasonable expectation of privacy also governs whether a communication is "in confidence" for purposes of the attorney-client privilege. As a result, analysis under the attorney-client privilege is often relevant to this opinion's discussion of e-mail and the duty of confidentiality. The relevance of privilege is not exhaustive, however, because of its more restrictive application in prohibiting the introduction of privileged communications between a lawyer and client in any official proceeding. In contrast to the requirement imposed by the duty of confidentiality to avoid disclosing any information "relating to the representation" of the client, see Model Rule 1.6(a), *supra* n.1, the attorney-client privilege applies only to actual "communications" made "in confidence" by the client to the lawyer. See JOHN H. WIGMORE, 8 EVIDENCE § 2295 (McNaughton rev. 1961).

6 See *infra* Section B. It should be noted that a lawyer's negligent use of any medium - including the telephone, mail and fax - may breach the duty of confidentiality. The relevant issue here, however, is whether, despite otherwise reasonable efforts to ensure confidentiality, breach occurs solely by virtue of the lawyer's use of e-mail.

7 A.C.L.U. v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996), *aff'd* 521 U.S. 844 (1997) ("Unlike postal mail, simple e-mail is not 'sealed' or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted).").

8 Frequently, what we understand to be regular or land-line telephone conversations are transmitted in part by microwave. For example, many corporate telephone networks are hard-wired within a building and transmitted by microwave among buildings within a corporate campus to a central switch connected by land-line or microwave to a local or interstate carrier.

9 It should be noted that the ECPA preserves the privileged character of any unlawfully intercepted "wire, oral, or electronic communication." 18 U.S.C.A. (2517(4). The inclusion of e-mail in this provision is important for two reasons. First, implicit in this provision is the assumption that electronic communications are capable of transmitting privileged material. To argue that the use of e-mail never is "in confidence" or constitutes an automatic waiver of otherwise privileged communications therefore appears to be inconsistent with an assumption of this provision of federal law. Second, the identical federal treatment of e-mail with other means of communication long assumed consistent with the maintenance of privilege likewise is inconsistent with the assertion that the use of e-mail poses unique threats to privileged communications.

10 See Peter R. Jarvis & Bradley F. Tellam, High-Tech Ethics and Malpractice Issues 7 (1996) (paper delivered at the 22nd National Conference on Professional Responsibility, May 30, 1996, in Chicago, Illinois) (on file with its author), reported in 1996 SYMPOSIUM ISSUE OF THE PROFESSIONAL LAWYER, 51, 55 (1996) (hereafter "Jarvis & Bradley"); David Hricik, E-mail and Client Confidentiality: Lawyers Worry Too Much about Transmitting Client Confidences by Internet E-mail, 11 GEO. J. LEGAL ETHICS 459, 479 (1999) (hereafter "Hricik").

11 See Jarvis & Tellam *supra* n.10, at 57; Hricik *supra* n.10, at 480.

12 See Hricik *supra* n.10, at 481.

13 See, e.g., Jarvis & Tellam *supra* n.10, at 59-61; Hricik *supra* n.10, at 481-85. Compare Mass. Ethics Opinion 94-5 (1994) (if risk of disclosure to third party is "nontrivial," lawyer should not use cellular phone); N.C. Ethics Op. 215 (1995) (advising lawyers to use the mode of communication that best will maintain confidential information); State Bar of Arizona Advisory Op. 95-11 (1995) (lawyers should exercise caution before using cellular phones to communicate client confidences) with United States v. Smith, 978 F.2d 171, 180 (5th Cir. 1992) (finding that there may be reasonable expectation of privacy in

cordless phone communications for Fourth Amendment purposes).

14 *McKarney v. Roach*, 55 F.3d 1236, 1238-9 (6th Cir. 1995), cert. denied, 576 U.S. 944 (1995); *Askin v. United States*, 47 F.3d 100, 103-04 (4th Cir. 1995).

15 By 1986, the protection under federal law for cellular phone communications was equal to traditional land-line telephone communications. The Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 202(a), 108 Stat. 4279 (1994), deleted previous exceptions under the Federal Wiretap Act that limited the legal protections afforded cordless phone communications under 18 U.S.C.A. ((2510(1), 2510(12) (A). Existing law criminalizes the intentional and unauthorized interception of both cordless and cellular phone communications, 18 U.S.C.A. (2511; the privileged status of the communication preserves in the event of intentional interception, 18 U.S.C.A. (2517(4); and bars the introduction of the unlawful interception as evidence at trial even if it is not privileged, 18 U.S.C.A. (2515.

16 State Bar of Arizona Advisory Op. 95-11 (1995). Some commentators have argued that in light of the 1994 amendment and the recent improvements in the security of both media (including the introduction of digital cellular phones), the expectation of privacy in communications by cordless and cellular telephones should not be considered unreasonable. *Jarvis & Tellam supra n.10*, at 60-61. See also *Hricik supra n.10*, at 483, 485 (arguing that despite the fact that their privileged status would not be lost if cellular and cordless phone conversations were intercepted, lawyers should consider whether the cost of potential disclosure is outweighed by the benefit derived from the use of cordless or cell phones). Further, 18 U.S.C.A. (2512 prohibits the manufacture and possession of scanners capable of receiving cellular frequencies, and cordless and cellular phone communications have been afforded greater legal protection under several recent state court decisions. See, e.g., *State v. Faford*, 128 Wash.2d 476, 485-86, 910 P.2d 447, 451-52 (1996) (reversing trial court's admission of defendants' cordless phone conversations violated state privacy act because defendants had reasonable expectation of privacy in such communication); *State v. McVeigh*, 224 Conn. 593, 622, 620 A.2d 133, 147 (1995) (reversing trial court's admission of defendants' cordless telephone conversations because such communications were within scope of state law forbidding the intentional interception of wire communications).

17 *Hricik supra n.10*, at 497.

18 See *United States v. Maxwell* 42 M.J. 568, 576, 43 Fed. R. Evid. Serv. (Callaghan) 24 (A. F. Ct. Crim. App. 1995) (holding that user of e-mail maintained by OSP was protected against warrantless search of e-mails because user had reasonable expectation of privacy in such communications, unlike cordless phone communication) *aff'd in part and rev'd in part*, 45 M.J. 406 (U.S. Armed Forces 1996) (expectation of privacy exists in e-mail transmissions made through OSP).

19 The risks of interception and disclosure may be lessened by the recent introduction of digital cellular phones, whose transmissions are considered more difficult to intercept than their analog counterparts. New communications technology, however, does not always advance privacy concerns. The use of airplane telephones, for example, exposes users to the interception risks of cellular telephones as well as a heightened risk of disclosure due to eavesdropping on the airplane itself. Most recently, a world-wide, satellite-based cellular telephone system called Iridium has been introduced by Motorola. The principles articulated in this opinion should be considered by a lawyer when using such systems.

20 See, e.g., Practice Guide, Electronic Communications, in ABA/BNA LAWYERS' MANUAL ON PROFESSIONAL CONDUCT 55:403 (1996) ("[C]ourts seem to have taken it for granted that fax machines may be used [to transmit confidential information]," citing *State ex rel. U.S. Fidelity and Guar. Co. v. Canady*, 144 W.Va. 431, 443-44, 460 S.E.2d 677, 689-90 (1995) (holding that faxed communication was protected by the attorney-client privilege)). See also *Jarvis & Tellam supra n.10*, at

61 ("[T]here seems to be no question that faxes are subject to the attorney-client privilege . . . no one asserts that the use of a fax machine or the possibility of misdirection destroys any hope of a claim of privilege," citing ABA Comm. on Ethics and Professional Responsibility, Formal Ops. 94-382 and 92-368).

21 The names for the varieties of e-mail described in this section of the opinion are based on those used by Hricik, *supra* n.10, at 485-92.

22 See, e.g., Alaska Bar Ass'n Op. 98-2 (1998); Ill. State Bar Ass'n Advisory Op. on Professional Conduct No. 96-10 (1997); S.C. Bar Ethics Advisory Comm. Op. No. 97-08 (1997); Vermont Advisory Ethics Op. No. 97-5 (1997). See also, Jarvis & Tellam, *supra* n.10, at 61; Hricik *supra* n.10, at 502-06.

23 In re Grand Jury Proceedings, 43 F.3d 966, 968 (5th Cir. 1994) (court considered e-mail messages along with other documents in work-product privilege analysis); United States v. Keystone Sanitation Co. Inc., 903 F. Supp. 803, 808 (M.D. Pa. 1995) (defendants waived privileged nature of e-mail messages due to inadvertent production).

24 Hricik *supra* n. 10, at 487.

25 See e.g., Alaska Bar Ass'n Op. 98-2 (1998); Ill. State Bar Ass'n Advisory Op. on Professional Conduct No. 96-10 (1997); S.C. Bar Ethics Advisory Comm. Op. No. 97-08 (1997); Vermont Advisory Ethics Op. 97-5 (1997). See also, Hricik *supra* n.10, at 486-87.

26 Examples include America Online ("AOL"), CompuServe, and MCI Mail.

27 Hricik *supra* n.10, at 487-88.

28 If the inadvertent recipient is a lawyer, then the lawyer must refrain from examining the information any more than necessary to ascertain that it was not intended for her and must notify the sender, ABA Comm. on Ethics and Professional Responsibility, Formal Op. 92-368 (1992), an obligation that extends to information received by e-mail or fax, ABA Comm. on Ethics and Professional Responsibility, Formal Op. 94-382 (1994).

29 For a basic explanation of encryption technology, including the use of digital signatures, see Kenneth E. Russell, Dealing with Security, Encryption, and Ethics Concerns, in THE LAWYER'S QUICK GUIDE TO E-MAIL 93-105 (ABA Law Practice Management Section 1998) ("Russell").

30 For a discussion of some additional matters such formal policies might address (deletion and retention of e-mail messages, remote checking of messages while out of office, etc.), see Russell, *supra* n. 29, at 104-05.

31 For example, the terms of AOL's policy forbid access to e-mail except (1) to comply with the law, (2) to protect its own rights, or (3) to act in the belief that someone's safety is at risk. Hricik *supra* n. 10, at 489.

32 18 U.S.C.A. (2511(2) (a) (i) (It is "not unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks").

The qualified right of interception of OSPs cannot be argued to create unique risks to the confidentiality of e-mail communications because phone companies (and other providers of wire or electronic communication services) are given identical rights under 18 U.S.C.A. (2511(2) (a) (i)). Moreover, many commercial mail services reserve the right to inspect all packages and letters handled, yet no one suggests this diminishes the user's expectation of privacy. See Hricik *supra* n.10, at 492. It also is noteworthy that in 1998, the New York Legislature amended the state's rules of evidence to provide that no otherwise privileged communication "shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication." N.Y. Civ. Prac. L. & R. § 4547 (1998).

33 18 U.S.C.A. (2511(3) (a)).

34 See e.g., *supra* n.18. See also Alaska Bar Ass'n Op. 98-2 (1998); D.C. Bar Op. 281 (1998); Ill. State Bar Ass'n Advisory Op. on Professional Conduct No. 96-10 (1997) (users of e-mail maintained by OSP have reasonable expectation of privacy despite greater risks than private network e-mail); S.C. Bar Ethics Advisory Comm. Op. No. 97-08 (1997); Vermont Advisory Ethics Op. 97-5 (1997); Jarvis & Tellam *supra* n.10, at 61; Hricik *supra* n.10, at 492.

35 Confidentiality also may be compromised by computer viruses, some of which have the capability of causing the user's document to be propagated to unintended recipients. However, a virus scanning program containing up-to-date definition files will detect and clean such viruses. See generally Carnegie Mellon Software Engineering Institute's CERT(r) Coordination Center Website, <http://www.cert.org/index.html>, for descriptions of these and other computer viruses.

36 See *supra* notes 30 & 31 and accompanying text.

37 18 U.S.C.A. (2511(2) (a) (i)).

38 See 18 U.S.C.A. ((2511, 2701, 2702.

39 See *Katz v. U.S.*, 389 U.S. 347, 352 (1967) (Fourth Amendment protection extended to conversation overheard by listening device attached to outside of public telephone booth).

40 See, e.g., Alaska Bar Ass'n Op. 98-2 (1998) (lawyers may communicate with clients via unencrypted e-mail; client consent is unnecessary because the expectation of privacy in e-mail is no less reasonable than that in the telephone or fax); D.C. Bar Op. 281 (1998) (lawyers' use of unencrypted e-mail is not a violation of duty to protect client confidences under District of Columbia Rule of Professional Conduct 1.6); Ky. Bar Ass'n Ethics Comm. Advisory Op. E-403 (1998) (absent "unusual circumstances" lawyers may use e-mail, including unencrypted Internet e-mail, to communicate with clients); New York State Bar Ass'n Comm. on Professional Ethics Op. 709 (1998) (lawyers may use unencrypted Internet e-mail to transmit confidential information without breaching the duty of confidentiality under state analogue to ABA Model Rule 1.6); Ill. State Bar Ass'n Advisory Op. on Professional Conduct No. 96-10 (1997) (lawyers may use unencrypted e-mail, including e-mail sent over the Internet, to communicate with clients without violating Rule 1.6 of the Illinois Rules of Professional Conduct; client consent is not required absent "extraordinarily sensitive" matter; expectation of privacy in e-mail is no less reasonable than that in ordinary telephone calls); N.D. St. B. Ass'n Ethics Comm. Op. 97-09 (1997) (attorneys may communicate with clients using unencrypted e-mail unless unusual circumstances warrant heightened security measures); S.C. Bar Ethics Advisory Comm. Op. No. 97-08 (1997) (finding reasonable expectation of privacy when sending confidential information by e-mail, including that sent through a private network, commercial service, and the Internet; use of e-mail to communicate client confidences

does not violate South Carolina Rule of Professional Conduct 1.6); Vermont Advisory Ethics Op. 97-5 (1997) (lawyers may use unencrypted Internet e-mail to transmit confidential information without breaching the duty of confidentiality under state analogue to ABA Model Rule 1.6). Two opinions similarly endorsed e-mail as a means of communicating client confidences, but advised lawyers to seek client consent or consider the use of encryption prior to its use, unlike the present opinion: Pa. Bar Ass'n Comm. on Legal Ethics Op. 97-130 (1997) (lawyers should not use unencrypted e-mail to communicate with or about a client absent client consent); State Bar of Arizona Advisory Op. 97-04 (1996) (lawyers should caution client or consider the use of encryption before transmitting sensitive information by e-mail). Two other opinions advised lawyers to avoid the use of e-mail to communicate with or about clients: Iowa Bar Ass'n Op. 1997-1 (1997) (sensitive material should not be transmitted by e-mail - whether through the Internet, a non-secure intranet, or other types of proprietary networks - without client consent, encryption, or equivalent security system); N.C. State Bar Opinion 215 (1995) (advising lawyers to use the mode of communication that will best maintain confidential information, and cautioning attorneys against the use of e-mail). Commentary supportive of the conclusions reached in this opinion, in addition to Hricik *supra* n.10 and Jarvis & Tellam *supra* n.10, include William Freivogel, *Communicating With or About Clients on the Internet: Legal, Ethical, and Liability Concerns*, ALAS LOSS PREVENTION JOURNAL 17 (1996) (concluding that it is not ethically or legally necessary to encrypt Internet e-mail but cautioning them in light of the absence of controlling legal authority). For a list of Web pages containing articles on e-mail and confidentiality, see Russell, *supra* n. 29, at 103.

© 1999 by the American Bar Association. All rights reserved

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 11-459

August 4, 2011

Duty to Protect the Confidentiality of E-mail Communications with One's Client

A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access. In the context of representing an employee, this obligation arises, at the very least, when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means, using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party.¹

Introduction

Lawyers and clients often communicate with each other via e-mail and sometimes communicate via other electronic means such as text messaging. The confidentiality of these communications may be jeopardized in certain circumstances. For example, when the client uses an employer's computer, smartphone or other telecommunications device, or an employer's e-mail account to send or receive e-mails with counsel, the employer may obtain access to the e-mails. Employers often have policies reserving a right of access to employees' e-mail correspondence via the employer's e-mail account, computers or other devices, such as smartphones and tablet devices, from which their employees correspond. Pursuant to internal policy, the employer may be able to obtain an employee's communications from the employer's e-mail server if the employee uses a business e-mail address, or from a workplace computer or other employer-owned telecommunications device on which the e-mail is stored even if the employee has used a separate, personal e-mail account. Employers may take advantage of that opportunity in various contexts, such as when the client is engaged in an employment dispute or when the employer is monitoring employee e-mails as part of its compliance responsibilities or conducting an internal investigation relating to the client's work.² Moreover, other third parties may be able to obtain access to an employee's electronic communications by issuing a subpoena to the employer. Unlike conversations and written communications, e-mail communications may be permanently available once they are created.

The confidentiality of electronic communications between a lawyer and client may be jeopardized in other settings as well. Third parties may have access to attorney-client e-mails when the client receives or sends e-mails via a public computer, such as a library or hotel computer, or via a borrowed computer. Third parties also may be able to access confidential communications when the client uses a computer or other device available to others, such as when a client in a matrimonial dispute uses a home computer to which other family members have access.

In contexts such as these, clients may be unaware of the possibility that a third party may gain access to their personal correspondence and may fail to take necessary precautions. Therefore, the risk that third parties may obtain access to a lawyer's e-mail communications with a client raises the question of what, if any, steps a lawyer must take to prevent such access by third parties from occurring. This opinion addresses this question in the following hypothetical situation.

An employee has a computer assigned for her exclusive use in the course of her employment. The company's written internal policy provides that the company has a right of access to all employees' computers and e-mail files, including those relating to employees' personal matters. Notwithstanding this

¹ This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2011. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

² Companies conducting internal investigations often secure and examine the e-mail communications and computer files of employees who are thought to have relevant information.

policy, employees sometimes make personal use of their computers, including for the purpose of sending personal e-mail messages from their personal or office e-mail accounts. Recently, the employee retained a lawyer to give advice about a potential claim against her employer. When the lawyer knows or reasonably should know that the employee may use a workplace device or system to communicate with the lawyer, does the lawyer have an ethical duty to warn the employee about the risks this practice entails?

Discussion

Absent an applicable exception, Rule 1.6(a) requires a lawyer to refrain from revealing “information relating to the representation of a client unless the client gives informed consent.” Further, a lawyer must act competently to protect the confidentiality of clients’ information. This duty, which is implicit in the obligation of Rule 1.1 to “provide competent representation to a client,” is recognized in two Comments to Rule 1.6. Comment [16] observes that a lawyer must “act competently to safeguard information relating to the representation of a client 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.” Comment [17] states in part: “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.... 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.”

This Committee has recognized that these provisions of the Model Rules require lawyers to take reasonable care to protect the confidentiality of client information,³ including information contained in e-mail communications made in the course of a representation. In ABA Op. 99-413 (1999) (“Protecting the Confidentiality of Unencrypted E-Mail”), the Committee concluded that, in general, a lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating Model Rule 1.6(a) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint. The opinion, nevertheless, cautioned lawyers to consult with their clients and follow their clients’ instructions as to the mode of transmitting highly sensitive information relating to the clients’ representation. It found that particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters.

Clients may not be afforded a “reasonable expectation of privacy” when they use an employer’s computer to send e-mails to their lawyers or receive e-mails from their lawyers. Judicial decisions illustrate the risk that the employer will read these e-mail communications and seek to use them to the employee’s disadvantage. Under varying facts, courts have reached different conclusions about whether an employee’s client-lawyer communications located on a workplace computer or system are privileged, and the law appears to be evolving.⁴ This Committee’s mission does not extend to interpreting the substantive law, and

³ See, e.g., ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 08-451 (2008) (Lawyer’s Obligations When Outsourcing Legal and Nonlegal Support Services) (“the obligation to ‘act competently to safeguard information relating to the representation of a client 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’” requires a lawyer outsourcing legal work “to recognize and minimize the risk that any outside service provider may inadvertently -- or perhaps even advertently -- reveal client confidential information to adverse parties or to others who are not entitled to access ... [and to] verify that the outside service provider does not also do work for adversaries of their clients on the same or substantially related matters.”).

⁴ See, e.g., *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650, 663 (N.J. 2010) (privilege applied to e-mails with counsel using “a personal, password protected e-mail account” that were accessed on a company computer); *Sims v. Lakeside Sch.*, No. C06-1412RSM, 2007 WL 2745367, at *2 (W.D. Wash. Sept. 20, 2007) (privilege applied to web-based e-mails to and from employee’s counsel on hard drive of computer furnished by employer); *National Econ. Research Assocs. v. Evans*, No. 04-2618-BLS2, 21 Mass.L.Rptr. 337, 2006 WL 2440008, at *5 (Mass. Super. Aug. 3, 2006) (privilege applied to “attorney-client communications unintentionally stored in a temporary file on a company-owned computer that were made via a private, password-protected e-mail account accessed through the Internet, not the company’s Intranet”); *Holmes v. Petrovich Development Co.*, 191 Cal.App.4th 1047, 1068-72 (2011) (privilege

therefore we express no view on whether, and in what circumstances, an employee's communications with counsel from the employee's workplace device or system are protected by the attorney-client privilege. Nevertheless, we consider the ethical implications posed by the risks that these communications will be reviewed by others and held admissible in legal proceedings.⁵ Given these risks, a lawyer should ordinarily advise the employee-client about the importance of communicating with the lawyer in a manner that protects the confidentiality of e-mail communications, just as a lawyer should avoid speaking face-to-face with a client about sensitive matters if the conversation might be overheard and should warn the client against discussing their communications with others. In particular, as soon as practical after a client-lawyer relationship is established, a lawyer typically should instruct the employee-client to avoid using a workplace device or system for sensitive or substantive communications, and perhaps for any attorney-client communications, because even seemingly ministerial communications involving matters such as scheduling can have substantive ramifications.

The time at which a lawyer has an ethical obligation under Rules 1.1 and 1.6 to provide advice of this nature will depend on the circumstances. At the very least, in the context of representing an employee, this ethical obligation arises when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means,⁶ using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party. Considerations tending to establish an ethical duty to protect client-lawyer confidentiality by warning the client against using a business device or system for substantive e-mail communications with counsel include, but are not limited to, the following: (1) that the client has engaged in, or has indicated an intent to engage in, e-mail communications with counsel; (2) that the client is employed in a position that would provide access to a workplace device or system; (3) that, given the circumstances, the employer or a third party has the ability to access the e-mail communications; and (4) that, as far as the lawyer knows, the employer's internal policy and the jurisdiction's laws do not clearly protect the privacy of the employee's personal e-mail communications via a business device or system. Unless a lawyer has reason to believe otherwise, a lawyer ordinarily should assume that an employer's internal policy allows for access to the employee's e-mails sent to or from a workplace device or system.

The situation in the above hypothetical is a clear example of where failing to warn the client about the risks of e-mailing communications on the employer's device can harm the client, because the employment dispute would give the employer a significant incentive to access the employee's workplace e-mail and the employer's internal policy would provide a justification for doing so. The obligation arises once the lawyer has reason to believe that there is a significant risk that the client will conduct e-mail communications with the lawyer using a workplace computer or other business device or via the employer's e-mail account. This possibility ordinarily would be known, or reasonably should be known, at the outset of the representation. Given the nature of the representation—an employment dispute—the lawyer is on notice that the employer may search the client's electronic correspondence. Therefore, the lawyer must ascertain, unless the answer is already obvious, whether there is a significant risk that the client will use a business e-mail address for personal communications or whether the employee's position entails using an employer's device. Protective measures would include the lawyer refraining from sending e-mails

inapplicable to communications with counsel using workplace computer); *Scott v. Beth Israel Medical Center, Inc.*, 847 N.Y.S.2d 436, 440-43 (N.Y. Sup. Ct. 2007) (privilege inapplicable to employer's communications with counsel via employer's e-mail system); *Long v. Marubeni Am. Corp.*, No. 05CIV.639(GEL)(KNF), 2006 WL 2998671, at *3-4 (S.D.N.Y. Oct. 19, 2006) (e-mails created or stored in company computers were not privileged, notwithstanding use of private password-protected e-mail accounts); *Kaufman v. SunGard Inv. Sys.*, No. 05-CV-1236 (JLL), 2006 WL 1307882, at *4 (D.N.J. May 10, 2006) (privilege inapplicable to communications with counsel using employer's network).

⁵ For a discussion of a lawyer's duty when receiving a third party's e-mail communications with counsel, see ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-460 (2011) (Duty when Lawyer Receives Copies of a Third Party's E-mail Communications with Counsel).

⁶ This opinion principally addresses e-mail communications, which are the most common way in which lawyers communicate electronically with clients, but it is equally applicable to other means of electronic communications.

to the client's workplace, as distinct from personal, e-mail address,⁷ and cautioning the client against using a business e-mail account or using a personal e-mail account on a workplace computer or device at least for substantive e-mails with counsel.

As noted at the outset, the employment scenario is not the only one in which attorney-client electronic communications may be accessed by third parties. A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, to which a third party may gain access. The risk may vary. Whenever a lawyer communicates with a client by e-mail, the lawyer must first consider whether, given the client's situation, there is a significant risk that third parties will have access to the communications. If so, the lawyer must take reasonable care to protect the confidentiality of the communications by giving appropriately tailored advice to the client.

⁷ Of course, if the lawyer becomes aware that a client is receiving personal e-mail on a workplace computer or other device owned or controlled by the employer, then a duty arises to caution the client not to do so, and if that caution is not heeded, to cease sending messages even to personal e-mail addresses.

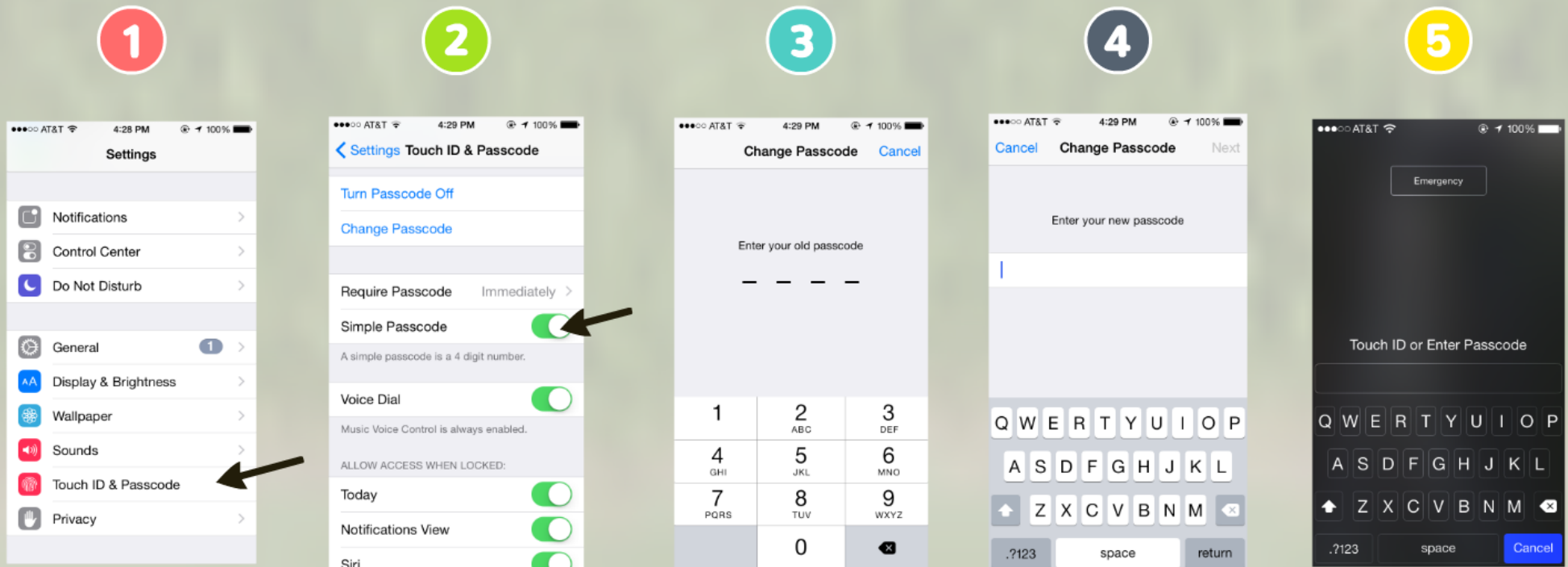
AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY
321 N. Clark Street, Chicago, Illinois 60654-4714 Telephone (312) 988-5310

CHAIR: Robert Mundheim, New York, NY ■ Nathaniel Cade, Jr., Milwaukee, WI ■ Lisa E. Chang, Atlanta, GA ■ James H. Cheek, III, Nashville, TN ■ Robert A. Creamer, Evanston, IL ■ Paula J. Frederick, Atlanta, GA ■ Bruce A. Green, New York, NY ■ James M. McCauley, Richmond, VA ■ Philip H. Schaeffer, New York, NY ■ E. Norman Veasey, Wilmington, DE

CENTER FOR PROFESSIONAL RESPONSIBILITY: George A. Kuhlman, Ethics Counsel; Eileen B. Libby, Associate Ethics Counsel

©2011 by the American Bar Association. All rights reserved.

Use a Complex Password on Portable Devices



1. In Settings, click "Touch ID & Passcode"
2. Click "Simple Passcode" to deselect
3. Enter current passcode
4. Enter complex passcode using letters, numbers, and symbols
5. New log-in passcode screen

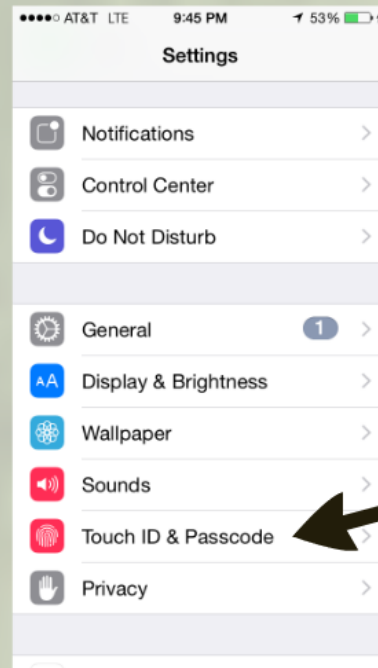
Device Security

- Set mobile device to wipe after certain number of incorrect entries

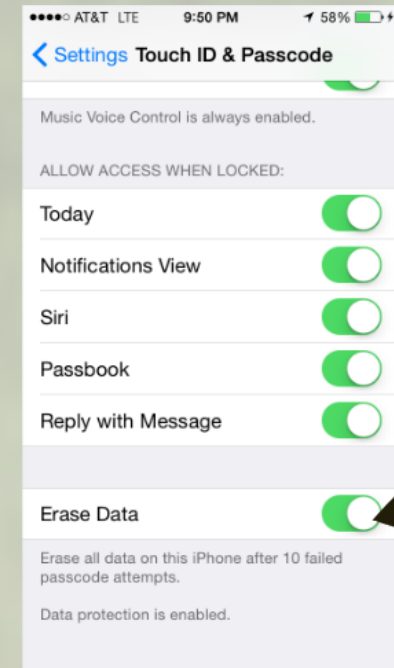
1



2



3



How Secure is My Password?

howsecureismypassword.net

https://howsecureismypassword.net

HOW SECURE IS MY PASSWORD?

This site could be stealing your password... it's not, but it easily *could* be.
Be careful where you type your password.

[Follow @hsimpnet](#) [Like](#) 9.6k

Top 10,000 Passwords by [Xato](#)
Typefaces by [The League of Movable Type](#) & [Łukasz Dziedzic](#)

Version 4.0
Sponsored by [RoboForm Password Manager](#)

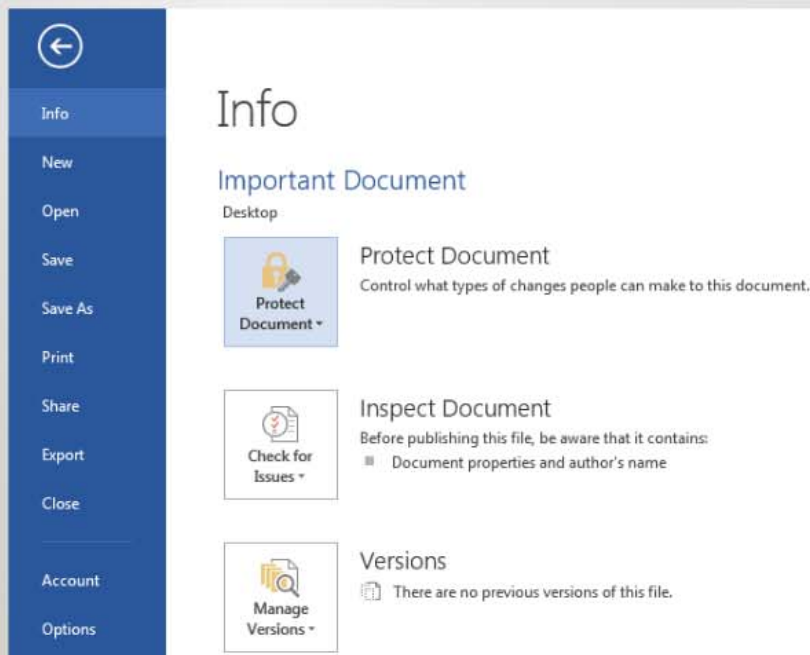
© Small Hadron Collider, 2009-2014

This site is for educational use. Due to limitations of the technology involved, its results *cannot* always be accurate.
Your password will not be transferred over the internet.

Password Protection on Microsoft Word

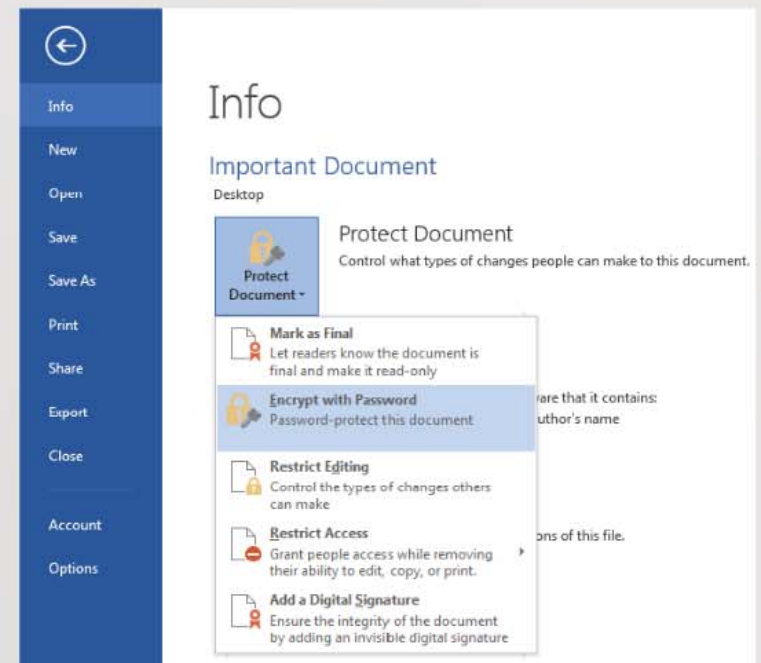
1

Click "File" then "Protect Document"



2

Click "Encrypt* with Password"

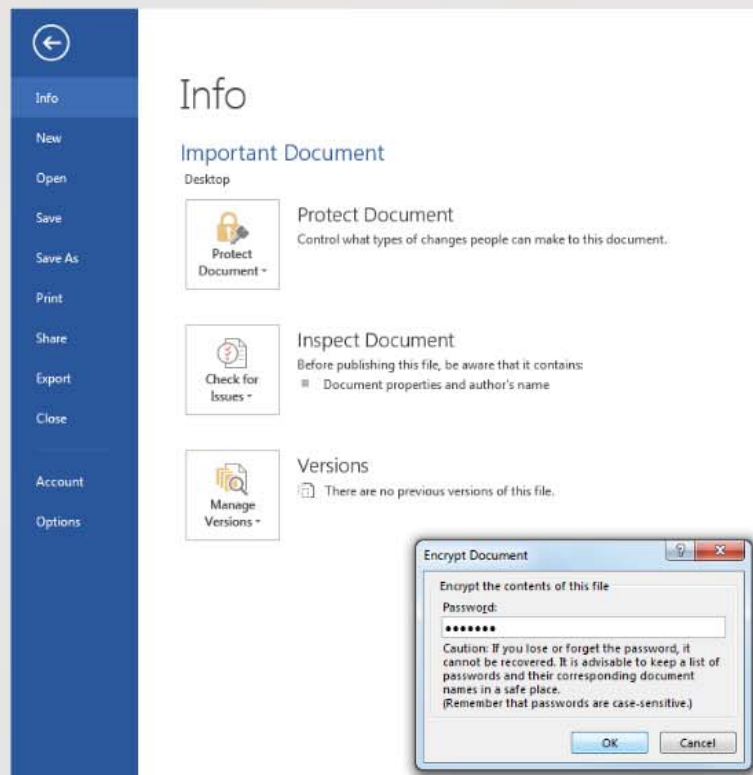


**Note that password protecting the document is not actually "encrypting" the data contained in the document*

Password Protection on Microsoft Word

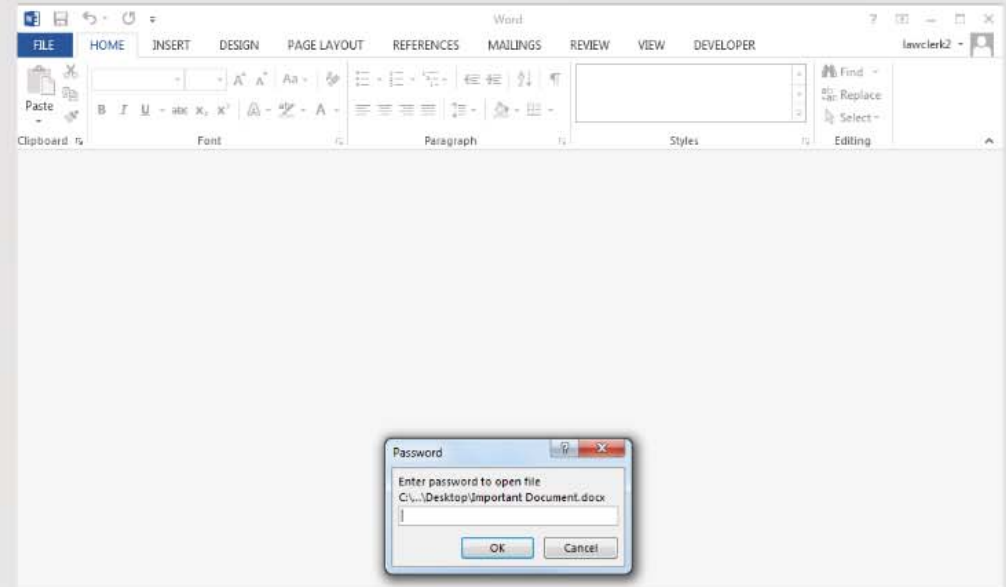
3

Enter a password



4

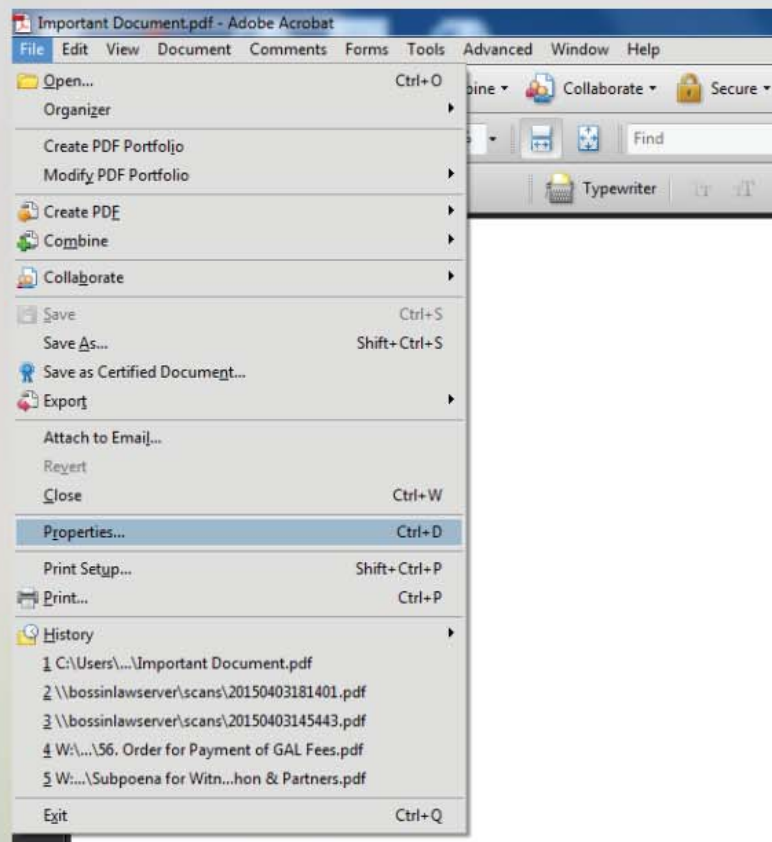
The recipient must enter the password to open the document



Password Protection in Adobe PDF

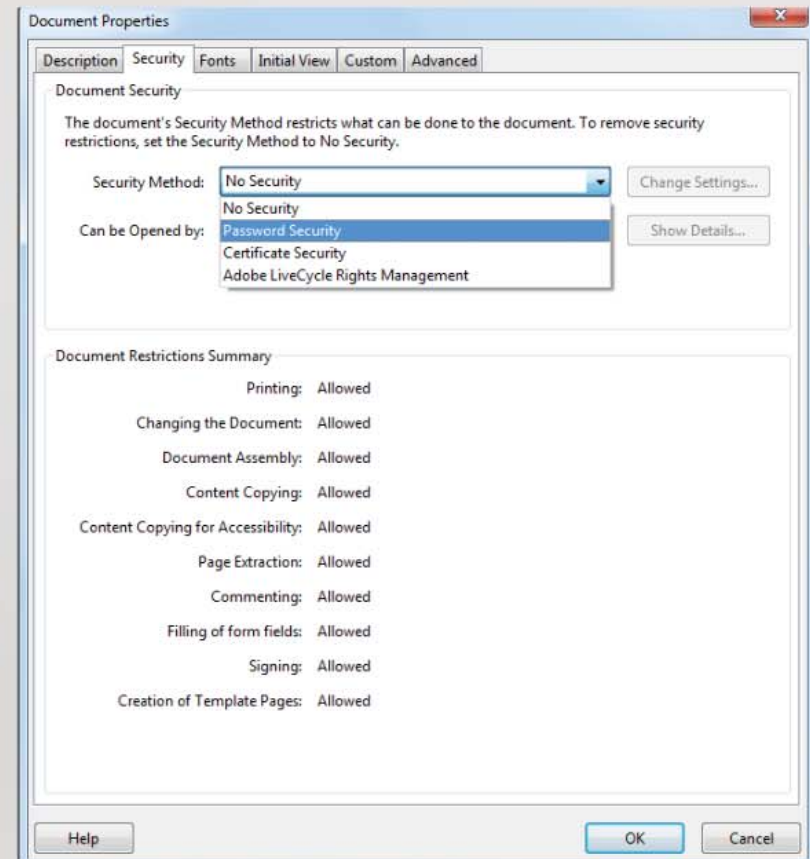
1

Click "File" and select "Properties"



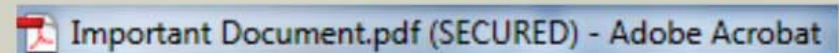
2

On the "Security" tab, select "Password Security"

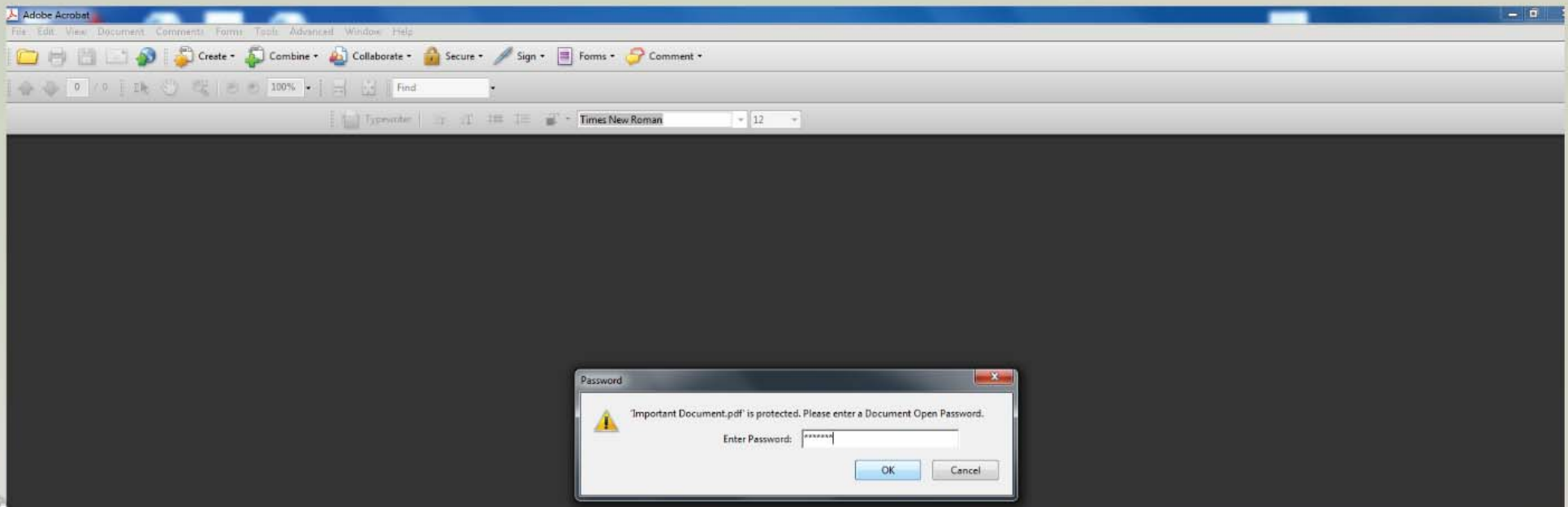


Password Protection in Adobe PDF

- 3 PDF file name will now include "(SECURED)"



- 4 The recipient must enter the password to open the PDF



► The Supreme Court of Texas appoints the chair and the nine members of the Professional Ethics Committee from the bar and the judiciary. According to Section 81.092(c) of the Texas Government Code, “Committee opinions are not binding on the Supreme Court.”

Opinion No. 648, April 2015

QUESTION PRESENTED

Under the Texas Disciplinary Rules of Professional Conduct, may a lawyer communicate confidential information by email?

Statement of Facts

Lawyers in a Texas law firm represent clients in family law, employment law, personal injury, and criminal law matters. When they started practicing law, the lawyers typically delivered written communication by facsimile or the U.S. Postal Service. Now, most of their written communication is delivered by web-based email, such as unencrypted Gmail.

Having read reports about email accounts being hacked and the National Security Agency obtaining email communications without a search warrant, the lawyers are concerned about whether it is proper for them to continue using email to communicate confidential information.

Discussion

The Texas Disciplinary Rules of Professional Conduct do not specifically address the use of email in the practice of law, but they do provide for the protection of confidential information, defined broadly by Rule 1.05(a) to include both privileged and unprivileged client information, which might be transmitted by email.

Rule 1.05(b) provides that, except as permitted by paragraphs (c) and (d) of the Rule:

“a lawyer shall not knowingly:

- (1) Reveal confidential information of a client or former client to:
 - (i) a person that the client has instructed is not to receive the information; or
 - (ii) anyone else, other than the

client, the client’s representatives, or the members, associates, or employees of the lawyer’s law firm.”

A lawyer violates Rule 1.05 if the lawyer knowingly reveals confidential information to any person other than those persons who are permitted or required to receive the information under paragraphs (b), (c), (d), (e), or (f) of the Rule.

The Terminology section of the Rules states that “[k]nowingly” . . . denotes actual knowledge of the fact in question” and that a “person’s knowledge may be inferred from circumstances.” A determination of whether a lawyer violates the Disciplinary Rules, as opposed to fiduciary obligations, the law, or best practices, by sending an email containing confidential information, requires a case-by-case evaluation of whether that lawyer knowingly revealed confidential information to a person who was not permitted to receive that information under Rule 1.05.

The concern about sending confidential information by email is the risk that an unauthorized person will gain access to the confidential information. While this Committee has not addressed the propriety of communicating confidential information by email, many other ethics committees have, concluding that, in general, and except in special circumstances, the use of email, including unencrypted email, is a proper method of communicating confidential information. See, e.g., ABA

Comm. on Ethics and Prof’l Responsibility, Formal Op. 99-413 (1999); ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 11-459 (2011); State Bar of Cal. Standing Comm. on Prof’l Responsibility and Conduct, Formal Op. 2010-179 (2010); Prof’l Ethics Comm. of the Maine Bd. of Overseers of the Bar, Op. No. 195 (2008); N.Y. State Bar Ass’n Comm. on Prof’l Ethics, Op. 820 (2008); Alaska Bar Ass’n Ethics Comm., Op. 98-2 (1998); D.C. Bar Legal Ethics Comm., Op. 281 (1998); Ill. State Bar Ass’n Advisory Opinion on Prof’l Conduct, Op. 96-10 (1997); State Bar Ass’n of N.D. Ethics Comm., Op. No. 97-09 (1997); S.C. Bar Ethics Advisory Comm., Ethics Advisory Op. 97-08 (1997); Vt. Bar Ass’n, Advisory Ethics Op. No 97-05 (1997).

Those ethics opinions often make two points in support of the conclusion that email communication is proper. First, the risk an unauthorized person will gain access to confidential information is inherent in the delivery of any written communication including delivery by the U.S. Postal Service, a private mail service, a courier, or facsimile. Second, persons who use email have a reasonable expectation of privacy based, in part, upon statutes that make it a crime to intercept emails. See, e.g., Alaska Bar Ass’n Ethics Comm. Op. 98-2 (1998); D.C. Bar Legal Ethics Comm., Op. 281 (1998). The statute cited in those opinions is the Electronic Communication Privacy Act (ECPA), which makes it a crime to

intercept electronic communication, to use the contents of the intercepted email, or to disclose the contents of intercepted email. 18 U.S.C. § 2510 *et seq.* Importantly, the statute provides that “[n]o otherwise privileged . . . electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.” 18 U.S.C. § 2517(4).

The ethics opinions from other jurisdictions are instructive, as is Texas Professional Ethics Committee Opinion 572 (June 2006). The issue in Opinion 572 was whether a lawyer may, without the client’s express consent, deliver the client’s privileged information to a copy service hired by the lawyer to perform services in connection with the client’s representation. Opinion 572 concluded that a lawyer may disclose privileged information to an independent contractor if the lawyer reasonably expects that the independent contractor will not disclose or use such items or their contents except as directed by the lawyer and will otherwise respect the confidential character of the information.

In general, considering the present state of technology and email usage, a lawyer may communicate confidential information by email. In some circumstances, however, a lawyer should consider whether the confidentiality of the information will be protected if communicated by email and whether it is prudent to use encrypted email or another form of communication. Examples of such circumstances are:

1. communicating highly sensitive or confidential information via email or unencrypted email connections;
2. sending an email to or from an account that the email sender or recipient shares with others;
3. sending an email to a client

when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client’s work email account, especially if the email relates to a client’s employment dispute with his employer (see ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 11-459 (2011));

4. sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;
5. sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
6. sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer’s email communication, with or without a warrant.

In the event circumstances such as those identified above are present, to prevent the unauthorized or inadvertent disclosure of confidential information, it may be appropriate for a lawyer to advise and caution a client as to the dangers inherent in sending or accessing emails from computers accessible to persons other than the client. A lawyer should also consider whether circumstances are present that would make it advisable to obtain the client’s informed consent to the use of email communication, including the use of unencrypted email. See Texas Rule 1.03(b) and ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 11-459 (2011). Additionally, a lawyer’s eval-

uation of the lawyer’s email technology and practices should be ongoing as there may be changes in the risk of interception of email communication over time that would indicate that certain or perhaps all communications should be sent by other means.

Under Rule 1.05, the issue in each case is whether a lawyer who sent an email containing confidential information knowingly revealed confidential information to a person who was not authorized to receive the information. The answer to that question depends on the facts of each case. Since a “knowing” disclosure can be based on actual knowledge or can be inferred, each lawyer must decide whether he or she has a reasonable expectation that the confidential character of the information will be maintained if the lawyer transmits the information by email.

This opinion discusses a lawyer’s obligations under the Texas Disciplinary Rules of Professional Conduct, but it does not address other issues such as a lawyer’s fiduciary obligations or best practices with respect to email communications. Furthermore, it does not address a lawyer’s obligations under various statutes, such as the Health Insurance Portability and Accountability Act (HIPAA), which may impose other duties.

Conclusion

Under the Texas Disciplinary Rules of Professional Conduct, and considering the present state of technology and email usage, a lawyer may generally communicate confidential information by email. Some circumstances, may, however, cause a lawyer to have a duty to advise a client regarding risks incident to the sending or receiving of emails arising from those circumstances and to consider whether it is prudent to use encrypted email or another form of communication. **TBJ**

**THE STATE BAR OF CALIFORNIA
STANDING COMMITTEE ON
PROFESSIONAL RESPONSIBILITY AND CONDUCT
FORMAL OPINION NO. 2010-179**

ISSUE: Does an attorney violate the duties of confidentiality and competence he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties?

DIGEST: Whether an attorney violates his or her duties of confidentiality and competence when using technology to transmit or store confidential client information will depend on the particular technology being used and the circumstances surrounding such use. Before using a particular technology in the course of representing a client, an attorney must take appropriate steps to evaluate: 1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; 3) the degree of sensitivity of the information; 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; 5) the urgency of the situation; and 6) the client's instructions and circumstances, such as access by others to the client's devices and communications.

AUTHORITIES

INTERPRETED: Rules 3-100 and 3-110 of the California Rules of Professional Conduct.

Business and Professions Code section 6068, subdivision (e)(1).

Evidence Code sections 917(a) and 952.

STATEMENT OF FACTS

Attorney is an associate at a law firm that provides a laptop computer for his use on client and firm matters and which includes software necessary to his practice. As the firm informed Attorney when it hired him, the computer is subject to the law firm's access as a matter of course for routine maintenance and also for monitoring to ensure that the computer and software are not used in violation of the law firm's computer and Internet-use policy. Unauthorized access by employees or unauthorized use of the data obtained during the course of such maintenance or monitoring is expressly prohibited. Attorney's supervisor is also permitted access to Attorney's computer to review the substance of his work and related communications.

Client has asked for Attorney's advice on a matter. Attorney takes his laptop computer to the local coffee shop and accesses a public wireless Internet connection to conduct legal research on the matter and email Client. He also takes the laptop computer home to conduct the research and email Client from his personal wireless system.

DISCUSSION

Due to the ever-evolving nature of technology and its integration in virtually every aspect of our daily lives, attorneys are faced with an ongoing responsibility of evaluating the level of security of technology that has increasingly become an indispensable tool in the practice of law. The Committee's own research – including conferring with computer security experts – causes it to understand that, without appropriate safeguards (such as firewalls, secure username/password combinations, and encryption), data transmitted wirelessly can be intercepted and read with increasing ease. Unfortunately, guidance to attorneys in this area has not kept pace with technology. Rather than engage in a technology-by-technology analysis, which would likely become obsolete shortly, this

opinion sets forth the general analysis that an attorney should undertake when considering use of a particular form of technology.

1. The Duty of Confidentiality

In California, attorneys have an express duty “[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client.”^{1/} (Bus. & Prof. Code, § 6068, subd. (e)(1).) This duty arises from the relationship of trust between an attorney and a client and, absent the informed consent of the client to reveal such information, the duty of confidentiality has very few exceptions. (Rules Prof. Conduct, rule 3-100 & discussion “[A] member may not reveal such information except with the consent of the client or as authorized or required by the State Bar Act, these rules, or other law.”.)^{2/}

Unlike Rule 1.6 of the Model Rules of Professional Conduct (“MRPC”), the exceptions to the duty of confidentiality under rule 3-100 do not expressly include disclosure “impliedly authorized in order to carry out the representation.” (MRPC, Rule 1.6.) Nevertheless, the absence of such language in the California Rules of Professional Conduct does not prohibit an attorney from using postal or courier services, telephone lines, or other modes of communication beyond face-to-face meetings, in order to effectively carry out the representation. There is a distinction between actually disclosing confidential information to a third party for purposes ancillary to the representation,^{3/} on the one hand, and using appropriately secure technology provided by a third party as a method of communicating with the client or researching a client’s matter,^{4/} on the other hand.

Section 952 of the California Evidence Code, defining “confidential communication between client and lawyer” for purposes of application of the attorney-client privilege, includes disclosure of information to third persons “to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted.” (Evid. Code, § 952.) While the duty to protect confidential client information is broader in scope than the attorney-client privilege (Discussion [2] to rule 3-100; *Goldstein v. Lees* (1975) 46 Cal.App.3d 614, 621, fn. 5 [120 Cal.Rptr. 253]), the underlying principle remains the same, namely, that transmission of information through a third party reasonably necessary for purposes of the representation should not be deemed to have destroyed the confidentiality of the information. (See Cal. State Bar Formal Opn. No. 2003-161 [repeating the Committee’s prior observation “that the duty of confidentiality and the evidentiary privilege share the same basic policy foundation: to encourage clients to disclose all possibly pertinent information to their attorneys so that the attorneys may effectively represent the clients’ interests.”].) Pertinent here, the manner in which an attorney acts to safeguard confidential client information is governed by the duty of competence, and determining whether a third party has the ability to access and use confidential client information in a manner that is unauthorized by the client is a subject that must be considered in conjunction with that duty.

2. The Duty of Competence

Rule 3-110(A) prohibits the intentional, reckless or repeated failure to perform legal services with competence. Pertinent here, “competence” may apply to an attorney’s diligence and learning with respect to handling matters for clients. (Rules Prof. Conduct, rule 3-110(B).) The duty of competence also applies to an attorney’s “duty to supervise the work of subordinate attorney and non-attorney employees or agents.” (Discussion to rule 3-110.)

^{1/} “Secrets” include “[a]ny ‘information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would likely be detrimental to the client.’” (Cal. State Bar Formal Opn. No. 1981-58.)

^{2/} Unless otherwise indicated, all future references to rules in this opinion will be to the Rules of Professional Conduct of the State Bar of California.

^{3/} In this regard, compare Cal. State Bar Formal Opn. No. 1971-25 (use of an outside data processing center without the client’s consent for bookkeeping, billing, accounting and statistical purposes, if such information includes client secrets and confidences, would violate section 6068, subdivision (e)), with Los Angeles County Bar Assn. Formal Opn. No. 374 (1978) (concluding that in most circumstances, if protective conditions are observed, disclosure of client’s secrets and confidences to a central data processor would not violate section 6068(e) and would be the same as disclosures to non-lawyer office employees).

^{4/} Cf. Evid. Code, § 917(b) (“A communication ... does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication.”).

With respect to acting competently to preserve confidential client information, the comments to Rule 1.6 of the MRPC^{5/} provide:

[16] A lawyer must act competently to safeguard information relating to the representation of a client 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.

[17] 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.

(MRPC, cmts. 16 & 17 to Rule 1.6.) In this regard, the duty of competence includes taking appropriate steps to ensure both that secrets and privileged information of a client remain confidential and that the attorney's handling of such information does not result in a waiver of any privileges or protections.

3. Factors to Consider

In accordance with the duties of confidentiality and competence, an attorney should consider the following before using a specific technology:^{6/}

- a) The attorney's ability to assess the level of security afforded by the technology, including without limitation:
 - i) Consideration of how the particular technology differs from other media use. For example, while one court has stated that, "[u]nlike postal mail, simple e-mail generally is not 'sealed' or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted)" (*American Civil Liberties Union v. Reno* (E.D.Pa. 1996) 929 F.Supp. 824, 834, aff'd (1997) 521 U.S. 844 [117 S.Ct. 2329]), most bar associations have taken the position that the risks of a third party's unauthorized review of email (whether by interception or delivery to an unintended recipient) are similar to the risks that confidential client information transmitted by standard mail service will be opened by any of the many hands it passes through on the way to its recipient or will be misdirected^{7/} (see, e.g., ABA Formal Opn. No. 99-413^{8/} [concluding that attorneys have a reasonable expectation of privacy in email communications, even if unencrypted, "despite some risk of interception and disclosure"]; Los Angeles County Bar Assn. Formal Opn. No. 514 (2005) ["Lawyers are not required

^{5/} In the absence of on-point California authority and conflicting state public policy, the MRPC may serve as guidelines. (*City & County of San Francisco v. Cobra Solutions, Inc.* (2006) 38 Cal. 4th 839, 852 [43 Cal.Rptr.3d 771].)

^{6/} These factors should be considered regardless of whether the attorney practices in a law firm, a governmental agency, a non-profit organization, a company, as a sole practitioner or otherwise.

^{7/} Rule 1-100(A) provides that "[e]thics opinions and rules and standards promulgated by other jurisdictions and bar associations may . . . be considered" for professional conduct guidance.

^{8/} In 1999, the ABA Committee on Ethics and Professional Responsibility reviewed state bar ethics opinions across the country and determined that, as attorneys' understanding of technology has improved, the opinions generally have transitioned from concluding that use of Internet email violates confidentiality obligations to concluding that use of unencrypted Internet email is permitted without express client consent. (ABA Formal Opn. No. 99-413 [detailing various positions taken in state ethics opinions from Alaska, Washington D.C., Kentucky, New York, Illinois, North Dakota, South Carolina, Vermont, Pennsylvania, Arizona, Iowa and North Carolina].)

to encrypt e-mail containing confidential client communications because e-mail poses no greater risk of interception and disclosure than regular mail, phones or faxes.”]; Orange County Bar Assn. Formal Opn. No. 97-0002 [concluding use of encrypted email is encouraged, but not required].) (See also *City of Reno v. Reno Police Protective Assn.* (2003) 118 Nev. 889, 897-898 [59 P.3d 1212] [referencing an earlier version of section 952 of the California Evidence Code and concluding “that a document transmitted by e-mail is protected by the attorney-client privilege as long as the requirements of the privilege are met.”].)

- ii) Whether reasonable precautions may be taken when using the technology to increase the level of security.^{9/} As with the above-referenced views expressed on email, the fact that opinions differ on whether a particular technology is secure suggests that attorneys should take reasonable steps as a precautionary measure to protect against disclosure.^{10/} For example, depositing confidential client mail in a secure postal box or handing it directly to the postal carrier or courier is a reasonable step for an attorney to take to protect the confidentiality of such mail, as opposed to leaving the mail unattended in an open basket outside of the office door for pick up by the postal service. Similarly, encrypting email may be a reasonable step for an attorney to take in an effort to ensure the confidentiality of such communications remain so when the circumstance calls for it, particularly if the information at issue is highly sensitive and the use of encryption is not onerous. To place the risks in perspective, it should not be overlooked that the very nature of digital technologies makes it easier for a third party to intercept a much greater amount of confidential information in a much shorter period of time than would be required to transfer the same amount of data in hard copy format. In this regard, if an attorney can readily employ encryption when using public wireless connections and has enabled his or her personal firewall, the risks of unauthorized access may be significantly reduced.^{11/} Both of these tools are readily available and relatively inexpensive, and may already be built into the operating system. Likewise, activating password protection features on mobile devices, such as laptops and PDAs, presently helps protect against access to confidential client information by a third party if the device is lost, stolen or left unattended. (See David Ries & Reid Trautz, *Law Practice Today*, “Securing Your Clients’ Data While On the Road,” October 2008 [noting reports that “as many as 10% of laptops used by American businesses are stolen during their useful lives and 97% of them are never recovered”].)
- iii) Limitations on who is permitted to monitor the use of the technology, to what extent and on what grounds. For example, if a license to use certain software or a technology service imposes a requirement of third party access to information related to the attorney’s use of the technology, the attorney may need to confirm that the terms of the requirement or authorization do not permit the third party to disclose confidential client information to others or use such information for any purpose other than to ensure the functionality of the software or that the technology is not being used for an improper purpose, particularly if the information at issue is highly sensitive.^{12/} Under Rule 5.3 [of the MRPC], a lawyer retaining such an outside service provider is required to make reasonable efforts to ensure that

^{9/} Attorneys also should employ precautions to protect confidential information when in public, such as ensuring that the person sitting in the adjacent seat on an airplane cannot see the computer screen or moving to a private location before discussing confidential information on a mobile phone.

^{10/} Section 60(1)(b) of the Restatement (Third) of The Law Governing Lawyers provides that “a lawyer must take steps reasonable in the circumstances to protect confidential client information against impermissible use or disclosure by the lawyer’s associates or agents that may adversely affect a material interest of the client or otherwise than as instructed by the client.”

^{11/} Similarly, this Committee has stated that if an attorney is going to maintain client documents in electronic form, he or she must take reasonable steps to strip any metadata containing confidential information of other clients before turning such materials over to a current or former client or his or her new attorney. (See Cal. State Bar Formal Opn. 2007-174.)

^{12/} A similar approach might be appropriate if the attorney is employed by a non-profit or governmental organization where information may be monitored by a person or entity with interests potentially or actually in conflict with the attorney’s client. In such cases, the attorney should not use the technology for the representation, absent informed consent by the client or the ability to employ safeguards to prevent access to confidential client information. The attorney also may need to consider whether he or she can competently represent the client without the technology.

the service provider will not make unauthorized disclosures of client information. Thus when a lawyer considers entering into a relationship with such a service provider he must ensure that the service provider has in place, or will establish, reasonable procedures to protect the confidentiality of information to which it gains access, and moreover, that it fully understands its obligations in this regard. [Citation.] In connection with this inquiry, a lawyer might be well-advised to secure from the service provider in writing, along with or apart from any written contract for services that might exist, a written statement of the service provider's assurance of confidentiality.” (ABA Formal Opn. No. 95-398.)

Many attorneys, as with a large contingent of the general public, do not possess much, if any, technological savvy. Although the Committee does not believe that attorneys must develop a mastery of the security features and deficiencies of each technology available, the duties of confidentiality and competence that attorneys owe to their clients do require a basic understanding of the electronic protections afforded by the technology they use in their practice. If the attorney lacks the necessary competence to assess the security of the technology, he or she must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant.^{13/} (Cf. Rules Prof. Conduct, rule 3-110(C) [“If a member does not have sufficient learning and skill when the legal service is undertaken, the member may nonetheless perform such services competently by 1) associating with or, where appropriate, professionally consulting another lawyer reasonably believed to be competent, or 2) by acquiring sufficient learning and skill before performance is required.”].)

- b) Legal ramifications to third parties of intercepting, accessing or exceeding authorized use of another person's electronic information. The fact that a third party could be subject to criminal charges or civil claims for intercepting, accessing or engaging in unauthorized use of confidential client information favors an expectation of privacy with respect to a particular technology. (See, e.g., 18 U.S.C. § 2510 et seq. [Electronic Communications Privacy Act of 1986]; 18 U.S.C. § 1030 et seq. [Computer Fraud and Abuse Act]; Pen. Code, § 502(c) [making certain unauthorized access to computers, computer systems and computer data a criminal offense]; Cal. Pen. Code, § 629.86 [providing a civil cause of action to “[a]ny person whose wire, electronic pager, or electronic cellular telephone communication is intercepted, disclosed, or used in violation of [Chapter 1.4 on Interception of Wire, Electronic Digital Pager, or Electronic Cellular Telephone Communications].”]; *eBay, Inc. v. Bidder's Edge, Inc.* (N.D.Cal. 2000) 100 F.Supp.2d 1058, 1070 [in case involving use of web crawlers that exceeded plaintiff's consent, court stated “[c]onduct that does not amount to a substantial interference with possession, but which consists of intermeddling with or use of another's personal property, is sufficient to establish a cause of action for trespass to chattel.”].)^{14/}
- c) The degree of sensitivity of the information. The greater the sensitivity of the information, the less risk an attorney should take with technology. If the information is of a highly sensitive nature and there is a risk of disclosure when using a particular technology, the attorney should consider alternatives unless the client provides informed consent.^{15/} As noted above, if another person may have access to the communications transmitted between the attorney and the client (or others necessary to the representation), and may have an interest in the information being disclosed that is in conflict with the client's interest, the attorney should take precautions to ensure that the person will not be able to access the information or should avoid using the technology. These types of situations increase the likelihood for intrusion.

^{13/} Some potential security issues may be more apparent than others. For example, users of unsecured public wireless connections may receive a warning when accessing the connection. However, in most instances, users must take affirmative steps to determine whether the technology is secure.

^{14/} Attorneys also have corresponding legal and ethical obligations not to invade the confidential and privileged information of others.

^{15/} For the client's consent to be informed, the attorney should fully advise the client about the nature of the information to be transmitted with the technology, the purpose of the transmission and use of the information, the benefits and detriments that may result from transmission (both legal and nonlegal), and any other facts that may be important to the client's decision. (Los Angeles County Bar Assn. Formal Opn. No. 456 (1989).) It is particularly important for an attorney to discuss the risks and potential harmful consequences of using the technology when seeking informed consent.

- d) Possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product, including possible waiver of the privileges.^{16/} Section 917(a) of the California Evidence Code provides that “a communication made in confidence in the course of the lawyer-client, physician-patient, psychotherapist-patient, clergy-penitent, husband-wife, sexual assault counselor-victim, or domestic violence counselor-victim relationship ... is presumed to have been made in confidence and the opponent of the claim of privilege has the burden of proof to establish that the communication was not confidential.” (Evid. Code, § 917(a).) Significantly, subsection (b) of section 917 states that such a communication “does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication.” (Evid. Code, § 917(b). See also Penal Code, § 629.80 [“No otherwise privileged communication intercepted in accordance with, or in violation of, the provisions of [Chapter 1.4] shall lose its privileged character.”]; 18 U.S.C. § 2517(4) [“No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of [18 U.S.C. § 2510 et seq.] shall lose its privileged character.”].) While these provisions seem to provide a certain level of comfort in using technology for such communications, they are not a complete safeguard. For example, it is possible that, if a particular technology lacks essential security features, use of such a technology could be deemed to have waived these protections. Where the attorney-client privilege is at issue, failure to use sufficient precautions may be considered in determining waiver.^{17/} Further, the analysis differs with regard to an attorney’s duty of confidentiality. Harm from waiver of attorney-client privilege is possible depending on if and how the information is used, but harm from disclosure of confidential client information may be immediate as it does not necessarily depend on use or admissibility of the information, including as it does matters which would be embarrassing or would likely be detrimental to the client if disclosed.
- e) The urgency of the situation. If use of the technology is necessary to address an imminent situation or exigent circumstances and other alternatives are not reasonably available, it may be reasonable in limited cases for the attorney to do so without taking additional precautions.
- f) Client instructions and circumstances. If a client has instructed an attorney not to use certain technology due to confidentiality or other concerns or an attorney is aware that others have access to the client’s electronic devices or accounts and may intercept or be exposed to confidential client information, then such technology should not be used in the course of the representation.^{18/}

4. **Application to Fact Pattern**^{19/}

In applying these factors to Attorney’s situation, the Committee does not believe that Attorney would violate his duties of confidentiality or competence to Client by using the laptop computer because access is limited to authorized individuals to perform required tasks. However, Attorney should confirm that personnel have been appropriately instructed regarding client confidentiality and are supervised in accordance with rule 3-110. (See *Crane v. State Bar* (1981) 30 Cal.3d 117, 123 [177 Cal.Rptr. 670] [“An attorney is responsible for the work product of his employees which is performed pursuant to his direction and authority.”]; *In re Complex Asbestos Litig.* (1991) 232 Cal.App.3d 572, 588 [283 Cal.Rptr. 732] [discussing law firm’s ability to supervise employees and ensure they protect client confidences]; Cal. State Bar Formal Opn. No. 1979-50 [discussing lawyer’s duty to explain to

^{16/} Consideration of evidentiary issues is beyond the scope of this opinion, which addresses only the ethical implications of using certain technologies.

^{17/} For example, with respect to the impact of inadvertent disclosure on the attorney-client privilege or work-product protection, rule 502(b) of the Federal Rules of Evidence states: “When made in a Federal proceeding or to a Federal office or agency, the disclosure does not operate as a waiver in a Federal or State proceeding if: 1. the disclosure is inadvertent; 2. the holder of the privilege or protection took reasonable steps to prevent disclosure; and 3. the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).” As a practical matter, attorneys also should use appropriate confidentiality labels and notices when transmitting confidential or privileged client information.

^{18/} In certain circumstances, it may be appropriate to obtain a client’s informed consent to the use of a particular technology.

^{19/} In this opinion, we are applying the factors to the use of computers and wireless connections to assist the reader in understanding how such factors function in practice. Use of other electronic devices would require similar considerations.

employee what obligations exist with respect to confidentiality[.]) In addition, access to the laptop by Attorney's supervisor would be appropriate in light of her duty to supervise Attorney in accordance with rule 3-110 and her own fiduciary duty to Client to keep such information confidential.

With regard to the use of a public wireless connection, the Committee believes that, due to the lack of security features provided in most public wireless access locations, Attorney risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on Client's matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall.^{20/} Depending on the sensitivity of the matter, Attorney may need to avoid using the public wireless connection entirely or notify Client of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so.^{21/}

Finally, if Attorney's personal wireless system has been configured with appropriate security features,^{22/} the Committee does not believe that Attorney would violate his duties of confidentiality and competence by working on Client's matter at home. Otherwise, Attorney may need to notify Client of the risks and seek her informed consent, as with the public wireless connection.

CONCLUSION

An attorney's duties of confidentiality and competence require the attorney to take appropriate steps to ensure that his or her use of technology in conjunction with a client's representation does not subject confidential client information to an undue risk of unauthorized disclosure. Because of the evolving nature of technology and differences in security features that are available, the attorney must ensure the steps are sufficient for each form of technology being used and must continue to monitor the efficacy of such steps.

This opinion is issued by the Standing Committee on Professional Responsibility and Conduct of the State Bar of California. It is advisory only. It is not binding upon the courts, the State Bar of California, its Board of Governors, any persons, or tribunals charged with regulatory responsibilities, or any member of the State Bar.

^{20/} Local security features available for use on individual computers include operating system firewalls, antivirus and antispam software, secure username and password combinations, and file permissions, while network safeguards that may be employed include network firewalls, network access controls such as virtual private networks (VPNs), inspection and monitoring. This list is not intended to be exhaustive.

^{21/} Due to the possibility that files contained on a computer may be accessed by hackers while the computer is operating on an unsecure network connection and when appropriate local security features, such as firewalls, are not enabled, attorneys should be aware that *any* client's confidential information stored on the computer may be at risk regardless of whether the attorney has the file open at the time.

^{22/} Security features available on wireless access points will vary and should be evaluated on an individual basis.

TAB B




Cincinnati Bar
ASSOCIATION



Social Media: Common Sense and Caution


Brian R. Redden Brett M. Renzenbrink
bredde@bhmklaw.com brenzenbrink@bhmklaw.com
513.579.1500

Buechner Haffer Meyers & Koenig



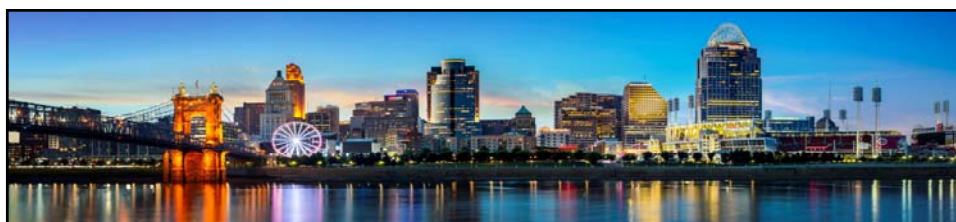
- 3 billion people use social media in some form – 42% of global population
 - 1.4 billion active Facebook accounts, visits from 76% daily
- 11 new users per second
- Site placement – 1) Facebook, 2)Instagram, 3)Snapchat.... 6) LinkedIn, 7)Twitter
- Average American uses 3 social media platforms, over half are on 2
- 80% of social media time is on mobile

www.skyword.com/contentstandard.marketing/marketing/10-social-media-usage-statistics-you-should-know-and-what-they-mean-for-your-marketing-strategy/ ; <http://www.pewinternet.org/2018/03/01/social-media-use-2018-acknowledgments/> ; <http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/>





Poses more significant threat in a regulated environment like a law practice – danger of imputed responsibility to lawyer for actions of staff / paralegals

BHMK

1. Social Media Profiles/Posts May Constitute Legal Advertising

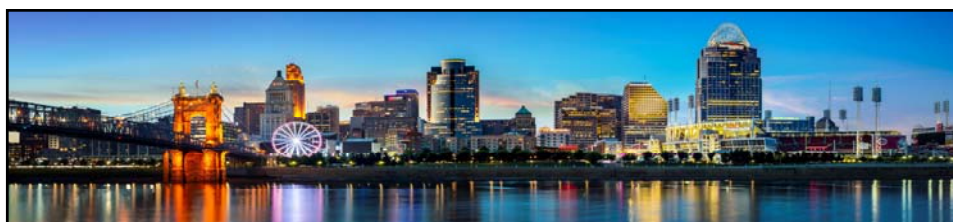
- In Ohio, lawyer and law firm websites are deemed to be advertisements. Because social media profiles (including blogs, Facebook pages, and LinkedIn profiles) are by their nature websites, they too may constitute advertisements. Safest to assume that they do.
- Florida – Specifically changed ethics rules to include lawyer websites, profiles, and on-line advertising to require advertising disclaimers
- California - Ethics Opinion 2012-186 concluded that the lawyer advertising rules in that state applied to social media posts, depending on the nature of the posted statement or content.

BHMK



2. Avoid Making False or Misleading Statements

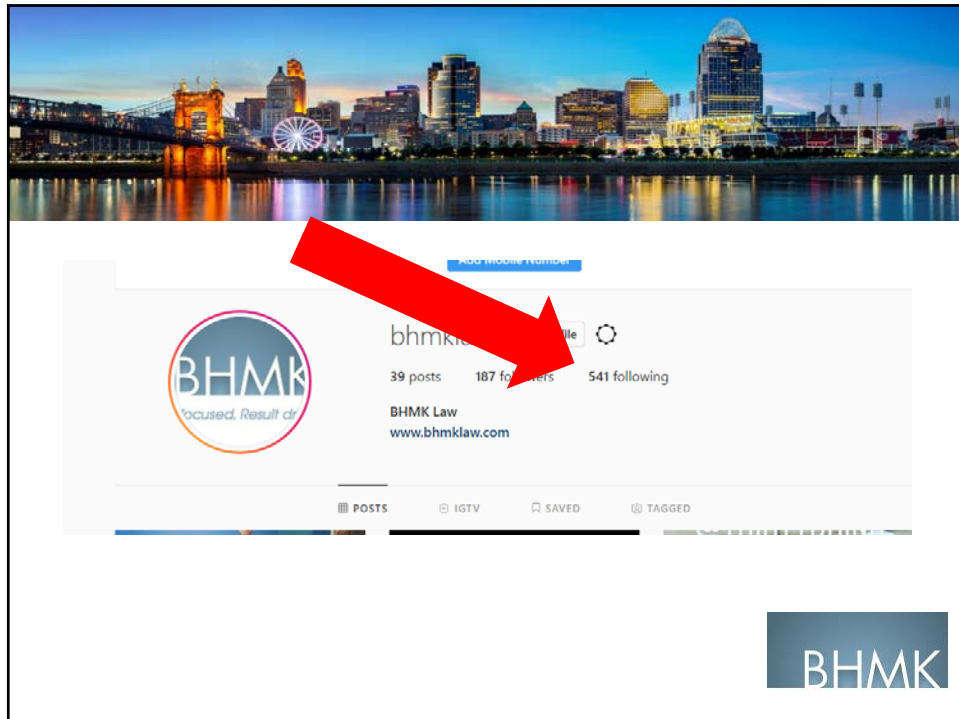
- Ohio Ethics Rules 4.1 (Truthfulness in Statements to Others), 4.3 (Dealing with Unrepresented Person), 4.4 (Respect for Rights of Third Persons), 7.1 (Communication Concerning a Lawyer's Services), 7.4 (Communication of Fields of Practice and Specialization), and 8.4 (Misconduct).
- ABA Formal Opinion 10-457 concluded that lawyer websites must comply with the ABA Model Rules that prohibit false or misleading statements. The same obligation extends to social media websites.
- Beware claims of "expertise" or "specialization"



3. Avoid Making Prohibited Solicitations

- Solicitations by a lawyer or a law firm offering to provide legal services and motivated by pecuniary gain are restricted under Ohio Ethics Rule 7.3. Ohio, but not all states, recognizes limited exceptions for communications to other lawyers, family members, close personal friends, persons with whom the lawyer has a prior professional relationship, and/or persons who have specifically requested information from the lawyer.
- Beware automatic connection requests and open solicitations. Beware LinkedIn automatic connection request renewals.





4. Avoid Disclosing Privileged or Confidential Information

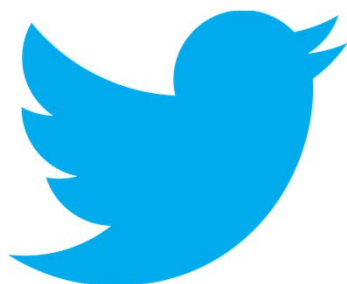
- Duty to protect privileged and confidential client information extends to current clients (ORPC 1.6), former clients (ORPC 1.9), and prospective clients (ORPC 1.18).
- ABA Formal Opinion 10-457 provides that lawyers must obtain client consent before posting information about clients on websites. Could include the casual use of geo-tagging in social media posts or photos that may inadvertently reveal your geographic location when traveling on confidential client business.
- In re Skinner, 740 S.E.2d 171 (Ga. 2013), the Georgia Supreme Court rejected a petition for voluntary reprimand (the mildest form of public discipline permitted under that state's rules) where a lawyer admitted to disclosing information online about a former client in response to negative reviews on consumer websites.



4. Avoid Disclosing Privileged or Confidential Information


- Illinois Supreme Court in *In re Peshek*, M.R. 23794 (Ill. May 18, 2010) suspended an assistant public defender from practice for 60 days for, among other things, blogging about clients and implying in at least one post that a client may have committed perjury. The Wisconsin Supreme Court imposed reciprocal discipline on the same attorney for the same misconduct. *In re Disciplinary Proceedings Against Peshek*, 798 N.W.2d 879 (Wis. 2011)
- Virginia Supreme Court held in *Hunter v. Virginia State Bar*, 744 S.E.2d 611 (Va. 2013), that confidentiality obligations have limits when weighed against a lawyer's First Amendment protections. Held that although a lawyer's blog posts were commercial speech, the Virginia State Bar could not prohibit the lawyer from posting non-privileged information about clients and former clients without the clients' consent where (1) the information related to closed cases and (2) the information was publicly available from court records

BHMK




"So #blessed to now be working
with @ABCcorp as legal counsel!
#BestFirmInAmerica"

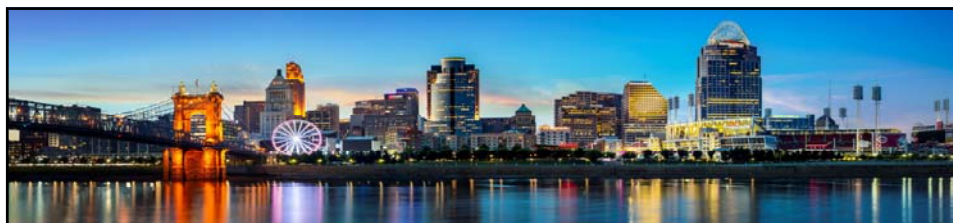
BHMK



5. Do Not Assume You Can "Friend" Judges

- ABA Formal Opinion 462 concluded that a judge may participate in online social networking, but in doing so must comply with the Code of Judicial Conduct. Several states have adopted similar views, including Connecticut (Op. 2013-06), Kentucky (Op. JE-119), Maryland (Op. 2012-07), New York (Op. 13-39, 08-176), *Ohio (Op. 2010-7)*, South Carolina (Op. 17-2009), and Tennessee (Op. 12-01).

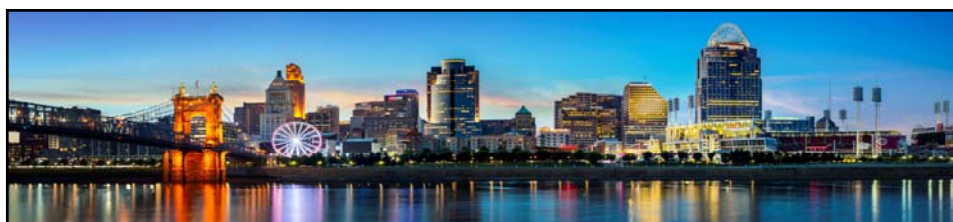




5. Do Not Assume You Can “Friend” Judges

- California (Op. 66), Florida, Massachusetts (Op. 2011-6), and Oklahoma (Op. 2011-3) have adopted a more restrictive view.
- Florida Ethics Opinion 2009-20 concluded that a judge cannot friend lawyers on Facebook who may appear before the judge because doing so suggests that the lawyer is in a special position to influence the judge. Florida Ethics Opinion 2012-12 extended the same rationale to judges using LinkedIn and the more recent Opinion 2013-14 further cautioned judges about the risks of using Twitter. Consistent with these ethics opinions, a Florida court held that a trial judge presiding over a criminal case was required to recuse himself because the judge was Facebook friends with the prosecutor. See *Domville v. State*, 103 So. 3d 184 (Fla. 4th DCA 2012).

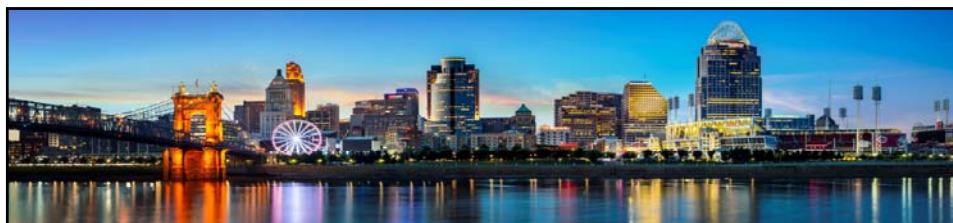
BHMK



6. Avoid Communications with Represented Parties

- Under ORPC 4.2, a lawyer is forbidden from communicating with a person whom the lawyer knows to be represented by counsel without first obtaining consent from the represented person's lawyer. Under ORPC 8.4(a), prohibition extends to any agents (secretaries, paralegals, private investigators, etc.) who may act on the lawyer's behalf.
- Effectively prohibit lawyers and their agents from engaging in social media communications with persons whom the lawyer knows to be represented by counsel. Means no Facebook friend requests or LinkedIn invitations to opposing parties known to be represented by counsel in order to gain access to those parties' private social media content.
- Viewing publicly accessible social media content that does not precipitate communication with a represented party (e.g., viewing public blog posts or Tweets) is generally considered fair game.

BHMK



7. Be Cautious When Communicating with Unrepresented Third Parties

- ORPC 3.4 (Fairness to Opposing Party and Counsel), 4.1 (Truthfulness in Statements to Others), 4.3 (Dealing with Unrepresented Person), 4.4 (Respect for Rights of Third Persons), and 8.4 (Misconduct) protects third parties against abusive conduct.
- In a social media, these rules require lawyers and their staff to be cautious in online interactions with unrepresented third parties. Publicly viewable social media content is generally fair game. If the information sought is behind the third party's privacy settings, ethical constraints may limit the options for obtaining it.
- Consensus appears to be that a lawyer may not attempt to gain access to non-public content by using subterfuge, trickery, dishonesty, deception, or an alias. Kentucky (Op. KBA E-434) has concluded that lawyers are not permitted (either themselves or through agents) to engage in false or deceptive tactics to circumvent social media users' privacy settings to reach non-public information.


BHMK



8. Avoid Inadvertently Creating Attorney-Client Relationships

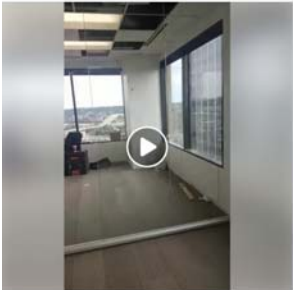
- ABA Formal Opinion 10-457 recognized that by enabling communications between prospective clients and lawyers, websites may give rise to inadvertent lawyer-client relationships and trigger ethical obligations to prospective clients under RPC 1.18.
- The interactive nature of social media creates a risk of inadvertently forming attorney-client relationships with non-lawyers, especially when the objective purpose of the communication from the consumer's perspective is to consult with the lawyer about forming a lawyer-client relationship regarding a specific matter or legal need. If an attorney-client relationship attaches, so do obligations to maintain the confidentiality of client information and to avoid conflicts of interest.
- Use of clear, obvious disclaimers can avoid the problem.

BHMK



Buechner Hoffer Meyers & Koenig Co., LPA
Published by BHMK Law 111 October 26 at 4:13 PM

Moving Your Business? So Are We. There are many legal, cost, and Contractual Considerations in moving Your Business Headquarters. Do your due diligence with BHMK and make sure your legal needs are covered, your contracts are tight, and your costs are minimized. We Grow Cincinnati! #BHMK #TheSolutionsFirm <https://www.bhmklaw.com/movingyourbusiness> #contracts #lease #Cincy



Are You Moving Your Business? We Are! [Send Message](#)


143 People Reached 12 Engagements [Boost Post](#)

John R Kauffer III and 4 others 1 Share 74 Views

Like Comment Share

Write a comment...
Press Enter to post.

Jane Doe: "Actually we are! My lease is "triple net" – what does that mean?"




9. Avoid UPL Allegations and be aware of jurisdictional boundaries

- Social media knows no geographic boundaries!!
- Under RPC 8.5 and analogous state rules, a lawyer may be disciplined in any jurisdiction where he or she is admitted to practice (regardless of where the conduct takes place) or in any jurisdiction where he or she provides or offers to provide legal services.

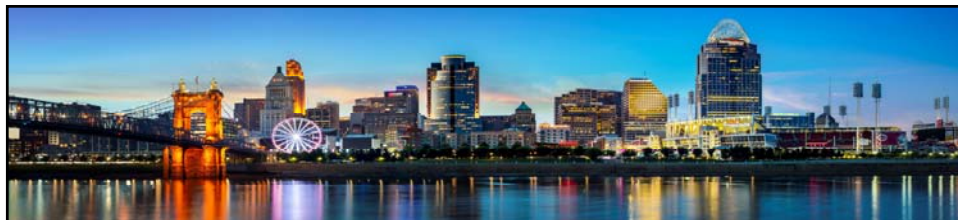




10. Caution with Testimonials, Endorsements, and Ratings

- LinkedIn and Avvo promote the use of testimonials, endorsements, and ratings (either by peers or consumers). But, there is little or no attention given to ethics rules.
- Some jurisdictions prohibit or severely restrict lawyers' use of testimonials and endorsements or may require those to be accompanied by disclaimers.
- South Carolina Ethics Opinion 09-10 provides that (1) lawyers cannot solicit or allow publication of testimonials on websites and (2) lawyers cannot solicit or allow publication of endorsements unless presented in a way that would be misleading or likely to create unjustified expectations. Also concluded that lawyers who claim their profiles on social media sites are responsible for conforming the information on their profiles to the ethics rules.

BHMK



ONLINE MARKETING-


KY vs. OH

BHMK






- **Kentucky**
- Advertising in Kentucky is governed by:
 - Supreme Court Rules 3.130-7.01 – 7.60
 - Attorneys’ Advertising Commission Regulations
- SCR 3.130(7.25) Identification of Advertisements
 - “The words ‘THIS IS AN ADVERTISEMENT’ must be prominently displayed on every page of any advertisement in writing, and displayed without scrolling on the first screen of every page of a website.”
- SCR 3.130-7.02(1) defines the word advertise: “to furnish any information or communication concerning a lawyer’s name or other identifying information.”
 - Numerous exceptions – see rule
 - Also see AAC Regulation No. 13
- The following information is available at:
<http://www.kybar.org/general/custom.asp?page=attorneyadvertising>






- The definition of advertise does not include information provided by a lawyer “in public speaking forms, radio, television broadcasts, or **postings on the Internet that permit real-time communication** and exchanges on topics of general interest in legal issues, provided there is no reference to an offer by the lawyer to render legal services.” SCR 3.130-7.02(1)(j)
- Advertisements, including websites, must be submitted to the AAC.
 - All websites qualifying as advertisement in Kentucky must be submitted to the Kentucky Bar Association.
 - Most websites (those that include more than “bare bones” information) must be submitted with a filing fee of \$75. An additional fee of \$100 may be imposed for those submissions received after the publication of the advertisement.
 - See SCR 3.130(7.05) for additional details regarding number of copies and other requirements.

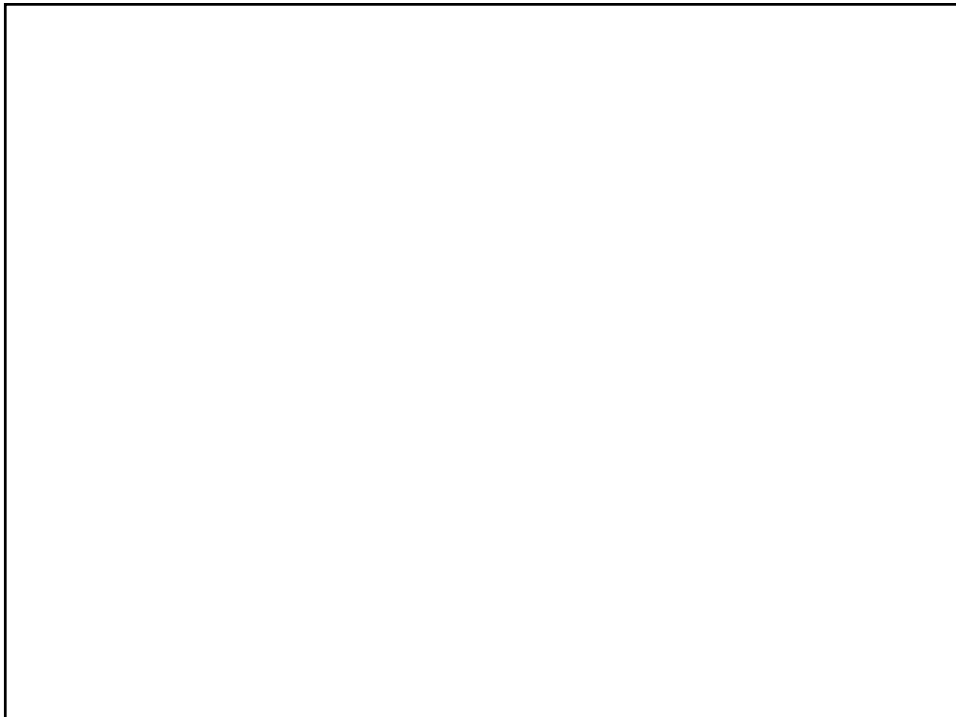
- Website Updates
 - Whenever “substantive changes” are made to a web site, the updates must be submitted to the AAC.
 - These do not include typographical changes, changes in links to sources, or any item listed in SCR 3.130-7.05(1)(a) or AAC Regulation 2.
- Social Media
 - If communication meets the definition of an advertisement under SCR 3.130-7.02(1), it must be submitted to the AAC.
- Generally, a lawyer **cannot** use real-time electronic means to initiate contact with potential clients. SCR 3.130-7.09(1). However, this is appropriate with existing clients, as this communication is not an advertisement. SCR 3.130-7.02(1)(h).
- KBA Frequently Asked Questions:
[http://cymcdn.com/sites/www.kybar.org/resource/resmgr/Advertising/AAC_FAQs_w-Links - Eff_07011.pdf](http://cymcdn.com/sites/www.kybar.org/resource/resmgr/Advertising/AAC_FAQs_w-Links_Eff_07011.pdf)





- **Ohio**

- Lawyers in Ohio are free to advertise through any medium, so long as they comply with the advertising standards established by the Supreme Court of Ohio.
 - Prof. Cond. Rule 7.1: Cannot contain any false, deceptive, or misleading statements.
 - o Comment 3: Client testimonials can be tricky. They can be misleading if they create an expectation that the same results would be obtained by a client in a similar situation.
 - o Comment 4: Use of the terms “special, lowest, below cost, giveaway, cut-rate, or discount” are considered misleading.



TAB C



Cincinnati Bar
ASSOCIATION

Brain Disorders and the Impaired Attorney: Problems and Solutions



Patrick J. Garry
Associate Director, Ohio Lawyers Assistance Program

1

“Houston, we’ve had a problem.”

“Houston, we [still] have a problem.”

2

Prevalence of Substance Use and Other Mental Concerns Among American Attorneys

The American Bar Association Commission on Lawyer Assistance Program and Hazelden Betty Ford Foundation released their study in the Journal of Addiction Medicine that, thus far, is the most comprehensive of its kind in February, 2016.

So, here are the new numbers...

3

... the old number were, well, old... from 1990. A few of the new numbers...

- Random sample of **12,825** licensed, employed attorneys completed surveys, assessing alcohol use, drug use, and symptoms of depression, anxiety, and stress.
- **20.6%** licensed, employed attorneys screen positive for hazardous, harmful and potentially alcohol-dependent drinking.
- **28%** struggle with some level of depression.
- **19%** demonstrate symptoms of anxiety.

4

... of note:

- “Younger attorneys – those in their first 10 years of practice – exhibit the highest incidence of these problems.
- Men had a higher proportion of positive screens.
- **The most common barriers for attorneys seeking help were fears of others finding out and general concerns about confidentiality.**
- Attorneys, compared with other professionals, are leaders in alcohol use disorders and mental health disease.
- Attorney impairment poses a variety of risks: to individuals, to organization [firms], to communities, to government, to the economy, and to families.

5

... of further note:

Brain disorders – and accompanying disordered thoughts – occur without regard to age, race, sexual preference, economic standing, religious views, political affiliation, etc. You get the idea, right?

Genetic predisposition may play a role, but recent studies reveal that behavior has a significant impact upon gene expression.

6

**... no one wants a health problem...
especially a “mental health” problem...**

Stigma. Stigma. Stigma.

- a mark of disgrace associated with a particular circumstance, quality or person.
- “the stigma of mental disorder”
- synonyms: shame, disgrace, dishonor, ignominy, opprobrium, humiliation, (bad) reputation

7

**... but these conditions are often chronic,
fatal, and progressive...**

... and, most importantly, treatable.

There is a solution.

8

... but, self-diagnosis is difficult

A few signs of disorders:

- Behavioral changes as simple as coming in late or leaving early.
- Decrease in production and quality of work product.
- Increased isolation. Few appearance at work-related functions.
- Discernable mood changes that may include irritability and apathy.
- When confronted, many plausible explanations, avoidance, and/or insistence that there is no problem.
- The odor of alcohol is “on or about” the person...at work.

9

“If you want something done right, do it yourself...right?”

...some exception, absent appropriate experience:

- Plumbing, electrical, HVAC
- Automobile repair, including body work.
- Roofing, house painting, chimney work.
- Blacktopping, concrete work.
- Severe lacerations.
- Treating broken bones, including vertebrae.
- Heart disease.
- Mental health problems, including alcohol use disorders.

10

Solutions

- Personally, prepare like a champion: rest, nutrition, physical activity, hobby, nurture healthy relationships, serve others, etc.
- Personally, seek services, if possible. This is not probable.
- On behalf of others, take action...

11

Take Action

- Contact OLAP for any reason. The communications are confidential.
- Educate yourself by speaking to those with experience and knowledge.
- Open your mind to the possibility that an intervention of some sort may be necessary and life saving... and career saving.
- Gather the undisputed facts.
- Assess the risk to the organization. The risk to the individual is their life.
- Assess organization's willingness to exercise leverage.
- Confidentiality, dignity, respect, support, and empathy are required.

12

The Good News

Attorneys recover from brain disorders and impairments at a remarkable rate... once they begin the process.

The challenge remains: On a case-by-case basis, just how do we – collectively and individually – create an environment that allows an impaired person to begin the process?

Let's talk about that. Do not hesitate to call.

13

ohiolap.org

Scott Mote, Executive Director

Patrick J. Garry, Associate Director, 513/623-6853

14

TAB D



Cincinnati Bar
ASSOCIATION

Gregory L. Adams

OSBA Certified Specialist in Family Relations Law
Croswell & Adams Co., L.P.A.
Cincinnati, Ohio

Mr. Adams received his BA from Wabash College and his JD from the Salmon P. Chase College of Law. He concentrates his practice in all facets of family relations law. Mr. Adams' distinctions include selection by Best Lawyers since 2007 – he was named as their 2015 Cincinnati Family Law "Lawyer of the Year" – and being identified as one of the Top 100 Ohio Super Lawyers as well as one of the Top 50 Cincinnati Super Lawyers. He is a Certified Family Relations Law specialist in Ohio. He is also a Fellow in the American Academy of Matrimonial Lawyers and a Life Fellow of the American Bar Foundation. Mr. Adams' other memberships include the American Bar Association, Ohio State Bar Association, Cincinnati Bar Association, Cincinnati Academy of Collaborative Professionals, and the International Academy of Collaborative Professionals. He has been involved with collaborative law since its inception in Ohio in 1998. Mr. Adams completed mediation training at Harvard Law School. He is a frequent lecturer on topics related to family law. For additional information, please visit www.croswelladams.com.

Phyllis G. Bossin

Location:

Cincinnati, Ohio

Phone:

513-421-4420

Fax:

513-421-0691

Email:

pbossin@bossinlaw.com

Phyllis Bossin is a dedicated and passionate family law attorney. She cares deeply about her clients and brings her passion, caring and skill to every case she and her associates handle.

Phyllis knows that the best path to resolution occurs outside of the courtroom where people can control their own outcomes. She brings her experience and expertise to settlement negotiations. When appropriate, Phyllis takes her cases to mediation. As a trained mediator herself, she can apply her expertise to help achieve resolution. Phyllis is also trained in collaborative law, another form of dispute resolution that involves a commitment by the parties to resolve their differences outside of the courtroom. Finally, as a trained arbitrator, Phyllis can serve parties and their counsel by arbitrating and deciding their cases.

However, when reasonable alternative paths to resolution fail, Phyllis is ready to litigate. As an experienced, persuasive, and successful litigator of family law, she brings decades of highly-honed trial skills to bear.

Phyllis is the principal and founder of Phyllis G. Bossin and Associates. Her practice includes all aspects of family law, including

- Divorce and dissolution of marriage
- Marital settlement agreements
- Spousal support
- Child custody and support
- Equitable division of property
- Prenuptial and cohabitation agreements
- Business valuations

Phyllis drafts highly detailed and nuanced settlement agreements involving complex cases, which may involve intricate business valuations and complicated tax issues. To assist in the resolution of these issues, Phyllis has developed long-standing relationships with highly competent experts in related fields, including forensic accountants and tax and estate planning attorneys, all of whom are ready to provide specialized support whether the case is resolved outside of the courtroom or in litigation.

Ms. Bossin is licensed to practice in the state of Ohio, and admitted to practice in the federal courts of the Southern District of Ohio, the Eastern District of Kentucky, **and** the United States Supreme Court.

Certification

Phyllis is a certified as a Family Relations Law Specialist by the Ohio State Bar Association.

Honors and Distinctions

- Best Lawyers of America (25+ years)
- Law and Politics Media, Inc. Super Lawyers since inception
 - Top 25 Women Lawyers in Cincinnati,
 - Top 50 Women Lawyers in Ohio,
 - Top 50 Lawyers in Cincinnati,
 - Top 100 Lawyers in Ohio, and
 - Family Law Super Lawyer.
- Cincy Magazine – Cincinnati Leading Lawyer
- Cincinnati Business Courier – Who's Who in Cincinnati Law

Organizational Leadership

ACFTL – Phyllis is a Diplomate of The American College of Family Trial Lawyers. The College is a select group of “100” of the top family law trial lawyers from across the United States. Diplomates are chosen based upon their recognized litigation skills and courtroom abilities

AAML – Phyllis is a long-standing fellow of the American Academy of Matrimonial Lawyers and has served as the President of the Ohio Chapter

ABA – As an active member of the American Bar Association, Phyllis has served in many capacities, including

- Chair of the Section of Family Law
- Member of the Commission on Domestic and Sexual Violence,
- Member of The Justice Kennedy Commission on Criminal Justice Reform,
- Liaison to the Commission on Women in the Profession
- Faculty of the ABA Family Law Section Trial Advocacy Institute, an intensive trial skills program for attorneys
- Member of the Section of International Law

Ms. Bossin graduated from the University of Cincinnati, where she received both her undergraduate degree and a master's degree. She received her law degree from the Salmon P. Chase College of Law.

PATRICK J. GARRY, Esq.
Associate Director, OLAP

Initial formative years: Pleasant Ridge, Cincinnati, OH.

St. Xavier High School, 1982.

Boston College, 1986.

University of Cincinnati College of Law, 1991.

Admitted to practice law in 1991.

Area of practice: Criminal law.

Continuously married since November 1994.

Parent since February 1998 and April 2000.

Gateway House, Board Member.

Mental Health and Recovery Services Board of Hamilton County, Board Member.

Interests: various, including being an appropriate spouse, son, sibling, parent, attorney, friend, neighbor, citizen, etc...

Brian R. Redden
Buechner Haffer Meyers & Koenig Co. LPA

Brian's primary work is helping privately-owned businesses avoid and, if necessary, defend against employment practices violations and lawsuits, and protect the competitive edge those businesses have gained through hard work and sacrifice. Brian handles the whole spectrum of employment and trade secret law: employment agreements, non-compete agreements, trade secret protection, employment policies, employee handbooks, executive compensation, employee recruiting and job placement, employee counseling, negotiation of severance agreements, non-litigated resolution of employment disputes, and trials and appeals of employment and trade secret disputes.

Brian also handles disputes involving business transactions, business ownership, personal injury, construction (particularly mechanic's liens, lien enforcement, and general contractor and subcontractor issues), and environmental matters.

In past practice, Brian represented amateur (high school and college age) and professional athletes in negotiating and enforcing player and endorsement contracts and has more recently pursued agent malpractice and professional liability claims for negligently negotiated agreements that damaged professional athletes and their earning potential. Brian has also assisted a number of professional athletes in creating and operating charitable foundations and non-profit organizations.

Education

- **Northern Kentucky University, Salmon P. Chase College of Law, Highland Heights, Kentucky**
 - Honors: cum laude
 - Honors: Student Bar Association Representative of the Year Award, 1997-1998
 - Honors: Who's Who Among Students in American Colleges and Universities, 1998-1999
- **Xavier University**
 - Bachelor of Arts *magna cum laude* - 1994
 - Honors: University Scholar
 - Major: History

Brett Renzenbrink
Buechner Haffer Meyers & Koenig Co. LPA

Brett acts as "Outside CLO" (Chief Legal Officer) for a number of start-ups, emerging, and established Cincinnati/Northern Kentucky organizations of all sizes (from single member LLC start-ups to companies with nine-figure annual revenue and hundreds of employees). In this role, Brett adds accretive value to his client-partner's growth, while forecasting blind spots and mitigating risk. In particular, Brett enjoys:

1. Working with entrepreneurs/investors/business-owners to design corporate strategy, and build out plans for growth/protection;
2. Analyzing property/leasing issues;
3. Developing and implementing best practices for compliance with employees and independent contractors;
4. Negotiating with vendors and customers to create maximum net-benefit business relationships;
5. Instituting pro-active/preventative litigation strategy and defending/enforcing corporate rights when suit is initiated (including internal partner disputes);

Brett also has extensive experience working with transportation/logistics companies (in particular 3PLs) on architecting motor carrier/customer strategy, handling unique employee or compliance issues, and pursuing commercial collections.

Brett has a track record of implementing creative techniques to assist clients (including architecting the "shared services platform" for Non-Profits, which dovetails with the "Outside CLO" platform) and go over and above to establish extreme, results/deliverable-oriented service without forcing clients into unreasonable big firm fee structures.

Education

- **Northern Kentucky University, Salmon P. Chase College of Law, Highland Heights, Kentucky**
 - J.D. *cum laude* - 2010
- **Ohio State University**
 - B.A. *cum laude* - 2007
 - Honors: With Honors
 - Major: Sociology and Honors Interpersonal Communication/Writing



Carolyn A. Taggart

As a trial attorney for more than 35 years, Carolyn has extensive jury and bench trial and appellate experience in both state and federal courts. She has substantial experience in the areas of product liability, legal malpractice, complex commercial cases, and has defended youth organizations in cases involving child sexual abuse.

Carolyn has been recognized for her litigation skills through her induction into the American College of Trial Lawyers as a Fellow, and is also a past president of the Ohio Association of Civil Trial Attorneys. She is a faculty member for the National Institute of Trial Advocacy at the University of Cincinnati College of Law. Carolyn has been recognized among the top ten attorneys in Ohio and the top five attorneys in Cincinnati by *Ohio Super Lawyers*®. She was named in 2012 and 2017 as *Best Lawyers*® Cincinnati, Ohio “Lawyer of the Year” – Product Liability Litigation-Defendants.

Bar Admissions

Ohio

Kentucky

U.S. Court of Appeals for the Sixth Circuit

U.S. District Court for the Northern District of Ohio

U.S. District Court for the Southern District of Ohio

U.S. District Court for the Eastern District of Kentucky

U.S. District Court for the Western District of Kentucky

Supreme Court of the United States

Presentations

- “Use of Social Media Searches of Jurors, Before, During and After Trial,” American College of Trial Lawyers, Cincinnati Bar Association, University of Cincinnati Law’s Center for Practice, Oct. 27, 2018
- “Sharing our Experience: How Women’s Initiatives Can Impact Your Legal Practice Setting,” OACTA Women in the Law Seminar, June 15, 2018
- “Arbitration v. Litigation: Where do you Want to Try Your Commercial Dispute?” Porter Wright Annual Ethics & Trends in Litigation Seminar, Dec. 1, 2010

Honors | Awards

Partner

ctaggart@porterwright.com

513.369.4231

www.porterwright.com

250 East Fifth Street
Suite 2200
Cincinnati, OH 45202

EDUCATION

University of Cincinnati College of
Law, J.D., 1978

Miami University, B.S., *cum laude*,
1973

SERVICES

Litigation

- Product liability
- Commercial litigation
- Catastrophic injuries
- Professional liability
- Class actions and mass tort litigation
- Appellate and Supreme Court practice
- Arbitration and mediation
- Health care litigation

Labor & Employment

- Employment litigation

Health Care

- Litigation

- Cincinnati Bar Association, John P. Kiely Professionalism Award, 2018
- *Best Lawyers*®, Cincinnati, Ohio Product Liability Litigation – Defendants “Lawyer of the Year,” 2012, 2017
- University of Cincinnati Law Alumni Association, Distinguished Alumni Award, 2016
- *The Best Lawyers in America*®, Product Liability Litigation-Defendants
- *Ohio Super Lawyers*®, Civil Litigation: Defense
- *Ohio Super Lawyers*®, “Top 5 Cincinnati Attorneys,” 2017, 2018
- *Ohio Super Lawyers*®, “Top 10 Attorneys in Ohio,” 2017
- Ohio Association of Civil Trial Attorneys, Excellence in Advocacy Award, 2015
- Ohio Association of Civil Trial Attorneys, Distinguished Contributions to the Community Award, 2013
- Ohio State Bar Association, Eugene R. Weir Award for Ethics and Professionalism, 2007
- Defense Research Institute Exceptional Performance Award, 2003-2004

Community

- Cincinnati Good Samaritan Hospital Foundation, Board of Trustees
- Andy Caress Melanoma Foundation, Board Member
- Lawyer to Lawyer Mentoring Program
- Diocesan Catholic Children’s Home, Member, Personnel Committee and past Board Member
- University of Cincinnati College of Law, Board of Visitors
- Product Liability Moot Court Competition Judge
- Federal Court, Volunteer Mediator

PROFESSIONAL ASSOCIATIONS

- Supreme Court of Ohio, *Board of Professional Conduct*
- Cincinnati Bar Association, *Grievance Committee*, past Chair
- Ohio State Bar Association
- Kentucky Bar Association
- Northern Kentucky Bar Association
- Federal Bar Association
- Ohio Association of Civil Trial Attorneys, Vice Chair, *Business and Commercial Litigation Committee*, past President
- American Board of Trial Advocates
- Defense Research Institute
- American College of Trial Lawyers, Fellow

ATTORNEY PROFILE

Melissa Thompson Millard is an associate attorney with Barbara J. Howard Co., L.P.A., A Legal Professional Association, located in Cincinnati, Ohio. From her position at the law firm, Ms. Thompson Millard focuses her practice primarily on family and matrimonial law; however, she also provides comprehensive and effective estate planning services for clients looking to protect themselves and their loved ones for the future.

Licensed to practice in Ohio and Kentucky, Ms. Thompson Millard represents clients throughout both states who are dealing with legal matters related to divorce, child custody and support, property division, alimony and other related issues. A highly rated attorney, Ms. Thompson Millard works closely with all clients she serves, treating them with the compassion and respect they deserve while advocating on behalf of their rights and best interests.

In 2011, Ms. Thompson Millard graduated with the highest distinction from Indiana University Bloomington, where she earned a Bachelor of Science in human development and family studies and a Bachelor of Arts in French. She then attended the University of Cincinnati College of Law, obtaining her Juris Doctor, magna cum laude, in 2014 and graduated as a member of the Order of the Coif. In 2014, she was admitted to the practice of law in Ohio, and in 2015, she was admitted to the practice of law in Kentucky.

While pursuing her legal degree, Ms. Thompson Millard was active with the *University of Cincinnati Law Review*, where she served as notes and comments editor, and she was a fellow with the college's *Glenn M. Weaver Institute of Law and Psychiatry*. She also published an article with the *University of Cincinnati Law Review* that discussed judicial remedies under the Hague Convention.