

CONFIDENTIALITY, CYBERSECURITY, AND AI ETHICS


Spywares
Worms
Virus
Bugs
Rootkits
Troja
EVERYONE TAKE COVER . . .
cybercodi

BUY A HELMET

“I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.”

Robert Muller – FBI Director, 2012



LAWYERS ARE TARGETS

Obtain, store, and use highly sensitive information about clients

Information stored is likely to be of interest to a hacker and less voluminous than other sources

TOP CYBER-SECURITY THREATS FACED BY LAW FIRMS

- Ransomware Attack (aka Phishing/Social Engineering)
- Social Media
- Misdirected Emails
- Stolen/Lost Portable Devices (client information)
- HIPAA Violations
- Improper Disposal of Information (trash v. shredding)

TOP CYBER-SECURITY THREATS FACED BY LAW FIRMS



Data Breaches



Insider Threats



Advanced Persistent Threats (APTs)



Supply Chain Attacks



Cloud Storage Vulnerabilities

TYPES OF PROTECTED INFORMATION

- Client Files/Information (e.g. HIPAA data, PHI information, SSN, trade secrets, analysis, strategies, etc.)
- Financial information (e.g. client and law firm)
- Human Resources Records (e.g. employees, clients, etc.)

FACELESS ATTACKERS

- Hacktivists
- Criminals
- Insiders
- Nation-States
- Terrorists
- Military – It is War!



RULES OF PROFESSIONAL CONDUCT

ABA Model Rule 1.1 Duty of Competence

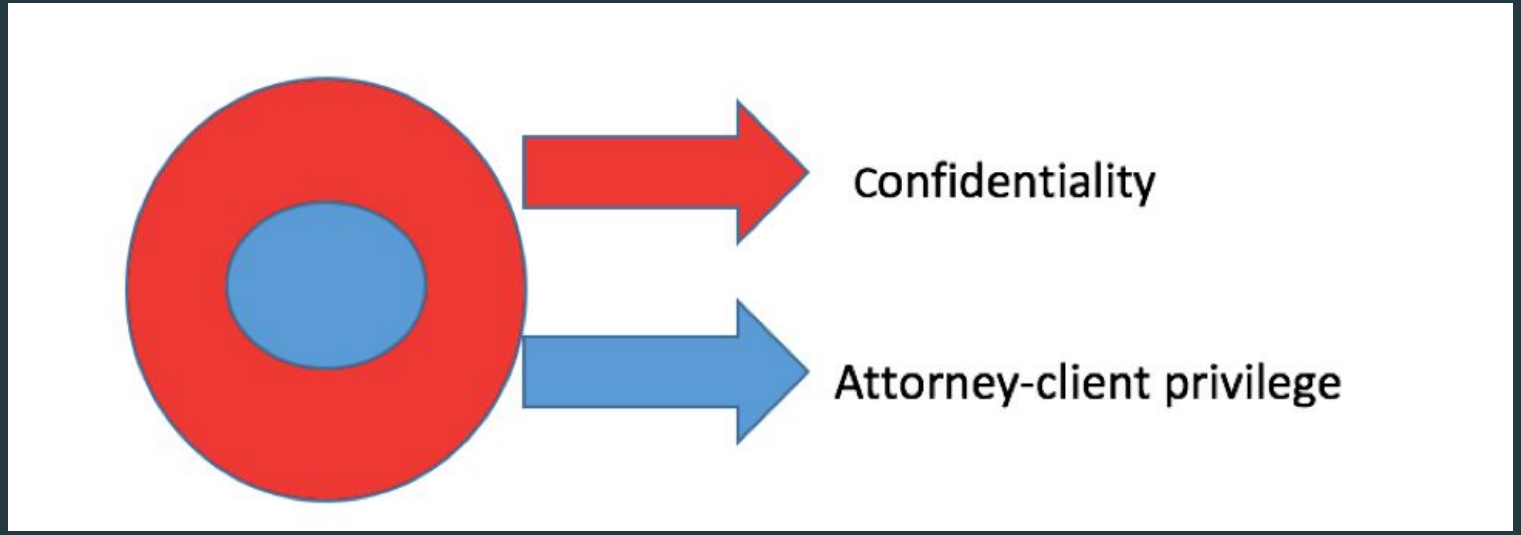
Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

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, . . .

ABA Model Rule 1.6(c) Duty of Confidentiality

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

RULE 1.6 CONFIDENTIALITY



An attorney's duty of confidentiality is far broader than the attorney-client privilege.

In Re Hultquist, 961 N.E.2d 999 (Ind. 2012)

COMBINE THE RULES

A lawyer must act *competently* to preserve/safeguard *confidential* client information against unauthorized disclosure by the lawyer or persons under his/her supervision.

ABA Model Rules, R. 1.6 Comment [18]

Safe Harbor: Unauthorized access is NOT a violation if the lawyers makes reasonable efforts.

REASONABLE EFFORTS

Reasonable Efforts to Prevent Unauthorized Disclosure, Model Rule:

NOT one size fits all

Multifactor analysis – (1) information sensitivity, (2) likelihood of disclosure without additional safeguards, (3) costs, (4) difficulty of implementation, (5) adverse effect of safeguards vis-à-vis lawyer's ability to represent clients

ABA Model Rule 1.6, Comment [18]

ABA Formal Opinion 477R (revised May 2017)

-Email encryption and other guidance

REASONABLE EFFORTS

- Reasonable Efforts to Prevent Unauthorized Disclosure, Guidance Under ABA Formal Opinion 477R:

Understand the Nature of the Threat

Understand How the client Confidential Information is Transmitted and where it is Stored

Understand and Use Reasonable Electronic Security Measures

Determine How Electronic Communications About Clients Matters Should be Protected

Label Client Confidential Information

Train Lawyers and non-lawyers Assistants in technology and Information Security – ABA Model Rule 5.1 (supervise subordinate lawyers); and 5.3, (supervise and train non-lawyer staff)

Conduct Due Diligence on Vendors – Next Slide

ABA Formal Opinion 477R (Revised May 2017)

DUTY TO COMMUNICATE

A lawyer shall promptly inform the client of any decision or circumstance with respect to which the client's informed consent is required, reasonably consult with the client about means of to accomplish objectives, keep the client informed of status of the matter, respond to requests for information, and consult on any relevant limitation on lawyer's conduct.

ABA Model Rule 1.4

DUTY TO DISCLOSE RISKS

Duty to Disclose After Cyberattack (ABA Formal Opinion 483)

- ntact General Counsel

Advise Clients About Potential Disclosure/Communicate Risks:

Advise clients about risks associated with email communications that may potentially compromise the client confidentiality depending on the server, device and transmission mode. (ABA Standing Comm. on Ethics and Prof. Resp., 11-459 Formal Opinion 2011.)

When a lawyer reasonably believes that highly sensitive/confidential client information is being transmitted so that extra measures to protect the email are warranted, the lawyer should inform the client about the risks involved. (ABA Model Rules 1.4 (a)(1)&(4))

The client may insist or require the lawyer to undertake or conduct certain forms of communication (ABA Model Rules 1.6 Comment [18])

DUTY TO DISCLOSE AFTER CYBERATTACK

- Obligation to monitor the breach
- Stop the breach and restore the systems
- Determine what occurred
- Provide noticed to current clients affected – extent of communication depends on type of breach – enough information for client to make informed decision on what to do next

ABA Formal Opinion 483

ELEMENTS OF AN INCIDENT RESPONSE PLAN

Assign Responsibility

Internal Reporting Procedures

Criteria for Activating the Plan

Internal Personnel and Resources

Alternative Communication Channels for Response

External Resources (e.g. data breach lawyer, insurance, law enforcement, forensic consultant, credit monitoring, crisis communications, bank, etc.)

Flexibility in the Plan For Unknown

Communications Plan (external and internal)

Notice (e.g., required/optional notifications, employees, clients, service providers, third parties)

Keep Records of Response Activities

Preserve Digital Evidence

Mitigation

Restore Systems

Practice the Incident Response Plan

Training/Periodic Review and Updates

CORE PLAN FUNCTIONS

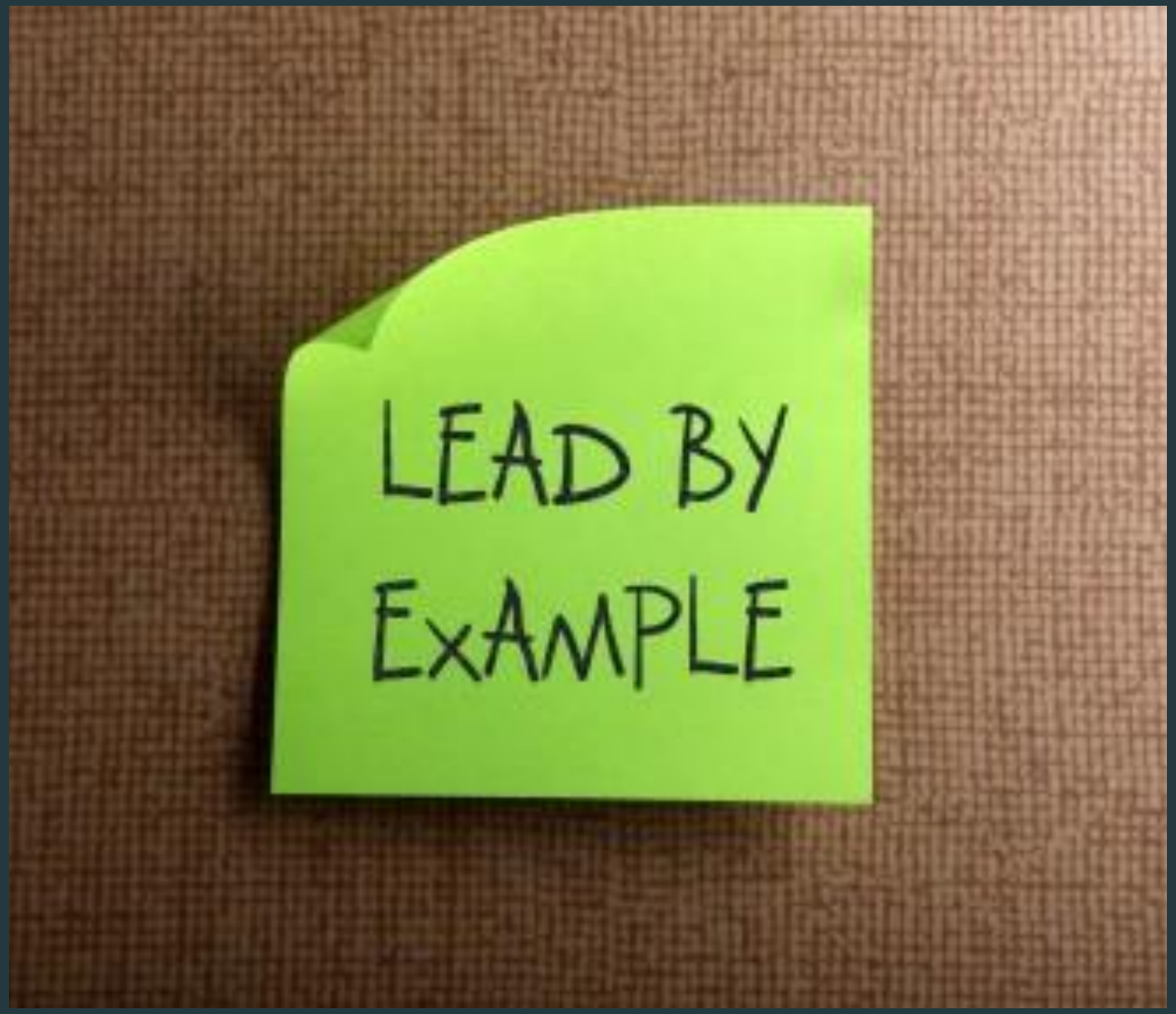
Identify

Protect

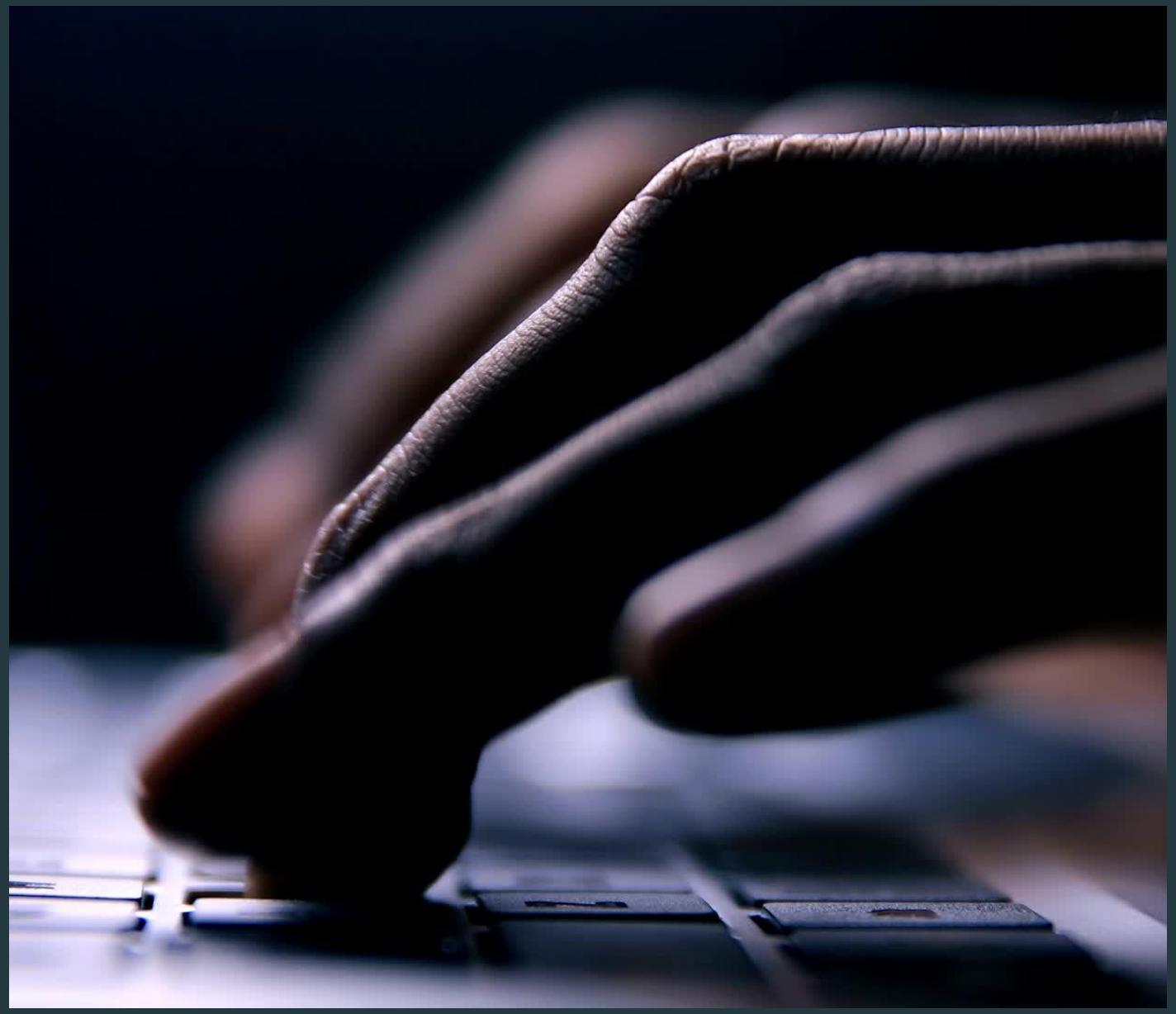
Detect

Respond

Recover



COMMON SCENARIOS



PHISHING/SOCIAL ENGINEERING

John works for a large law firm. One afternoon he notices an email from his information systems (“IS”) department. The message states that his email has been compromised and instructs him to immediately reset his username and password information by clicking on the attached link, which John promptly does. The next day, the managing partner of the firm calls stating that the organization has experienced a significant breach of over 3,000 client files, which has been traced to John’s computer. He asked John what he has done and/or clicked on recently.

What did John do wrong?

What is the proper ethical response?

What disclosure duties does John have after the cyberattack?

IMPROPER DISPOSAL

Betty is a paralegal at Mickey Mouse, LLP. She regularly handles client medical records and sensitive data (e.g. PHI for clients). Occasionally, Betty must dispose of the printed PHI. She understands the information is sensitive and must dispose of it securely, but the nearest secure shred receptacle in her practice is down the hall. Betty keeps a "shred" pile under her desk in a box, and empties it in the secure shred receptacle once a week. Betty last emptied the box 3 days ago, but this morning when she arrived to work she noticed it was empty again. She later learned that the custodial staff emptied the box in the regular trash.

What did Betty do wrong?

Ethical obligations of supervising attorneys?

What should Betty do now?

BREACH OF CONFIDENTIALITY

Linda is a law partner at her law firm. One day she receives a phone call from a client, Bob, who is very tearful and clearly upset. At the time of the call Linda was waiting in her doctor's office (in the public waiting area). However, Linda proceeded to take the call from Bob, and even put it on speaker phone to hear him better. During the call Linda repeated (out loud) back to Bob the facts of his case (e.g. his medical condition, evidence, strategy, etc.) and gave him legal advice. The other persons in the waiting room overheard the entire conversation.

After the call Linda opened up her laptop and typed out notes about the call with Bob. Susie, who was sitting next to Linda, read all of Linda's notes over her shoulder and even corrected a spelling mistake for Linda as she was typing.

What did Linda do wrong?

What are Linda's ethical obligations?

What should Linda do now?

MISDIRECTED EMAIL

Todd is an attorney at a large law firm. Todd was in a hurry and didn't properly look at the "auto-fill" email address that populated into an email that he was drafting to his client. Instead of going to Todd's client, the email was misdirected to opposing counsel. The email contained case strategy and evidence that Todd had successfully kept out of discovery that could harm the client.

What did Todd do wrong?

What should Todd do now?

Does the opposing counsel have any obligations?

ABA Model Rule 4.4



This Photo by Unknown Author is licensed under CC BY-NC

PORTABLE DEVICES

Dan is a lawyer at a law firm. He is traveling out of town for vacation and took his computer and cell phone with him in order to work some on vacation. Dan's devices have confidential information on them for all of Dan's 250+ clients, including PHI information. Dan inadvertently leaves his laptop in the taxi that dropped him off from the airport to his hotel. He contacts the taxi service, but several customers have been in the cab since Dan got dropped off and Dan's laptop was nowhere to be found. The laptop was no encrypted or password protected.

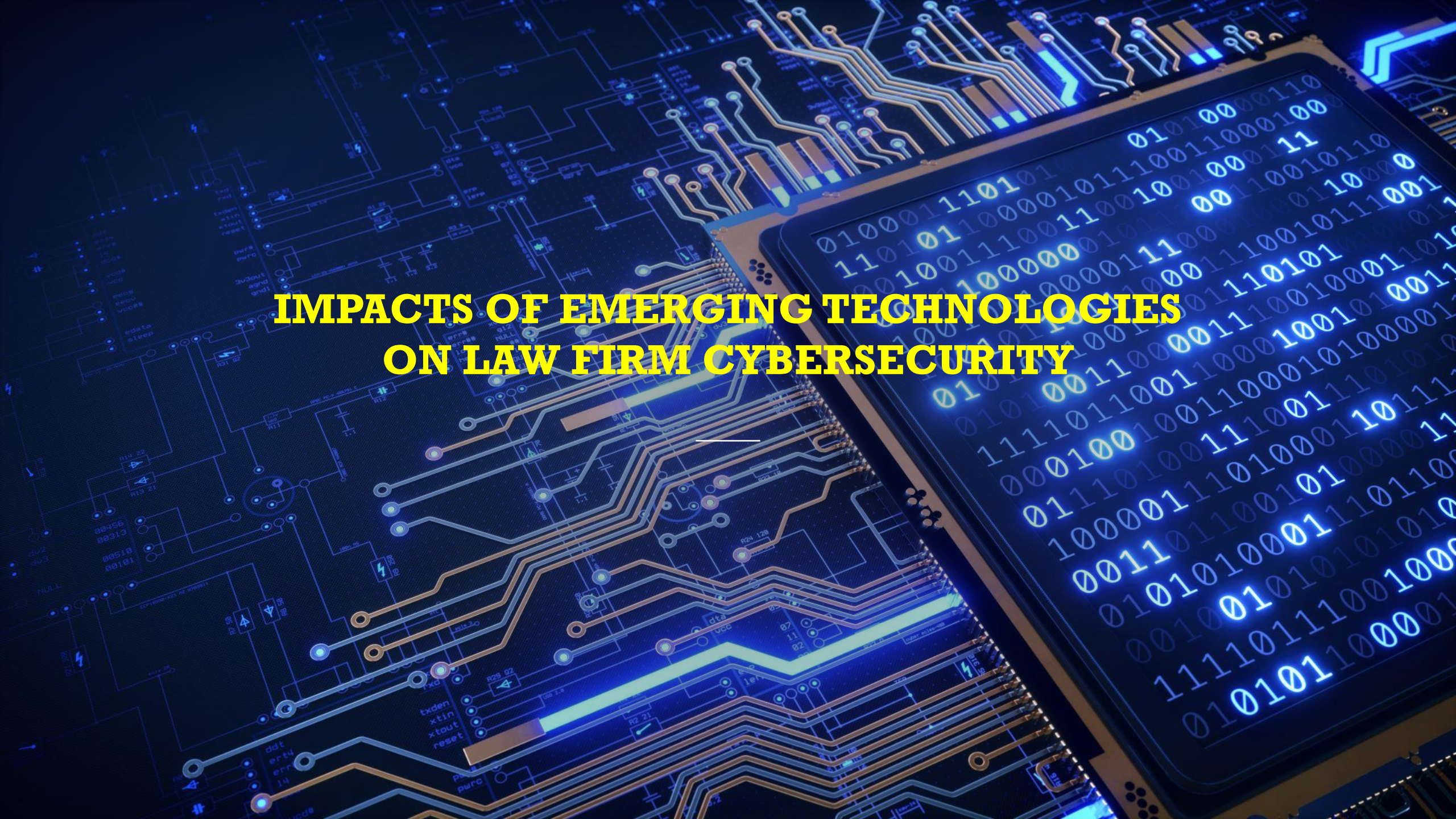
What did Dan do wrong?

What should Dan do now?

What are Dan's client obligations?

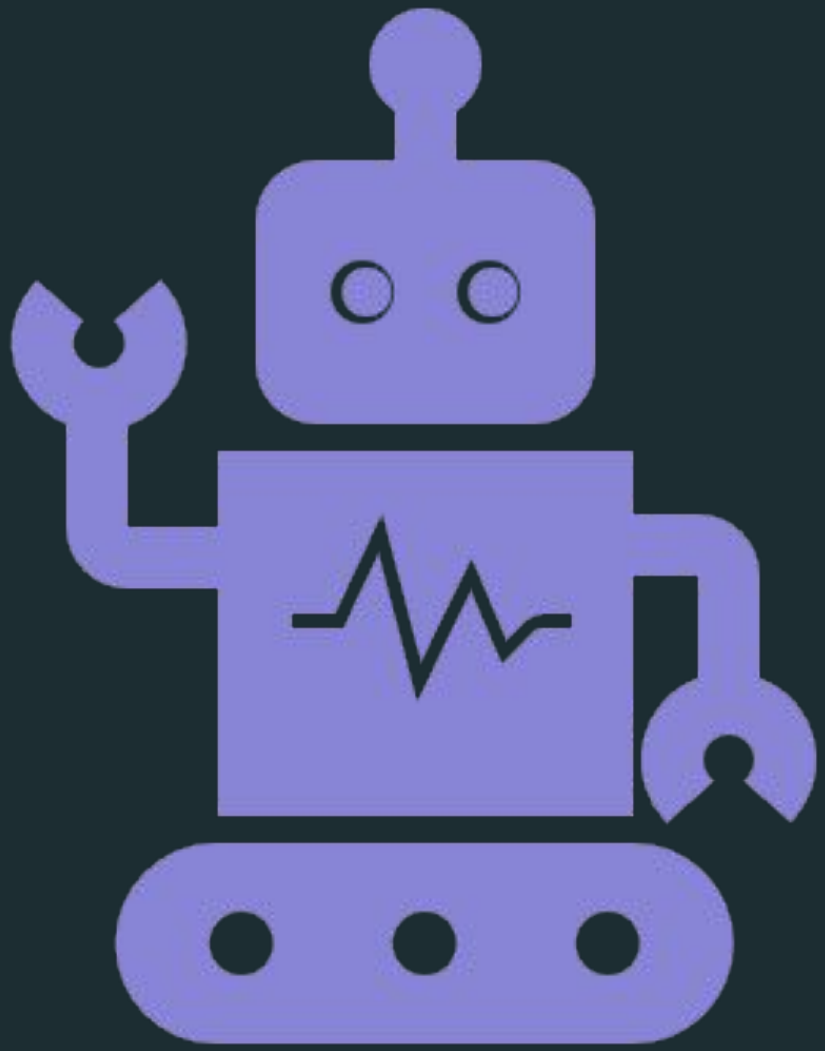


This Photo by Unknown Author is licensed under CC BY-SA-NC



IMPACTS OF EMERGING TECHNOLOGIES ON LAW FIRM CYBERSECURITY

CHATGPT AND AI TIPS AND TRAPS



CHATGPT

ChatGPT: ChatGPT (openai.com)

Chat GPT (Generative Pre-trained Transformer) is an AI language model developed by OpenAI, based on the transformer architecture. It is a machine learning model that has been trained on a massive amount of data, including web pages, books, and articles, and can generate human-like responses to text-based prompts.

ChatGPT 3.5 (Plus): Free Service; Not as reliable or accurate

GPT-4: most advanced system, producing safer and more useful responses; Costs $20/month for faster speed and exclusive access to beta features like browsing, plugins, and code interpreters

DALL-E: AI system that can create realistic images and art from a description in natural language; Cost 'credits' per usage

CHATGPT CAPABILITIES

Language Generation:

It can generate text in a natural language that is difficult to distinguish from text written by a human.

Question Answering:

It can answer questions based on a given context or topic.

Text Completion:

It can complete partially written text with suggestions that are contextually relevant.

CHATGPT CAPABILITIES

Text Summarization:
It can summarize long pieces of text into a shorter, more concise version.

Language Translation:
It can translate text from one language to another.

Sentiment Analysis:
It can analyze the tone and sentiment of text.

Chatting:
It can engage in conversations with users and provide them with relevant responses.

CHATGPT CAPABILITIES

Explain Stock (buying/selling) Options Trading

Design Database Schema

E.g., design for online merchandise store

Brainstorm Names

Recommend Activities

E.g., team-building day with remote employees

OTHER ETHICAL CONCERNS WITH CHATGPT

Rule 1.6 Confidentiality

Rule 1.4 Communication

Rule 1.5 Fees

Rules 5.1 and 5.3 Supervision

Rule 8.4 Prejudicial to the Administration of Justice/Bias

SO WHY USE CHATGPT?



POTENTIAL ADVERTISING FORUMS

Blogs: If the blog is being used (whole or in part) to try and get clients to hire you, it is advertising and subject tot the Rules.

- It should contain the "Advertising Material" disclaimer and all other required disclosures.

Lawyer Listings: Information contained here cannot be false or misleading.

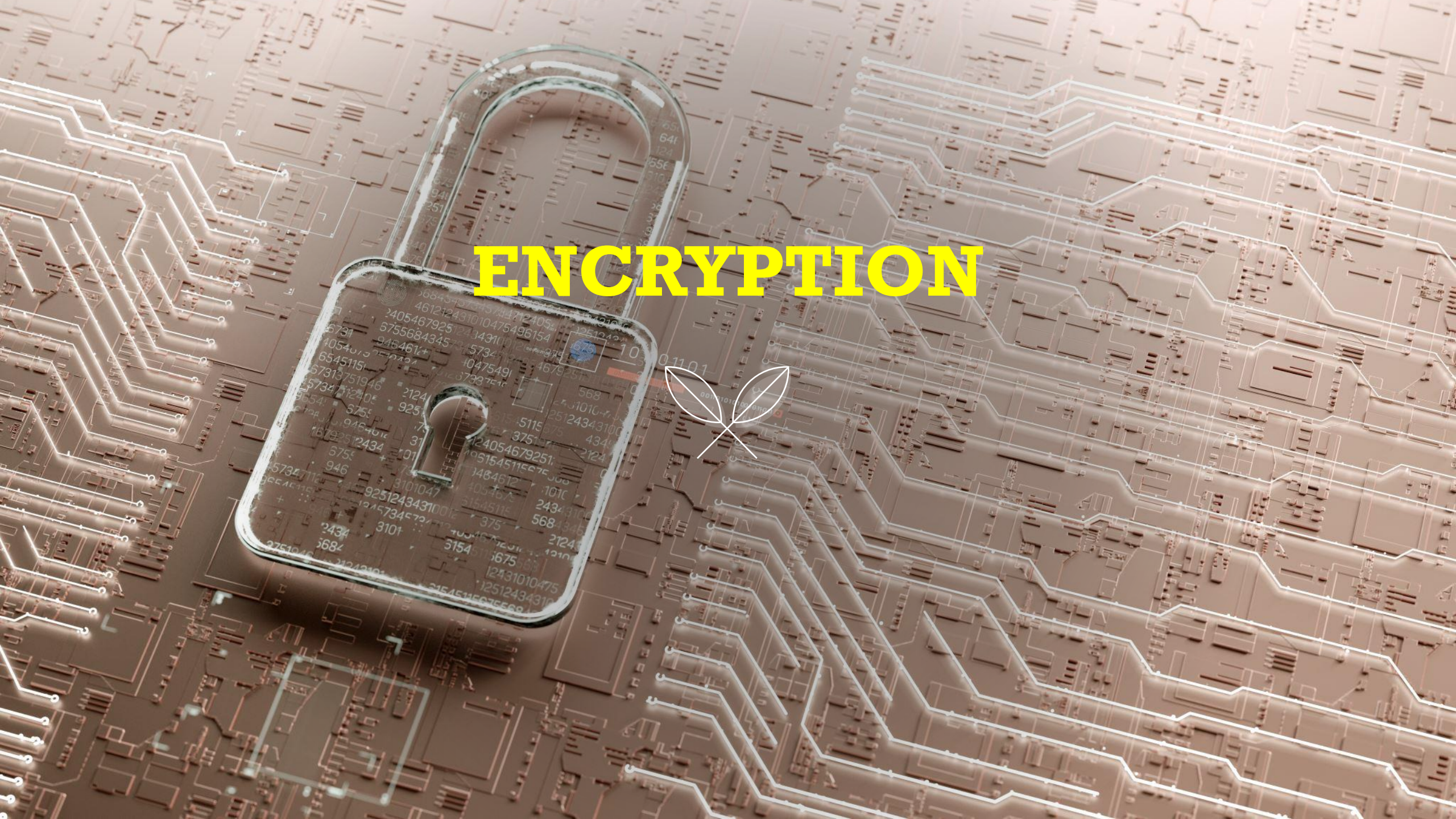
- Pay attention to practice areas and memberships listed.
- No direct guidance but conservation approach is to add the "Advertising Material" disclaimer and all other required disclosures.

YouTube: Acts like television commercials.

Social Media Platforms (TikTok, LinkedIn, Twitter, Facebook, Instagram, Snapchat, etc.): Keep your personal life professional. Your personal page, if advertise, or post about your work could be considered attorney advertising (even Facebook).

- All endorsements must be truthful and not misleading.
- It is YOUR responsibility to comply and monitor you own accounts even if you are not the one that posted it (but tagged).
- It should contain the "Advertising Material" disclaimer and all other required disclosures.

Newspapers/Print Media/Billboards/Bus /Commercials: The traditional advertisements in which we are familiar.


ENCRYPTION

WHAT IS ENCRYPTION?

The process of converting information or data into a code, especially to prevent unauthorized access. Protects sensitive information, such as financial data, personal information, and government secrets, from being accessed by unauthorized parties.



TYPES OF ENCRYPTION



Symmetric: same key is used for both encryption and decryption of the data. Sender and receiver must both have the same key and must keep it secret from everyone.



Asymmetric: uses 2 different keys for encryption and decryption. Sender and receiver have private keys.

WHY LAW FIRMS NEED ENCRYPTION



Regulatory compliance requirements (e.g., GDPR, HIPAA, etc.)



Protecting client confidentiality and trust



Mitigating risk of data breaches and cyber threats


TOP 5 TIPS FOR EVALUATING CYBERSECURITY SERVICES AND SOFTWARE

- **Prioritize Compliance and Industry Standards**:
  - Ensure that any cybersecurity or software service under consideration is compliant with legal industry standards and regulations, such as those related to data protection (e.g., GDPR, HIPAA in the US, or PIPEDA in Canada). Check for certifications that are pertinent to legal data security, such as ISO 27001, which indicates a provider's commitment to information security management.
- **Evaluate Data Security and Privacy Features**:
  - Focus on services that offer robust encryption protocols, both for data at rest and in transit. The ability to control and monitor access to sensitive information is crucial. Look for features such as end-to-end encryption, role-based access controls, and detailed auditing capabilities that can track who accessed what data and when.
- **Assess Vendor Experience in the Legal Sector**:
  - Choose vendors that have proven experience and a positive track record within the legal sector. Vendors should understand the unique challenges and needs of law firms, such as the handling of privileged information and the requirement for high availability and disaster recovery capabilities.
- **Check for Scalability and Integration**:
  - The chosen service should scale with the growth of the firm and easily integrate with existing systems (such as document management systems, client management software, and communication tools). Integration is key to ensuring that workflows remain streamlined and that new security measures do not disrupt daily operations.
- **Understand Support and Incident Response**:
  - Evaluate the vendor’s support structure and incident response times. Effective customer support is crucial for resolving issues swiftly to minimize any potential downtime. An ideal service should offer 24/7 support given the critical nature of legal work. Additionally, understanding the vendor’s incident response plan is essential to ensure they can effectively handle and mitigate a data breach or cyber attack.

QUESTIONS/COMMENTS?



THANK YOU!

Cari L. Sheehan, Esq.

Assistant Clinical Professor of Business Law & Ethics

Conflicts Attorney

(812) 239-4187

The content of this presentation is for general information purposes only.
It does not constitute legal advice or an attorney-client relationship.