Ethical Obligations Related to Cybersecurity and Use of Technology in Law Practice: What Every Attorney Needs to Know

By JoAnn Kohl and Yvonne Tingleaf

Cyber Attacks: A Growing Problem

- The total number of global security incidents detected by survey respondents was 42.8 million in 2014, an increase of 48% from 2013 (it was 28.9 million in 2013). This is a total of 117,339 attacks per day, every day, globally. *PricewaterhouseCoopers LLP, Global State of Information Security Survey 2015.*
- Seven percent of U.S. organizations lost $1 million or more due to cybercrime incidents in 2013, compared with 3% of global organizations. Nineteen percent of U.S. entities reported financial losses of $50,000 to $1 million, compared with 8% of worldwide respondents. *PricewaterhouseCoopers LLP , Global Economic Crime Survey 2014.*
- In 2013, the FBI notified 3,000 U.S. companies that they had been victims of cyber intrusions. These were undetected incidents. *2014 US State of Cybercrime Survey, co-sponsored by PricewaterhouseCoopers LLP, CSO magazine, the CERT® Division of the Software Engineering Institute at Carnegie Mellon University, and the U.S. Secret Service.*

What is a Security Incident?

- Non-exhaustive list:
  - Insider incident (employee disclosure)
  - Loss of device + sloppy password
  - Malware
  - Phishing
  - Spyware
  - Denial of service attacks
  - Others

Why Should You Care?

- Types of client data you house: Personally identifiable information, health information, financial information, confidential and proprietary business records, strategic business data, litigation-related theories and records, trade secrets, research data.
- You have an ethical and legal obligation to prevent the unauthorized disclosure of information relating to the representation of your clients.
- If you don't use reasonable measures to safeguard the confidentiality of documents and communications, it may result in waiver of attorney-client and/or work-product privilege.

Why Should You Care? (cont'd)

- If (or, when) you are breached, your data security practices will come under scrutiny by clients and the press. If you did not use best practices to safeguard client information, it will be a PR and client relationship disaster.
- Clients may require security audits, and you want to be ready for those audits. Even if clients don't require audits, they have security requirements that must be met.
- $$$ - You may incur the cost of battling administrative investigations and lawsuits, regulatory fines, and civil damages. The costs associated with forensic investigation and breach notification increase if you haven't planned for a data breach in advance.

Cybersecurity of Law Firms: At Risk of NSA Intrusion

- The National Security Agency is prohibited from targeting Americans, including U.S. law firms, for surveillance without warrants. But the NSA can intercept such communications if they involve foreign intelligence targets.
- Growing concern that the NSA will intercept or otherwise obtain communications between U.S. law firms and their foreign clients: Snowden revelation.
- In February 2014, then ABA President James R. Silken at wrote a letter to the NSA to express concerns regarding the NSA's access to and use of privileged and confidential communications between attorneys and overseas clients.

What Else is the ABA Doing?

- ABA passed Report and Resolution 118 in August 2013 condemning the unauthorized, illegal governmental, organizational, and individual intrusions into computer systems and networks used by lawyers and law firms that risk undermining the attorney-client privilege and compromising client confidences; and urging federal, state, and other governmental bodies to develop legal mechanisms and policies to deter, prevent, and punish illegal intrusions.

What Else is the ABA Doing? (cont'd) - American Bar Association Report and Resolution 109

- ABA Resolution 109: To encourage private and public sector organizations, including law firms, to implement cybersecurity programs to tackle mounting data security threats. The program must comply with "applicable ethical and legal obligations and [be] tailored to the nature and scope of the organization and the data and systems to be protected."
- Specific application to law firms: Law firms "are facing unprecedented challenges from the widespread use of electronic records and mobile devices as well as increased attention by hackers enticed by the sensitive client data they hold."

ABA Resolution 109 (cont'd)

- The cybersecurity program should include regular assessments of the threats, vulnerabilities, and risks to a law firm's data, networks, and operating platforms; and should implement appropriate security controls to address the identified threats, vulnerabilities, and risks, consistent with the types of data and systems to be protected and the nature and scope of the organization.
- Develop and test a response plan to possible cyber attacks.
- Engage in cooperative relationships to address the problem of cyber attacks by sharing information about cyber threats.
  - 82% of companies with high-performing security practices collaborate with others to deepen their knowledge of security and threat trends. *PwC, CSO magazine, CIO magazine, The Global State of Information Security® Survey 2014, September 2013.*

ABA Resolution 109 (cont'd)

- A cybersecurity program includes at least the following activities: Governance by boards of directors and senior executives; development of security strategies, policies, and procedures; creation of inventories of digital assets and data; conducting risk assessments; continuous monitoring and log analysis; performance of annual audits; delivery of training; and preparation of an incident response plan and business continuity/disaster recovery plan.

ABA Model Rules of Professional Conduct

- Lawyers and law firms have a responsibility to protect confidential and privileged client information from unauthorized access and disclosure, whether malicious or unintentional, including to protect the information from hackers.
- Adopted in Oregon
- Amended in 2012 “to provide guidance regarding lawyers’ use of technology and confidentiality”

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."

Maintaining Competence

Comment [6] to Rule 1.1

"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."

*(**Underlined language** added by 2012 amendments)*

Rule 1.6
Confidentiality of Information

"(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

* * * *

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

Acting Competently to Preserve Confidentiality

Comment [16] to Rule 1.6

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. ***

Added by the 2012 amendments.

Inadvertent Disclosure ≠ Violation

Comment [16] to Rule 1.6 (continued)

" * * * 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."

(emphasis added)

What Are "Reasonable Efforts?"

Comment [16] to Rule 1.6 (continued)

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).

Added by the 2012 amendments

Return to NSA Discussion

- Ethical implications of potential surveillance of client communications: You must use reasonable efforts to protect the information against disclosure or unauthorized access.
  - Encrypt email.
    - Recent bar opinions take the position that attorneys have a reasonable expectation of privacy in unencrypted e-mail.
    - Encryption may be required in some situations: "[I]n circumstances in which a lawyer is on notice for a specific reason that a particular email transmission is at heightened risk of interception…the lawyer must select a more secure means of communication than unencrypted Internet email." NYSSA Comm. On Prof'l Ethics, Op. 709 (1998).

Return to NSA Discussion (cont'd)

- In person meetings. Sometimes, email may not be permitted at all.
  - "Because of the FAA's expansion of the government's surveillance power, [the attorney plaintiffs] do not have a reasonable expectation of privacy in their international electronic communications in connection with the representation of their clients. The rules of professional conduct governing these lawyers therefore compel them to take appropriate precautions to protect against government access to those communications. The precautions that they have taken in their factual circumstances, including international travel, are both reasonable and required." *Brief of the New York State Bar Association as Amicus Curia, Clapper v. Amnesty Int'l USA*, 2011 U.S. Briefs 1025 (U.S. 2012).

Directions from Client

Comment [16] to Rule 1.6 (continued)

"A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. * * * "

Added by the 2012 amendments

Compliance with Laws

Comment [16] to Rule 1.6 (continued)

"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. * * * "

Added by the 2012 amendments

Other Laws That May Apply

There is a complex network of federal, state, and international privacy and data protection laws that may apply to lawyers, law firms, and their clients. Examples:

- FTC Act
- Online privacy (COPPA, targeted behavior-based marketing, website privacy policies)
- E-mail privacy & CAN-SPAM
- Industry-specific, if applicable (e.g., HIPAA, financial privacy)
- Telephone privacy & telephone marketing
- Employee privacy (social media, background checks, employer monitoring of employee e-mails, etc.)
- State breach notification laws
- Industry self-regulation

What Should You Be Doing?

- Physical security
- Procedural security
- Technical security
- Specific contexts & technologies

Physical Security

- Lock drawers
- Clean desk
- Shred
- Log out and lock
- Do not let mobile data storage, including mobile devices, out of your control

Procedural & Administrative Security

- Security awareness training for lawyers & staff
- Use good passwords
- Use business e-mail (and not personal e-mail account) for client-related communications
- Be careful with WiFi
- Incident response plans and policies
- Click with caution
- Vendor due diligence and contractual arrangements

Technical Security

- Encrypt e-mail when it is warranted
- Cleanse metadata
- Encrypt flash drives, and use only known clean devices
- Beware of wi-fi
- Firewalls
- Anti-malware software
- Intrusion detection systems

Specific Contexts & Technologies

- E-mail
- Metadata
- Vendors
- Cloud storage
- Free e-mail services
- Mobile computing & storage devices
- Waiver of privilege using employer device or e-mail account

Metadata

Metadata

- What is metadata?
- Examples:
  - Date stamps, version & editing history, & author information on documents may establish “who knew what when”
  - Redlining or comments in an agreement that suggest how much more or less opposing party is willing to pay

Metadata
Your Ethical Obligations

"Lawyers have a duty…to use reasonable care when transmitting documents by e-mail to prevent the disclosure of metadata containing client confidences or secrets."

NYSBA Eth. Op. 782 (Dec. 8, 2004). *See also, e.g.*, ABA Formal Op. 06-442 (2006); MN Eth. Op. 22, 2010 WL 7378367 (2010)

Metadata
Your Ethical Obligations

"Competence requires that lawyers who use electronic documents understand that metadata is created in the generation of electronic documents, that transmission of electronic documents will include transmission of metadata, that recipients of the documents can access metadata, and that actions can be taken to prevent or minimize the transmission of metadata."

MN Eth. Op. 22, 2010 WL 7378367 (2010)

Metadata
Best Practices

- If sending a document to opposing counsel or another party, or sending a document to your client that may be forwarded to opposing counsel or another party, clean the metadata first
- Be cautious when forwarding e-mails with attachments from smartphones and iPads.

What Can You Do When You Receive Metadata?

You receive a document from opposing counsel that contains balloon comments, tracked changes, or other metadata. The document likely contains other metadata that may be useful to you that you can easily discover if you just look for it. You do not know whether opposing counsel intended to share this metadata with you.

- Can you use the metadata?
- Can you search the document for metadata?

What Can You Do When You Receive Metadata? (cont.)

In 2012, the ABA revised Rule 4.4 to clarify that an attorney should promptly notify the sender if hey receive electronically stored information that was inadvertently sent.

Rule 4.4 Respect for Rights of Third Persons

* * *

(b) A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender.

What Can You Do When You Receive Metadata? (cont.)

Comment to Rule 4.4

For purposes of this rule, "document or electronically stored information" includes…embedded data (commonly referred to as "metadata")…

What Can You Do When You Receive Metadata? (cont.)

Comment to Rule 4.4

If a lawyer knows or reasonably should know that such a document or electronically stored information was sent inadvertently, then this Rule requires he lawyer to promptly notify the sender in order to permit that person to take protective measures. Whether the lawyer is required to take additional steps, such as returning the document or electronically stored information ~~original document~~, is a matter of law beyond the scope of these Rules, as is the question of whether the privileged status of a document or electronically stored information has been waived.

What Can You Do When You Receive Metadata? (cont.)

Comment to Rule 4.4

Some lawyers may choose to return a document or **delete** electronically stored information unread…Where a lawyer is not required by applicable law to do so, the decision to voluntarily return such a document or **delete** electronically stored information is a matter of professional judgment ordinarily reserved to the lawyer.

What Can You Do When You Receive Metadata? (cont.)

Several states (e.g., Alabama, Arizona, Florida, Maine, New York, and North Carolina) have taken the position that a lawyer who receives an electronic communication from another party or the party's lawyer may not search for and use confidential information embedded in the metadata of the communication without the consent of the other party or lawyer.

What Can You Do When You Receive Metadata? (cont.)

The ABA and the District of Columbia Bar Association have taken the position that:

- If the receiving lawyer did not obtain the electronic documents in a manner that was criminal, fraudulent, deceitful, or otherwise improper, the lawyer may use the information.
- If the receiving lawyer knows or reasonably should know that opposing counsel's sending, producing or otherwise making available an electronic document that contains metadata was "inadvertent" within the meaning of Rule 4.4(b), the sole obligation is for the attorney to provide notice to the sender of the receipt of inadvertently sent information pursuant to rule 4.4(b).

ABA Formal Op. 06-442 (2006) & D.C. Ethics Op. 341 (September 2007).

Vendors, Cloud Storage, & Free E-mail Providers

Popular Cloud Storage & Free E-mail Providers

- Dropbox
- Evernote
- Google Drive
- iCloud
- Gmail
- Yahoo mail
- Hotmail

Your Ethical Obligations When Engaging a Vendor

Rule 5.3 Responsibilities Regarding Nonlawyer Assistance

- Nonlawyer assistance includes both staff (e.g., your secretary) and vendors
- When retaining a vendor (*e.g.*, an e-discovery vendor, deal room provider, cloud storage provider), the lawyer or law firm should confirm that the vendor's privacy and data security practices and policies are consistent with the lawyer's obligation to maintain client confidentiality.

Ore. Formal Op. 2011-188

Lawyer may store client materials on a third-party server.…To do so, the lawyer must take reasonable steps to ensure that the storage company will reliably secure client data and keep information confidential. Under certain circumstances, this may be satisfied though a third-party vendor's compliance with industry standards... This may include, among other things, **ensuring the service agreement requires the vendor to preserve the confidentiality and security of the materials**. It may also require that **vendor notify Lawyer of any nonauthorized third-party access** to the materials. Lawyer should also **investigate how the vendor backs up and stores its data and metadata** to ensure compliance with the Lawyer's duties.

Vendor Engagement Best Practices

- Contractually require vendor to
  - Maintain confidentiality of your data
  - Notify you immediately if they receive a court order, subpoena, or government request to produce your data
  - Notify you immediately if there is a breach, and perhaps even indemnify you

Vendor Engagement Best Practices (cont.)

- Confirm that:
  - Vendor's employees have limited access to client data on a need-to-know basis
  - Vendor requires its contractors, employees, and consultants to sign NDAs that are sufficiently protective
  - Vendor uses reasonable IT, physical, and administrative safeguards to protect confidentiality
  - Vendor stores confidential data only in jurisdictions with adequate privacy laws

Vendor Engagement Best Practices (cont.)

Are you or your law firm applying these best practices?

Application of these best practices is especially challenging when using free, publicly available email and cloud storage services.

Use of Free E-mail Providers

Attorney would breach obligation to preserve client confidentiality "if the service provider reserved the right to disclose e-mails or the substance of the communications to third parties without the sender's permission." NYSBA Comm. On Prof'l Ethics, Op. 820 (2008)

Dropbox privacy policy

Dropbox privacy policy:

"We may disclose to parties if we determine that such disclosure is reasonably necessary to

(a) comply with the law;
(b) protect any person from death or serious bodily injury;
(c) prevent fraud or abuse of Dropbox or its users; or
(d) to protect Dropbox's property rights."

There is no obligation for Dropbox to notify you if they provide your content in response to a subpoena or government request , or if your information is breached.

Google privacy policy

"We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:

- meet any applicable law, regulation, legal process or enforceable governmental request.
- enforce applicable Terms of Service, including investigation of potential violations.
- detect, prevent, or otherwise address fraud, security or technical issues.
- protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law."

Evernote Privacy Policy

"We only disclose your information – and then only to the minimum information necessary - when:

* * *

- We believe it is necessary to investigate potential violations of our Terms of Service, to enforce those Terms of Service, or where we believe it is necessary to investigate, prevent or take action regarding illegal activities, suspected fraud or potential threats against persons, property or the systems on which we operate the Service.
- We determine that the access, preservation or disclosure of information is required or permitted by law to protect the rights, property or personal safety of Evernote and users of the Service, or is required to comply with applicable laws, including compliance with warrants, court orders or other legal process.

Apple Privacy Policy (applies to iCloud)

- It may be necessary − by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence − for Apple to disclose your personal information. We may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate.
- We may also disclose information about you if we determine that disclosure is reasonably necessary to enforce our terms and conditions or protect our operations or users. Additionally, in the event of a reorganization, merger, or sale we may transfer any and all personal information we collect to the relevant third party.

Apple Privacy Policy – Governmental Requests

The most common [governmental] requests we receive for information come from law enforcement in the form of either a Device Request or an Account Request. Our legal team carefully reviews each request, ensuring it is accompanied by valid legal process. All content requests require a search warrant. If we are legally compelled to divulge any information and it is not counterproductive to the facts of the case, we provide notice to the customer when allowed and deliver the narrowest set of information possible in response. National security-related requests are not considered Device Requests or Account Requests and are reported in a separate category altogether.

Risks of Using Free E-mail & Cloud Storage

It can be challenging to apply best practices to free, publicly available services such as Gmail, Google docs, or Dropbox.

- You don't know where they store their data
- They are not obligated notify you if they receive a subpoena, court order, or governmental request to produce your data
- In many cases, they will not be require to notify you if your data is breached
- They can change their terms of use and privacy policies at any time, without notice or your consent
- You do not have the ability to negotiate different terms of service or investigate their data security practices

If the Client Requests it

If a client asks you to use one of these services, however:

- Read the applicable T&C and privacy policy
- Advise your clients about the risks of using the service and obtain your client's informed consent before using the service

Under Rule 1.6, a client can give informed consent to forgo security measures that would otherwise be required by Rule 1.6.

Additional Recommendations

- Encrypt sensitive information stored in the cloud (but note that even encryption keys can be cracked – the NSA has already cracked most standard encryption technology)
- Consider adjusting your mobile device settings so that they do not automatically back up e-mails and other confidential information to the cloud
- Avoid sending confidential information to your personal e-mail account

Mobile Devices

Types of Mobile Devices

- Mobile computing:
  - Laptop computers
  - Smartphones
  - iPads and other tablets
- Mobile storage
  - Flash drives
  - External hard drives
  - CDs & DVDs

Mobile Devices
Best Practices

- Password protect with automatic log-off after a few minutes of inactivity
- Use remote wiping technology
- Encrypt all client information stored on mobile storage devices. For some types of information (e.g., social security number), this is required by law.

Mobile Devices
Best Practices (cont.)

- Keep track of stored passwords
- If you lose a mobile computing or storage device:
  - Report it to your IT department **immediately** (or follow whatever reporting requirements are set forth in your incident response plan)
  - Change your network password **immediately**
  - Change all stored passwords **immediately**

Use of Employer Provided Equipment or Systems: Avoiding Inadvertent Waiver of Privilege

Hypothetical

- Joe is an employee of XYZ Corporation
- Joe founds ABC Startup as a side project and engages you as ABC Startup's counsel
- 1 year later, Joe quits his job at XYZ to devote himself to ABC Startup full time
- XYZ sues ABC Startup and Joe, alleging misappropriation of trade secrets Joe learned while he was an employee

Hypothetical (cont.)

- Was privilege waived with respect to Joe's communications with counsel if they were sent:
  - From Joe's XYZ email account Joe@xyz.com?
  - From Joe's personal email account but using a computer or smartphone provided by XYZ?
  - From Joe's personal device that was subject to the employer's BYOD policy?

Employer Provided Equipment or Systems (cont.)

If employer policy indicates that employees have no right to privacy on anything contained in employer-owned equipment, then the employee waives the attorney-client privilege with respect to e-mail or other content stored on or transmitted from the employer-provided computer or mobile device.

See, e.g., *Dombrowski v. Governor Mifflin School Dist.*, 2012 WL 2501017 (E.D. Pa. 2012); *Holmes v. Petrovich Development Co.*, 191 Cal. App. 4th 1047 (3d Dist 2011); *Kaufman v. SunGard Inv. System*, 2006 WL 1307882 (D.N.J. 2006) (e-mail messages were deleted from laptop, but employer hired technician to recover them).

Employer Provided Equipment or Systems (cont.)

- There are also cases holding that an employee did not waive attorney-client privilege by communicating with attorney on private e-mail account, accessed on an employer-provided computer.
  - Employer policy allowed "occasional personal use" of employer provided computer. *Stengart v. Loving Care Agency, Inc.*, 408 N.J. Super. 54, 973 A.2d 390 (App. Div. 2009), aff'd 201 N.J. 300, 990 A.2d 650 (2010).
  - The company's policy concerning technology use did not expressly notify employees that e-mail sent via a private, password protected e-mail account, accessed through the Internet, was subject to review by the company, nor were employees advised that screen shots of their private e-mail would be retained on the computer's hard drive even after the e-mail messages were deleted. *National Economic Research Associates, Inc. v. Evans*, 21 Mass. L. Rptr. 337 (Mass. Super. Ct. 2006).

Employer Provided Equipment or Systems

- Advise clients to avoid using a workplace device or system to store or transmit confidential information (unless the employer is your client)
- Employer policies matter

Additional Thoughts

- Technology is always changing. So are the risks, available safeguards, & best practices
- Continue to educate yourself
- If your law office doesn't already have a security policy, consider adopting one
- If your law office has a security policy, familiarize yourself with it