Vermont Bar Association
Seminar Materials

Best Practices for Cloud Security & Storage

October 14, 2016
Lake Morey Resort
Fairlee, VT

Speakers:

Michael Kennedy, Esq.
Drew Palcsik, Esq.
Protect Yourself:
Cloud & Mobile Security Basics

Michael Kennedy, Esq.
And
Drew Palcsik, Esq.

SAAS is:

1. Centrally Hosted; and
2. Licensed on a Subscription Basis
Microsoft Word
Version 6.0

Office 365

KEEP CALM because WE HAVE NO RULES
How Hackable Is Your Wireless Keyboard and Mouse?

An Internet-of-things security startup says a flaw with some non-Bluetooth wireless keyboards and mice makes it simple to hack into your computer.

By Rachel Metz    February 23, 2016
Communication

Data Storage
Data Synchronization
Duty to Preserve Confidentiality

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

When transmitting information relating to the representation, lawyer must:

Take reasonable precautions to prevent information from coming into hands of unintended recipients
VBA Ethics Opinion 10-06
Factors

- The vendor's security system
- Practical/foreseeable limits to access of data
- Material terms of the user agreement
- Vendor's commitment to protecting confidentiality

VBA Ethics Opinion 10-06
Factors

- Nature and sensitivity of data
- Practice-specific obligations
- Notice provisions if a third party seeks or gains access

VBA Ethics Opinion 10-06
Other Considerations Noted

- Giving notice to client
- Asking competent personnel to review the security
- Establishing system for periodic review
- Staying abreast of developments
VBA Ethics Opinion 10-06

retrieving client property, as long as they take re

Formal Opinion 2010-079

Factors

What makes this tool different?
Is it reasonably simple to add security?
Are there limits to who has access?
What are the client’s instructions?
Formal Opinion 2010-079
Factors

How sensitive is the data?
Would a privilege be waived?
Are there consequences to a third-party who g
How urgent is the need?

"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 monitor the efficacy of such steps."

Takeaways:

Not just for the “tech savvy.”
Reasonable, not perfect.
No substitution for communication.
NYSBA Ethics Opinion 842

Factors

Does the storage provider have an obligation to preserve the client data?

Will the lawyer be notified prior to complying with the provider's request?
Are you confident the provider’s security measures are adequate?
Is technology employed to reasonably safeguard against unauthorized access?
Can you wipe data securely?
Can you export data in a conventional format?

Technological advances to ensure that the security measures remain effective.
NYSBA Ethics Opinion 842

Privilege to ensure that storing information in

Goal is NOT minimum competency to avoid bar discipline

Instead, goal is maximum competency to avoid losing client files.
Good Passwords

Don't worry about digits/symbols/numbers as much as how likely it is to predict

Good Passwords

Use Spaces
Don't Tell The Truth
Don’t Make Sense
Avoid Predictable Phrases
Avoid Secrets or Personal Meaning
Avoid Obvious Punctuation
FIREWALLS & VPNs

Firewall
ENCRYPTION

ENCRYPTION IN TRANSIT
ENCRYPTION AT REST
Securing The Device
SSL - ENCRYPTION IN TRANSIT
ENCRIPTING FILES
SHARING
E-MAIL

Sure!
BACKUPS

Simple System
+
Multiple Locations

Don’t Forget To Encrypt Your Backups
SUGGESTED PRACTICES

Communication

14. The Client acknowledges that the Firm may use cloud-based electronic data storage services, such as those provided by Dropbox or Apple Computer, to store and utilize provided Client data. The Firm will take all reasonable precautions to protect Client data as required by the Rules of Professional Responsibility.
For our advanced users

- Dropbox files at rest are encrypted using 256-bit Advanced Encryption Standard (AES).
- Dropbox uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) to protect data in transit between Dropbox apps and our servers. It's designed to create a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption.
- Dropbox applications and infrastructure are regularly tested for security vulnerabilities and hardened to enhance security and protect against attacks.
- Two-step verification is available for an extra layer of security at login. You can choose to receive security codes by text message or via any Time-Based One-Time Password (TOTP) apps, such as those listed here.
- Public files are only viewable by people who have a link to the file(s).

Bucket Approach

Bucket #1: Less Sensitive Data
Bucket #2: More Sensitive Data

SECURE
- Help ensure that information is only seen by your intended audience.
- Restrict what other people can do with your document content.
- Find and remove content such as metadata from your PDF files.

Resources
https://www.eff.org/privacybadger

https://www.eff.org/https-everywhere
www.paperlesschase.com

http://legaltalknetwork.com/podcasts/digital-edge/

drew@champlainvalleylaw.com
Thoughts on Email Encryption

Michael Kennedy
Bar Counsel

Rule 1.6

• A lawyer shall not reveal
  – Information relating to the representation of a client
  – Unless the client gives informed consent, or,
  – The disclosure is impliedly authorized to carry out the representation; or
  – The disclosure is required or permitted by this rule

Information Relating to the Representation

• Is much broader than the a/c privilege

• “applies not only to matters communicated in confidence by the client, but to all information relating to the representation, no matter the source.” Comment [4]
Duty to Preserve Confidentiality

• “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.”

• Rule 1.6, Comment [16]

Comment 17

• When transmitting information relating to the representation, lawyer must:

• Take reasonable precautions to prevent information from coming into hands of unintended recipients

Comment 17

• Lawyer’s duty:

  – Does not require lawyer to take special security measures

  – As long as the method of communication affords a reasonable expectation of privacy
Comment 17

• Special circumstances might warrant special precautions.
  – Sensitivity of the communication
  – Extent to which privacy of info is protected by law or by security agreement

Comment 17

• However, a client may require the lawyer to implement special security measures not required by this rule

  OR

May give informed consent to use of a means of communication otherwise prohibited by this rule

Competently Preserving Confidences

• Rule 1.1 requires lawyers to provide competent representation.

• Competence includes keeping abreast of technology and advising clients as to the benefits and risks of relevant technology.
Failing to Act Competently to Protect Confidences

- Ideas as to recent examples in Vermont?

Admonition for Violating Rule 1.6

- PRB Decision 183 (January 2015)
  - Clients fire lawyer
  - Call to ask to stop by to pick up file between 12 -2
  - Lawyer calls back and says that works
  - Clients show up, lawyer isn’t there, office is locked.
  - File on floor in common hallway shared by other tenants in the building

Admonition for Violating Rule 1.6

  - Attorney described prior outcome in such detail that new client figured out identity of previous client
Admonition for Violation Rule 1.6

- PRB Decision 3 (2000)

- Lawyer sold her computer. Her work computer. It had a hard drive.

---

E-Mail

- Right now, in Vermont, what is an attorney’s duty with respect to using email?

---

Rule 1.6

- It's most likely information relating to the representation.

- So, duty is not to disclose it absent client consent or an exception.

- Also, duty is to act competently to keep it from falling into hands of unintended recipients.

- And, to take reasonable precautions with the transmission.
So, encrypt?

• Thoughts?

Comment 17

• No duty to use special security measures.

• Is encryption a special security measure?

VBA Advisory Opinion 97-05

• A lawyer does not violate the rules by communicating with a client via unencrypted email.

• Why not?
VBA Advisory Opinion 97-05

- Not a violation to communicate via unencrypted email because:
  - 1. no less of an expectation of privacy in email than with an ordinary phone call.
  - 2. Intercepting an email is against the law.
  - Also suggests: encryption (and decryption) are difficult and very expensive

---

Expectation of Privacy

- Things I’ve seen:
  - Reply-all
  - Shared accounts
  - Forwarding emails

---

Against the Law

- Closing the barn door after the horses have escaped isn’t the best idea.
A Changing Tide – ABA Opinion 11

- When communicating via electronic means, a lawyer must:
  - Warn client about risk if there is a significant chance a third party might gain access.
    - Employers – work issued computers & mobile devices, and email accounts
    - Spouses, significant others, family members

ABA Opinion 11-459

- Instances of risk will depend on circumstances.
- Lawyer must consider whether “given the client’s situation, there is a significant risk that third parties will have access.”

State Bar of California
Formal Opinion 2010-079

- Whether attorney violates duty of confidentiality will depend on particular circumstances, including:
  - Level of security attendant to particular device/technology
  - Legal ramifications to third party who intercepts
  - Degree of sensitivity of the information
  - Possible impact on client of inadvertent disclosure
  - Urgency of situation that led to communication
  - Client’s instructions regarding means of communication
Competence = Tech Competence

• Cal Bar Opinion cited one factor as:
  
  Ability to assess level of security attendant to particular device/technology

    1. On the attorney
    2. Includes how one technology differs from others
    3. What precautions can, or cannot, be taken with each technology
    4. Can third parties access it

Cal. Bar Opinion 2010-179

• Encrypting email may be:
  
  – a reasonable step for an attorney to take in an effort to ensure the confidentiality of such communications

  – Required when the circumstance calls for it, particularly if the information at issue is highly sensitive and the use of encryption is not onerous

Cal Bar Opinion – Attorneys Must Take Steps to Protect Client Confidences

• “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 monitor the efficacy of such steps.”
Encryption

- It has become:
  - Less expensive
  - Less burdensome

So, is it a reasonable precaution?

State Bar of Wisconsin

- Encryption made easy for lawyers:

Vermont Bar Association
138th Annual Meeting
October 13-14, 2016
Lake Morey Resort, Fairlee

Best Practices for Cloud Security & Storage

Links to additional materials

VBA Advisory Ethics Opinion 2010-006:

Ethical Grounds: The Official Blog of Vermont Bar Counsel:
Hey! You! Ethics & The Cloud (January 8, 2016)
https://vtbarcounsel.wordpress.com/2016/01/08/hey-you/