



1

Presenters



David M. Buddingh, President and General Counsel
David has spent over a decade in the legal profession where his work is always guided by a genuine commitment to his clients. It was his commitment to providing his clients with better options for communication that sparked the idea for EIE Legal. He is a graduate of the DePaul University College of Law and the University of Iowa.



2

The Age of Hacking: Organization and Client Data at Risk

- **Equifax** – 143 million Social Security Numbers
Source: [CNN](#)
- **Yahoo** – 200 million users' private information
Source: [AP](#)
- **Uber** – 57 million customer data breach
Source: [TechCrunch](#)



3

The Age of Hacking: Firm Data at Risk

- E-mail compromise scams continue to grow, evolve, and target businesses of all sizes.
- Between January 2015 and December 2016, there was a **2,370% increase in identified exposed losses**. Email scams were reported in all 50 states and in 131 countries.
- From October 2013 to December 2016, The IC3 (Internet Crime Complaint Center) had reports of:
 - **22,292 U.S. Victims**
 - **\$1,594,503,669 exposed losses**

Source: [FBI](#)



4

Law Firms at Risk

“According to the ABA’s 2016 Legal Technology Survey Report, **more than one quarter of firms with more than 500 lawyers admitted they experienced some type of breach.**”

- Approx. 40% of those firms reported **significant resulting business downtime** and **loss of billable hours**
- Approx. 25% recounted **hefty fees** to correct the problems.
- One in six also reported loss of important files and information.”

Source: [ABA](#)



5

Law Firms Targeted


- 2015 Verizon Report shows corporate lawyers are the easiest lawyers to phish [findlaw](#)
- The Top Ten Law Firms Attacks of 2017 according to the Disruptor Daily [disruptordaily.com](#)



6

Threats


- **Ransomware:** Criminals infect a computer or network with malicious software that encrypts data. The files cannot be decrypted without a mathematical key known only by the attacker. The thief will then demand payment in exchange for the return of that data.
- **Phishing:** Attempts to trick people into sharing confidential information via email. For example, a fraudster might pose as a Title company and send wiring instructions to your Title Agent steal their funds. These emails can be very convincing that phishing emails have become increasingly challenging to identify. They are "designed to mimic legitimate communication to gain access to sensitive information, such as usernames and passwords," he explains." [\[Inc\]](#)



7

Threats


- **Malware:** a malicious 3rd party software that is designed gain unauthorized access to or otherwise damage a network.
- **Individuals:** organization employees allow unauthorized access to a network due to failure to follow protocols or insufficient training



8

Threats

- **Spoofing:** 3rd Party impersonation of a email, phone number or text messages
- New York lawyer's clients spoofed by false email [fortune.com](#)
- Chinese hackers make \$4 million using hacked information to trade stocks [nytimes.com](#)



9

Case Study

- **Real Estate Transactions:** E-mail (BEC/EAC) scams target all participants in real estate transactions, including buyers, sellers, agents, **and lawyers.**



Source: [FBI](#)



10

Case Study

- The IC3 saw a **480% increase** in the number of complaints in 2016 filed by title companies that were the primary target of the BEC/EAC scam.
- **\$5.3 billion targeted** by perpetrators in the mortgage industry alone in 2016
- BEC/EAC perpetrators were able to monitor real estate proceedings to time the fraudulent request for a change in payment type (frequently from check to wire transfer) or a change from one account to a different account under their control.



Source: [FBI](#)



11

Texting Popularity

- 81% of Americans text regularly. ([Pew Research Center](#))
- 2.27 trillion texts are sent every year. ([CTIA](#))
- Americans text twice as much as they call, on average. ([Nielsen](#))
- Sending and receiving text messages is the most prevalent form of communication for Americans younger than 50. ([Gallup](#))



12

Why Lawyers Turn to Texting

- **Ease** – It's what clients already do. The clients' need to have good communication with the lawyer in ways that make sense for them.
- **Efficiency** – It can keep clients up to date in the moment from the office or from court without having to get on the phone. There is certainty of receipt.
- **Effective** – It creates an instantaneous record / reference, running dialogue.



13

Lawyers' Concerns about Texting

- Ethical Obligations
- Confidentiality Concerns
- Over Accessibility
- Record Preservation
- Simplistic



14

Duty of 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.

Florida Ethics Rule 4-1.1
 Rule 1.1



15

Rules of Confidentiality

- (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 [Rule 1.6 Confidentiality of Information](#)
- Florida's Rule 4-1.6(a) Consent Required to Reveal Information. A lawyer shall not reveal information relating to representation of a client except as stated in subdivisions (b), (c), and (d), unless the client gives informed consent

16

Duty of Competence Again

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

Florida Ethics Rule 4-1.1



17

Rules of Confidentiality Again

- (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 [Rule 1.6 Confidentiality of Information](#)
- Florida's Rule 4-1.6(a) Consent Required to Reveal Information. A lawyer shall not reveal information relating to representation of a client except as stated in subdivisions (b), (c), and (d), unless the client gives informed consent

18

Considerations in Protecting Your Client's Communications

- Understand the Nature of the Threat
- Understand How Client Confidential Information is Stored and Transmitted
- Understand and Use Reasonable Electronic Security Measures (Important)
- Determine How Electronic Communication about Client Matters Should be Protected
- Label Client Information

ABA Formal Opinion 477

19

Considerations Continued

- Train Lawyers and Nonlawyer Assistants in Technology and Information Security
- Conduct Due Diligence on Vendors Providing Communication Technology

ABA Formal Opinion 477



20

Reasonable Efforts Standard

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 used
- 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 (e.g., by making a device or important piece of software excessively difficult to use)

ABA Formal Opinion 477



21

Sensitivity of Data ABA Analysis

- The ABA states a fact based analysis of information is necessary to determine what information should be protected or encrypted are warranted in some circumstances.
- Routine communications need not be protected while sensitive substantive communications ought to be protected.
- What does it mean? Perhaps not the best practice for lawyers.

22

Reasonable Efforts Standard

HOWEVER,

- Special circumstances may warrant special precautions such as communication protected by law or by a confidentiality agreement.



23

What communications to preserve

- [ABA Formal Opinion 477](#) makes a distinction between routine and substantive information
- Lawyers may need to discuss security with clients
- The opinion notes a lawyer's need to "keep abreast of knowledge of the benefits and risks associated with relevant technology"



24

Data Storage Requirements in Florida

- (1) identification of the potential threat to confidentiality along with the development and implementation of policies to address the potential threat to confidentiality;
- (2) inventory of the Devices that contain Hard Drives or other Storage Media;
- (3) supervision of nonlawyers to obtain adequate assurances that confidentiality will be maintained; and
- (4) responsibility for sanitization of the Device by requiring meaningful assurances from the vendor at the intake of the Device and confirmation or certification of the sanitization at the disposition of the Device [Florida Bar Ethics Opinion 10-2](#)



25

Is Texting Ethical?

- Yes – No prohibition exists.
- BUT – American Bar Association Formal Opinion 477R states that an attorney is responsible to insure that communications are secure. [ABA Formal Opinion 477](#)



26

Solicitation of New Clients via Text

- Text message solicitations of new clients is permissible in Florida [The Florida Bar](#)
- The first line of the text must say it is an advertisement
- The lawyer must track who receives the texts and the content
- The lawyers must insure that the prospective client is not responsible for the data costs by working with cell phone service providers
- Must have a method for prospective clients to opt out



27


Law Firms at Risk

- Any firm relying on existing non-secure messaging systems to communicate with and about clients is **putting themselves and their clients' confidential information and privileged communications at risk.**
- Using a non-secure communication channel can also be a **breach of ethical responsibility.**



28

Steps law firms can take towards secure mobile communication

- Password protection
- Multifactor authentication
- Hardware firewalls
- Encryption protocols for data sharing
- Training
-  Using to insure compliance

29

Texting Weakness

- Vulnerability due handoff to intermediaries
- Lack of encryption
- Spoofing
- Individual error
- Data on device
- Network connection exposure



30

Reasonable Efforts in Current Environment

- Encryption Industry Standard AES 256 Bit
- End to End Encryption



31

Encryption Standards

- Why 256 bit?
- What is 256 aes bit encryption?



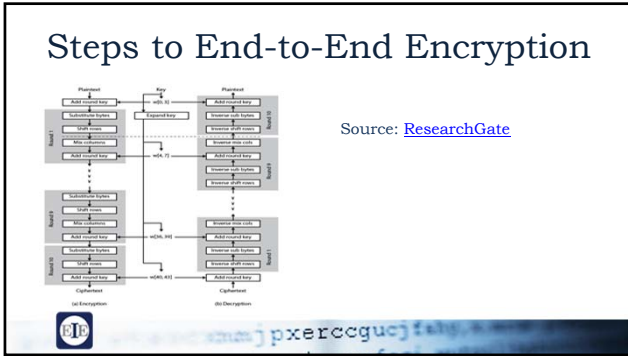
32

End to End Encryption

- Data is encrypted on the senders' devices or networks and remains encrypted until it is decrypted on recipients' devices or networks
- Decryption occurs at the end point of the communication



33



34

Data on Device

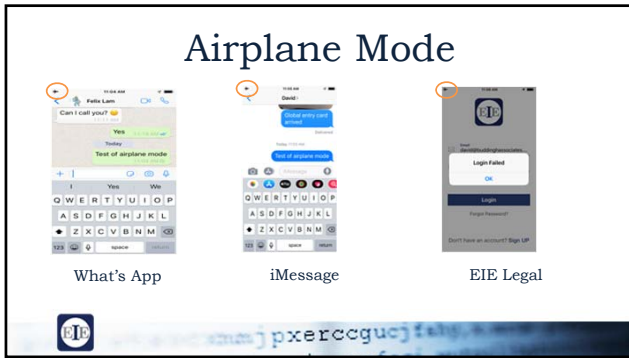
- Information on device
- Susceptible to data breach
- Unencrypted

35

What is the Cloud?

- Endless data centers
- Endless networks
- Redundancy
- Speed
- Cost of operations

36



37

Can a lawyer ethically use cloud based technology in Florida?

- Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;
- Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;
- Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored.

38

Ephemeral Platforms

- Seem like the solution – no record, nothing to hack.
- But...
- Not favored by Department of Justice Regulators fnablog.com
- Uber/Waymo
 - IP theft
 - \$245 million settlement
- Missouri Former Governor Greitens
FOIA and state laws/regulations

Source: Wired

39

Ephemeral Platforms

- Problem: no record, no proof
- Existing messaging apps don't create an archived record of conversations – leaving firms exposed to liability.



40

Preserve Communications

- Necessary to document every communication to properly represent the client.
- Unalterable record: best practice limiting liability from potential misconduct accusation.



41

Third Party Help

- Lawyers are generally not technology experts
- But ethical obligations still apply



42

Model Rule 5.3 Responsibilities Regarding Nonlawyer Assistance

What questions should lawyers ask their potential vendors when it comes to messaging and encryption or due diligence consideration.

- Reference checks and review of 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 diversity.
- The availability of legal redress.

43

Florida Standard

- Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;



44

What Do You Need?

A communications platform that is:

- **Transparent**
- **Instant**
- **Secure**
- **Unalterable**



45

What is EIE Legal?

EIE Legal is a **secure mobile messaging app** for lawyers that puts encrypted transparency in the palm of their hands.



46

What is EIE Legal?

Most importantly, it's a solution to a problem lawyers and clients face every day:

Clients want to communicate as easily with their lawyer as they do with everyone else – through a messaging app.

But, existing messaging options do not meet the necessary legal standards, putting both lawyers and clients at risk.

Lawyers can protect their privacy by not giving out their cell phone number, but their information is still be accessible.



47

Beyond Traditional Messaging

- As a lawyer, your communications with clients need to be secure and recorded for the future.
- Our service encrypts not only your conversation but also any PDFS, notes, photos, or other documents. Then, it stores the conversations until the user archives them.
- The archived record can be “printed” out and retained in hard copy files or moved to electronic storage (i.e. cloud). Both preserve evidence of the conversation.
- EIE Legal app goes beyond end-to-end encryption – users’ information and communications are always encrypted and can never be accessed by our servers.



48

EIE Legal App Features

- Quick, convenient messaging system that meets lawyers' security needs
- "Encrypted Transparency"TM: Archived record of communications to retain for their files and option to "print" communications
 - Text messages
 - Notes
 - Photos
 - Videos
 - Microsoft Office documents
 - PDF documents



In addition, the app stores them until the user deletes them, when a record is made for safekeeping.

49

Encrypted TransparencyTM

- EIE Legal automatically creates a record of every conversation so users will never be in jeopardy of losing information or evidence in a text.
- That provides the firm with the security it needs to face future challenges from clients and protect themselves from costly lawsuits.



50

Communication Record Options

- When the conversation has been completed all parties involved will receive an encrypted archive of the discussion on their phones. Allowing you to protect yourself with "Encrypted Transparency"TM.
- Each party then has four options:
 - **KEEP** the archived encrypted conversation on in their cloud based account for as long as they choose.
 - **PRINT** the archived conversation to a wireless printer. The document will become unencrypted at the point of printing.
 - **STORE** the conversation electronically. I.E. save to One Drive cloud or send to a file folder.
 - **DELETE** the archived conversation completely, retaining no personal record of the conversation on their own phone. This does not mean the other parties' copies will be deleted.



51

Tracking Your Communications

- Our team can never access any of your communications due to the encryption process EIE Legal.
- You will immediately receive a notification if a contact took a screenshot of the conversation.



pxerccguqj falg

52

Selective Accessibility

- Securely engage your clients on your terms
- Your clients have access to you always and securely
- But they don't have your cell phone number
- That means you (the lawyer) can choose how and when to respond to your portion of the 2.27 trillion texts sent every year.



pxerccguqj falg

53



pxerccguqj falg

54


Contact Us

- Custom encryption services and app development available for your law firm.
- Contact us at: Info@EncryptedInfoEx.com
- Or dmbuddingh@encryptedinfoEx.com



55

COURSE #3596



Legal EIE: Encrypted Messaging App for Law Firms.
Always Secure. Always Transparent. Always Recorded.

56
