PROGRAM MATERIALS
Program #31100
June 10, 2021

New Developments in Law Firms' Obligations to Protect Against Data Breaches

- Barry Temkin, Esq. – Mound Cotton Wollan & Greengrass LLP
- Jennifer Goldsmith – Ironshore Insurance
- David Standish – Ironshore Insurance

Celesq® AttorneysEd Center
www.celesq.com

5255 North Federal Highway, Suite 100, Boca Raton, FL 33487
Phone 561-241-1919

New ABA Guidance on the Ethics of Working Remotely

Jennifer Goldsmith, Esq. IronPro Professional Liability
David Standish, Esq. IronPro Professional LIability
Barry Temkin, Mound Cotton Wollan & Greengrass, LLP

* Whole lot of hacking going on

* INTRODUCTION

Rising Tide of Law Firm Data Breaches

* 80% of the largest law firms in the U.S. have experienced data breaches recently.
* Some data breaches attributable to employee negligence, e.g. lost laptop, cell phone or other electronic device left in public
* Information stored in the cloud, or transmitted via unsecured servers may be vulnerable to unauthorized intrusions.

Cybersecurity for Law Firms: Professional Liability and Ethical Considerations

* Organized bar: recent ethics opinions which presage a trend toward regulatory vigilance by lawyers on encryption and cybersecurity
* Hackers are coming after law firms
* Regulators may be next

Recent Law Firm Data Breaches

* Mossack Fonseca hacked and data published
* Panamanian lawyers set up off-shore entities to evade their respective countries' income taxes on eye-popping wealth.


THE
LAUNDROMAT

* 2016,hack of Cravath, Swaine & Moore and Weil, Gotshal & Manges by insider trading ring.
* SEC enforcement action against three Chinese nationals for insider trading based on hacked information stolen from M & A departments at firms
* Intruders installed malware on the firms' networks, and accessed gigabytes of emails from remote internet locations.
* Traders reaped profits of $1 million, moving the markets by trading in up to 25% of all trades in the target stocks.

* Ethical Guidance from Organized Bar

* ABA
* Cal. State Bar Assoc.
* NYCLA

ABA MRPC 1.6

* (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).

* https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/

Duty of Confidentiality MRPC 1.6

Rule of Professional Conduct 1.6 (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."

* https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/

Comment [18] to MRPC 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. . . 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).

* Lawyers must also supervise and are responsible for staff

ABA MRPC 1.6

* RPC 1.6 is broader than the attorney-client privilege, which is an evidentiary principle.
* Applies to "information relating to the representation of a client"
* includes information that the client has requested to keep confidential, or which might be embarrassing to the client, regardless of whether it emanated from an attorney-client communication.
* E.g., investigative materials or witness statements
* Public documents?

Duty of Competence RPC 1.1

* ABA Model Rule 1.1: “A lawyer shall provide competent representation to a client.”
* New York comment on RPC 1.1: “To maintain the requisite knowledge and skill, a lawyer should … keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information.”

The Organized Bar and Cybersecurity

* NYCLA ethics opinion 749: lawyers should keep up with technological developments, “cannot knowingly reveal client confidential information, and must exercise reasonable care to ensure that the lawyers, employees, associates and others whose services are utilized by the lawyer not disclose or use client confidential information.”

* NYCLA: prevent unauthorized data breaches:

> The risks associated with transmission of client confidential information electronically include disclosure through hacking or technological inadvertence. A lawyer's duty of technological competence may include having the requisite technological knowledge to reduce the risk of disclosure of client information through hacking or errors in technology where the practice requires the use of technology to competently represent the client.

* Lawyers should be mindful of their ethical obligations to maintain client confidential data, whether in the cloud, in an email or in a portable device.

* NYCLA Eth. Op. 749

The Organized Bar and Cybersecurity

* ABA Ethics Opinion 477R: “Securing Communication of Protected Client Information.”
* ABA :“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.”

*ABA Op. # 477 R

* ABA: “lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters,” based upon the sensitivity of the information, the risk of cyber-intrusion and the needs of the client.
* lawyers should understand clients’ needs for cyber-security, vet outside vendors and conspicuously to label e-mail communications as privileged and confidential.

*ABA Eth. Op. 498 (2021)

* March 10, 2021
* ABA Standing Committee on Ethics and Professional Responsibility
* ABA Formal Opinion 498, which contains guidance on ethical issues specific to working remotely

ABA Formal Opinion 498:

* lawyers' ethical duties of competence, confidentiality and supervision,
* Rules 1.1, 1.6, 5.1 and 5.3 of the ABA Model Rules of Professional Responsibility;
* Relies on NYCLA Opinion 754-2020 and California State Bar Formal Opinion No. 2020-203
* The concept of professional competence increasingly encompasses technological know-how.

Challenges for lawyers working remotely

* Other household members may pass through or even share the same room.
* Portions of client meetings or depositions might be audible to other household members in different rooms.
* Parents may need to leave a screen unattended in order to assist a child with school, homework, or to prepare a meal, thereby potentially exposing confidential information.

Securing devices which contain client material

- Other family members may have access to lawyers' devices, which could be left unattended in the home.
- devices should be fully encrypted and subject to dual factor authentication

ABA Eth.Op. 498 Recommendations

1. Avoiding unsecured Wi-Fi systems when accessing confidential information.

2. Utilizing VPNs that encrypt information and shield online activity from third-parties.

3. Use multifactor authentication.

4. Ensuring that computer systems are up to date, with appropriate firewalls and anti-malware software.

5. Backing-up data stored remotely.

6. Portable devices remotely scrubbable.

7. Requiring strong passwords to protect data access in devices.

8. Written work-from-home protocol that specifies procedures to safeguard confidential information.

9. Train employees on security protocols, data privacy and confidentiality policies.

*ABA 498 recommendations

* Avoid using unsecured public Wi-Fi networks at coffee shops, airports and other public places

ABA: Limitations on Zoom and other video software

* Lawyers conducting meetings, depositions or court proceedings via video "should review the terms of service (and any updates to those terms) to ensure that using the virtual meeting or videoconferencing platform is consistent with the lawyer's ethical obligations."
* Is video secure?
* Is meeting recorded?
* Is meeting private?

ABA: Read the fine print

* Lawyers should review the terms of service applicable to hardware devices and software systems “to assess whether confidentiality is protected”

* Do lawyers do this?
* If not, who does?

ABA Confidentiality Recommendations

* Use virtual private networks, or VPNs.
* Unplug/ disable the listening capacity of Amazon Echo, Alexa, Apple Homepod to prevent electronic eavesdropping.

* Ensure that portable devices can be remotely wiped, so that confidential client information can be erased in the event that a laptop or smartphone is stolen, or inadvertently misplaced.

* ABA: remote scrubbing

Analysis and Implications

ABA Ethics Opinion 498:

* Links duty to maintain client confidences with the overall ethical obligation of competence under Rule 1.1, thereby raising the stakes for lawyers who might have previously lagged in technology.
* Part of a larger movement by which lawyers are being exhorted to develop competence in 21st century technology

*ABA borrows from CA

* ABA borrows from CA State Bar 2020-203 https://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/Formal-Opinion-No-2020-203-Data-Breaches.pdf

* CA State Bar: law firms should secure electronic data storage systems from the risk of unauthorized access and provide for remote lockdown and scrubbing if device is lost or compromised.
* In the event of a breach, “lawyers have an obligation to conduct a reasonable inquiry to determine the extent and consequences of the breach and to notify any client whose interests have a reasonable possibility of being negatively impacted by the breach."

Opinion No. 2020-203, California State Bar

* Duty of competence includes knowledge about cybersecurity technology.
* Managing partners should understand tools and procedures for protecting client confidential information.
* Implement internal policies and procedures to protect against inadvertent disclosure of client confidential information;

* Have staff training to protect against phishing attacks and other cyber intrusions.
* Law firms should be able to lock down or scrub lost devices remotely
* Do not use unprotected public networks; use virtual private networks (VPN) or encrypted networks.

*CA State Bar 2020-203

Other Bar trends

* Florida: all Florida lawyers need three CLE credit hours on technology per 3 years, including use of encryption and other technology to preserve client confidential data.

Analysis and Implications

* Can ABA 498 prompt LPL claims?

Can lawyers be sued for violating RPC?

* Ethics rules proscribe offensive use in civil suits
* But some courts admit them as some evidence of standard of practice
* ABA ties cyber-security to competence under 1.1
* Is negligence to maintain security incompetence?

*What to do if your firm is breached?

*The morning after

When to notify clients of Data Breaches? ABA Eth. Op. 18-483

* Law firms should have data breach plans in place to remediate cyber intrusions
* "An obligation exists for a lawyer to communicate with current clients about a data breach."
* While a cyber intrusion which does not gain access to client confidential information needn't be disclosed, "disclosure will be required if material client information was actually or reasonably suspected to have been accessed, disclosed or lost in a breach."

*ABA: When to Notify Clients?

* ABA Opinion 483 defines a data breach as cyber episode in which "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."

* [N]o 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*.

* ABA Op. 483: When to disclose

NYSBA 842: Breach of online storage provider

* NYSBA: "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, notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated."
* N.Y. State Bar Ass'n Eth. Op. 842 (2010).

* A lawyer has a duty to inform a client of a material data breach in a timely manner. . . . A data breach is "material" if it involves the unauthorized access, destruction, corruption, or ransoming of client ESI protected by RPC 1.6 or other applicable law, or materially impairs the lawyer's ability to perform the legal services for which the lawyer has been hired."

* MI Op. 381

* "The duty to inform includes the extent of the breach and the efforts made and to be made by the lawyer to limit the breach."

* MI Eth. Op. 381

* What information to disclose to client?

New Developments in Law Firms' Obligations to Protect Against Data Breaches

* California State Bar Ethics Op. 2020-203:
* In the event of a breach, "lawyers have an obligation to conduct a reasonable inquiry to determine the extent and consequences of the breach and to notify any client whose interests have a reasonable possibility of being negatively impacted by the breach."

Four Hypotheticals When to notify clients

* **Hypothetical A**: Lawyer A's laptop was stolen, but he did not use it to store confidential information. Pilfered laptop was used for remote access to the lawyer's desktop, and the firm had software that allowed it to be wiped clean remotely.
* Promptly after the theft, Lawyer A notified his firm's information technology department, which remotely cleansed the device of confidential information.

* Notify clients of laptop theft?

* Hypo A

* Remote scrubbing was held by the state bar to be a prudent and reasonable procedure which did not require client notification, as no confidential information was accessed or penetrated.

* Hypo A: Needn't notify client

*Hypo B

* **Hypothetical B**: Lawyer B left a smart phone in a bag in a restaurant, which was retrieved undisturbed and in the same pocket of the bag the next morning after the lawyer realized that the phone was missing. The phone had a four digit password and no biometric code, and the restaurant assured the lawyer that the phone had been placed in a secured cabinet overnight.

* Should client be notified in Hypo B?

* Hypo B

* While it would have been preferable to have a biometric code on the smart phone and a more complex password, there was no evidence that the phone had been disturbed or that client confidential information had been accessed. Accordingly, Lawyer B has no obligation to notify firm clients.

Hypo B (bag left in restaurant): No notification

CA State Bar Hypo C

* **Hypothetical C**: The firm's receptionist inadvertently clicked on an email which subjected the firm to a ransomware attack by an intruder. The firm paid the ransomware, and an investigation conducted by an outside forensic technology firm found no evidence of unauthorized access to confidential information.

* Law firm C was not obligated to give notice to its clients, as there was no evidence of unauthorized access to its confidential information. However, law firms should train their employees to identify and avoid phishing attacks.

* CA Hypo C: No notice required

* Query: How long did outside forensic exam take?
* How soon should clients be notified?

* CA Hypo C

* Hypothetical D: Lawyer D used an unsecure public Wi-Fi network to access confidential client information while on vacation. This confidential client data was accessed by an intruder, and was sensitive as it contained information about pending patent applications.

* Hypo D CA State Bar

* Given the sensitive nature of this data, Lawyer D's law firm should give notice to the client whose confidential information was accessed.

* CA Hypo D: Yes, notify clients

* Should law firm notify all clients in Hypo D or just the clients whose data was compromised?

Statutory Concerns

* CA Business and Professions Code 6068(e): lawyers should "maintain inviolate the confidence, and at any peril to himself or herself to preserve the secrets, of his or client."
* lawyers should keep clients reasonably informed of "significant developments in matters" for which the attorneys are providing legal services.
* ABA MRPC 1.4 similarly requires client updates

CA Notification Statutes

* California Civil Code Section 1798.82 imposes confidentiality and notification obligations upon any "person or business that conducts business in California."
* CCC: any company which does business in California and owns or licenses confidential client data must "disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California" when encrypted personal information is believed to be "acquired by an unauthorized person."

Statutory Basis

* CA Civil Code: notification required when encrypted personal information is acquired by an unauthorized person whom the business owner "has a reasonable belief that the encryption key or security credential could render that personal information readable or usable." Cal. Civil Code 1798.82(a).
* Where encrypted data is accessed by an unauthorized user, client notification must be made in circumstances in which there is a reasonable possibility of a breach of encryption. (Broader than CA State Bar hypos)

When to notify clients? CCC

* California Civil Code: disclosure "in the most expedient time possible and without unreasonable delay," consistent with any ongoing law enforcement investigation.

* Other consumer privacy laws: Maryland, Hawaii, New York and Massachusetts.

Other Cyber Regulation

* Regulators in health care, insurance and financial services, require specific cybersecurity protections. These regulations will affect lawyers as service providers to companies in regulated industries.
* Financial firms must implement cybersecurity measures under Gramm-Leach-Bliley Act of 1999, which "sets forth high-level cybersecurity directives, but mainly delegates rule-making authority to various government regulators to promulgate information security rules applicable to entities under their respective jurisdictions."
* Information security regulations: the Office of the Comptroller of the Currency, the Federal Reserve System, the FDIC, and other agencies.

Regulatory notice

- Broker-dealers, investment companies and RIAs: SEC Regulation S-P requires regulated entities to "adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information."
- The National Institute of Standards and Technology: non-binding Framework for Improving Critical Infrastructure Cybersecurity, a voluntary risk-based cybersecurity framework.

Regulatory Enforcement

* In 2016, the SEC sued Morgan Stanley Smith Barney because 700,000 customer accounts containing PII were accessed by a financial advisor, who stored data on his own personal website.
* The financial advisor sustained a data breach whereupon he was terminated by the firm.
* Morgan Stanley contacted the FBI within two weeks of the breach; the SEC extracted a $1 million fine.

Regulatory Enforcement

* broker dealer Sterne Agee agreed to pay a fine of $225,000 for its failure to encrypt confidential data on a laptop that was left in a restaurant, thereby exposing the personal identifying information of 350,000 customers. This conduct was found by FINRA to violate regulation SP and FINRA Rules 3010 and 2010.

NY DFS Cybersecurity Regulations effective 2017

* apply to insurance companies, insurance agents, banks, charitable foundations, holding companies and premium finance agencies.
* encryption of all non-public information held or transmitted by the covered entity,
* must appoint a chief information security officer (“CISO”), who must report directly to the board of directors and issue an annual report, setting forth an assessment of the company’s cybersecurity compliance and any identifiable risks for potential breaches.

NY DFS Cyber Regs

- §500.11 requires each covered entity to "implement written policies and procedures designed to ensure the security of information systems and non-public information that are accessible to, or held by third-parties doing business with the covered entity."
- Covered entities, including insurance companies, who provide access to PII to third-party vendors must certify that the information security systems of vendors are secure

NY DFS Regs, cont'd

* Vendors who do business with regulated financial service companies should comply with the cybersecurity standards of their represented clients.

New Cybersecurity Regulations

* Massachusetts “Standards for the Protection of Personal Information of Residents of the Commonwealth,” requires companies to encrypt personal data and to retain and store digital and physical records and implement network security controls, such as firewalls, to protect sensitive consumer information.
* MA regs reach across all industries: “Every person that owns or licenses personal information about a resident of the Commonwealth,”
* requires “a comprehensive information security program that it is written in one or more readily accessible parts,” and contains safeguards to protect and encrypt confidential consumer information.
* MA requires secure user authentication protocols, control of data security passwords, restricted access to active users, unique and complex passwords and encryption of all transmitted records and files.

* Ethical Issues for Remotely Working Lawyers: Unauthorized Practice of Law and RPC 5.5

Working Remotely

The butt in the chair theory of law practice

*Restaino: FL S. Ct. 5/20/21

*NJ Lawyer resident in FL may work remotely

*Federal IP practice on behalf of NJ clients

*No office in FL

*https://www.floridasupremecourt.org/content/download/743446/opinion/sc20-1220.pdf

Retaino FL UPL Opinion 2021 (Lawyer's inquiry)

* "I am recently retired from my position as Chief IP Counsel for a major US corporation. My prior position was located in New Jersey. Contemporaneously with my retirement, I moved from New Jersey to Florida. Recently, I have accepted an offer of employment as an attorney with [a NJ law firm]. . . My professional office will be located at Tong, Rea's business address in New Jersey, although I will do the majority of my work from my Florida home using a personal computer securely connected to the Tong, Rea computer network."
* https://www-media.floridabar.org/uploads/2019/12/Restaino_Request.pdf

Restaino works remotely in FL: UPL opinion

* Restaino: “we’ve tried to set up and utilize the technology in a fashion that essentially places me virtually in New Jersey. But for the fact that I’m physically sitting in a chair in a bedroom in Florida, every other aspect of what I do is no different than where I’m physically sitting in a chair in Eatontown, New Jersey….”
* https://www.floridasupremecourt.org/content/download/743446/opinion/sc20-1220.pdf

*Restaino Opinion:

* “the Petitioner who simply establishes a residence in Florida and continues to provide legal work to out-of state clients from his private Florida residence under the circumstances described in this request does not establish a regular presence in Florida for the practice of law.”
* https://www.floridasupremecourt.org/content/download/743446/opinion/sc20-1220.pdf

Important Elements

* No FL office
* No solicitation of FL Clients
* No practice of FL law
* All federal IP law

D.C. Covid Opinion 24-20

* Non-DC lawyer may practice from home in D.C.
* if attorney (1) is practicing from home due to the COVID-19 pandemic; (2) maintains a law office in a jurisdiction where the attorney is admitted to practice; (3) avoids using a D C address in any business document or otherwise holding out as authorized to practice in DC, and (4) does not meet with clients or third parties in person in DC. https://www.dccourts.gov/sites/default/files/matters-docs/CUPL-Opinion-24-20.pdf

NY Judiciary Law 470:

* Non-resident NY lawyers must have office in NY
* "A person, regularly admitted to practice as an attorney and counsellor, in the courts of record of this state, whose office for the transaction of law business is within the state, may practice as such attorney or counsellor, although he resides in an adjoining state."

* Upheld in Schoenfeld v. New York, 25 N.Y.3d 22 (2015): Nonresident NY lawyers must have physical offices in NY

* NYC Bar recommends repealing Jud. Law 470
* https://s3.amazonaws.com/documents.nycbar.org/files/20200732-JudiciaryLaw470Repeal.pdf

* It poses hurdles for out of state residents admitted in NY

RPC 5.5

- Can't maintain regular and systematic presence here
- Can act in furtherance of ADR
- Can act in connection with licensed attorney
- Can act if expect to be admitted pro hac
- Can act if arises from lawyer's licensed practice

ABA Ethics Op. 495 (Dec. 2020)

* Lawyers may work remotely from states where not admitted:
* "Lawyers may ethically engage in practicing law as authorized by their licensing jurisdiction(s) while being physically present in a jurisdiction in which they are not admitted under specific circumstances enumerated in this opinion."
* https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba-formal-opinion-495.pdf

ABA Ethics Op. 495

* the purpose of rule 5.5 (barring UPL) was “to protect the public from unlicensed and unqualified practitioners of law.”
* “That purpose is not served by prohibiting a lawyer from practicing the law of a jurisdiction in which the lawyer is licensed, for clients with matters in that jurisdiction, if the lawyer is for all intents and purposes invisible as a lawyer to a local jurisdiction where the lawyer is physically located, but not licensed,” Formal Opinion 495 states.

Don’ts

- Don’t hold yourself out as licensed where you aren’t
- Don’t solicit clients
- Don’t advertise
- Don’t practice law of (unlicensed) home state
- Don’t violate local UPL rules

Conclusion

* Lawyers working remotely should exercise reasonable diligence to secure the confidentiality of confidential client information
* law firms should ensure that their portable electronic devices either do not contain client information, or can be remotely deactivated and scrubbed.
* Breached Law firms should consider the four hypothetical situations outlined by the California State Bar in determining when to notify clients, and should resolve reasonable doubts in favor of prompt client notification.
* different states may vary in their interpretation of lawyers' professional responsibilities with respect to data breaches.

* Jennifer Goldsmith
* Barry Temkin

* Questions?