KNOWING AND MANAGING CYBERWORLD RISKS

HON. REBECCA SIMMONS, *San Antonio*
Acelity

State Bar of Texas
10TH ANNUAL
BUSINESS DISPUTES
September 26-27, 2018
Austin

CHAPTER 9

Honorable Rebecca Simmons
Rebecca Simmons PLLC
P.O. Box 12408
San Antonio, Texas 78212

Education

Austin College B. A. 1978
Baylor University School of Law J.D. l980
Durham University, England post-graduate study 1981

Current Professional Activities

Rebecca Simmons PLLC providing arbitration, mediation and consulting services
Visiting Judge sitting by special assignment to appellate and trial courts 2013 – present
Adjunct Professor, St. Mary's University School of Law 1994 – present
American Arbitration Association commercial litigation and labor panel member

Experience

Associate General Counsel, Litigation Acelity LLP 2013-2016
Justice, Fourth Court of Appeals 2005 – 2012
Judge, 408th District Court of Bexar County Texas 2003 –2005
Akin Gump Strauss Hauer & Feld LLP 1992 –2003
Cox & Smith Incorporated 1983 – 1992
Briefing Attorney, Texas Supreme Court l980 – 1981
Specially Commissioned as Texas Supreme Court Justice to hear a designated case in 2005

Awards and Recognition

Winning Women of Texas 2014, Texas Lawyer
Lee Cusenbury Ethical Life Award 2014, Association Corporate Counsel San Antonio
Lumen Gentium Award, Archdiocese of San Antonio 2013
Interfaith Dialogue Community Justice Award 2010
Honorary San Antonio Young Lawyer of the Year 2008
Austin College Alumni of the Year 2006
State Bar of Texas Presidential Citation 2004

Activities

Chair, Texas Judicial Committee on Information and Technology 2009 – present
Council Member, Texas State Bar Litigation Section 2014 – present
Director, State Bar of Texas District 10, place 1 2015 - 2018
Member, State Bar of Texas Rules Committee
Former President, San Antonio Bar Association 2013 – 2014
Former Chair, Texas Bar Foundation with an endowment of over $20,000,000
Former President of the Bexar County Women's Bar Association 2006
Former Chair of the William S. Sessions American Inns of Court 2008
Trustee, Austin College 2012 – present

Speaker and Author

Speaker on numerous subjects; recent topics include:
Breaking the Glass Ceiling: Women in the Law: Advanced Insurance Course 2018
Texas Court of Criminal Appeals: Future, Present, Past
Texas Criminal Defense Lawyers Association 2018
Access to Electronic Court Records: Litigation Update 2018
Recent Cases Affecting Business Disputes; General Practitioner Update 2018
Update on Electronic Filing: What's on the Horizon: Litigation Update 2017
Spoliation Under the Texas Framework: Advanced Civil Trial Course 2016
Maintaining Client Confidentiality in the Digital Era: Advanced Civil Appellate Course 2015
E-Filing Update 2015: E-Filing, E-Service, and Access; What's on the Horizon? Advanced Personal Injury Course 2015
Law Office Security in the Cloud: Technology and File Management, Essentials for the General Practitioner Course 2014
Technology and File Management: Best Practices for Reducing, Managing and Storing Your "Paper", UTCLE, 48th Annual William W. Gibson, Jr. Mortgage Lending Institute 2014
Hot Cases and Emerging Law: Spoliation in Texas, UTCLE; 38th Annual Page Keeton Civil Litigation Conference 2014
E-Filing and E-Service: Tips, Traps, and the TRCP: Advanced Civil Trial Course 2014
Vanishing Documents and Emerging Law: Spoliation in Texas
Vanishing Documents and Emerging Law: Spoliation in Texas
UTCLE State and Federal Appeals 2013
Tech Tips for Real Estate Practitioners: Advanced Real Estate Course 2013
E-Filing Update; Advanced Civil Trial 2013
Traveling in the Cloud; Advanced Personal Injury Course 2012
Plea to the Jurisdiction; Advanced Personal Injury Course 2011
Judicial Recusal; Advanced Personal Injury Course 2010
E-Filing and Technology; Bexar County Women's Bar Association 2011
E-Filing and Apps for the I-Pad; Winter Judicial Conference 2012
Cloud Security, San Antonio Appellate Section 2012
Panel Discussion on Appellate Practice; Advanced Appellate Conference 2010 and 2012

Author of several articles in the San Antonio Lawyer magazine, various papers for continuing legal education seminars and the following law journal articles:

*Section 3 and Liability for the Condition and Use of Real Property Under the Texas Tort Claims Act***,** 31 Baylor Law Review 506 (1979).
The Enhancement of Anticompetitive Activity through Group Purchasing Organizations: A Case Study. 17 Antitrust Healthcare Chronicle 1, Spring 2003.
Exploring Grounds for Attorney Disqualification and Deciphering Exacting Standards, 37 ST. MARY'S L.J. 1009 (Spring 2006).
Plea to the Jurisdiction: Defining the Undefined, 40 St. Mary's L.J. 627 (Spring 2009).
Texas's Spoliation "Presumption", 43 ST. MARY'S L.J. 691 (Spring 2012)

Personal

Teacher of 6th grade CCD at Our Lady of Grace Parish Married to Richard Clemons and mother of 3 children Hobbies include: running, gardening and cooking

TABLE OF CONTENTS

KNOWING AND MANAGING CYBERWORLD RISKS

I. ABSTRACT

Change in the legal profession is accelerating. Technology has been the driver of rapid change, and is transforming the practice of law and will continue to do so. The advent of technology has provided remarkable convenience and efficiency in the practice of law but will also create disruption that will have a profound impact on the practice. While the use of portable devices, e-filing and file share applications have created the opportunity to practice outside the confines of a brick and mortar law office, the increasing threat of hackers and security breaches require diligence and appropriate countermeasures. Smart devices and the internet of things (IoT) have multiplied hacking possibilities. Attorneys and their clients must implement appropriate cyber-security countermeasures or risk costly and possibly career ending cyber incidents. Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. Clients and regulators are increasingly demanding that their attorneys develop policies and procedures to protect client information. Cybersecurity is too broad a topic to cover in one paper. This article is an introduction to some of the more prevalent security issues faced by lawyers in protecting their client's information and securing the firm's assets. In addition to offering suggestions on securing client information, it will address the increasing ethical obligations of lawyers to understand technology and plan accordingly.

II. CYBERCRIMINALS ARE AFTER YOUR INFORMATION

As this article goes to press, British Airways just apologized for a "sophisticated, malicious criminal attack" on its website.[1] The breach occurred between August 21 and September 5, 2018. Approximately 380,000 names, email addresses, and credit card information including the CVV numbers of passengers booking flights within the time period were taken. It is unclear how the hackers got into the system, but British Airways claims it does not store CVV numbers (storing CVV is forbidden in EU) so the hack may have been during transmission rather than in the storage of the data. Digital attacks aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes is increasing exponentially.[2] Foreign governments, including North Korea, China, Iran and Russia, have increasingly been the source of security breaches. The FBI and CIA have noted that Russia made systematic attempts to hack US political institutions in 2015 and 2016 and deliberately intervened in the US presidential election through their revelation of hacked emails.[3] There is a new mantra in cybersecurity: "It's when not if", an entity will be hacked.[4] Implementing effective cybersecurity measures is particularly challenging because the sheer number and variety of devices and attackers are becoming more innovative.

The variety and ingenuity of cyberattacks are fascinating and informative; both in the method of the attack and the cost to the victims. Billions of records containing sensitive personal information have been involved in security breaches since early 2005. In 2017 Equifax suffered one of the severest data breaches recorded. Attackers had used a flaw in its website software (a patch was available) to extract the personal information of as many as 145.5 million Americans. The stolen data included names, Social Security numbers, birth dates, addresses and driver's license numbers. The cost to date has been in excess of $314 million. (Equifax had $125 million in cyber insurance). Soft cost losses included the ouster of its security and technology executives as well as CEO. Two employees who traded in the stock after learning of the breach but before public disclosure have been criminally charged. Costs will continue to mount as lawsuits, additional regulatory requirements and lack of public trust take their toll.[5] Recently, one of the most ingenious hacks involved a "smart" internet-connected fish tank located in a Nevada casino. The fish tank had sensors connected to a PC regulating its settings. Through the PC the hackers gained access to other data including the high rollers list and sent it to Finland before the threat was discovered and stopped.[6] Concern over internet connected toys has prompted the FBI to issue a toy warning. Clearly security is a growing business concern.

The WannaCry ransomware made many large corporations, universities and the National Health Service of the United Kingdom want to cry when it was unleashed in May 2017. The ransomware worm infected more than 230,000 computers in more than 150 countries as well as Texas. It particularly affected hospitals and facilities in the United

[1] British Airways boss apologizes for "malicious" data breach. BBC News Sept. 7, 2018. www.bbc.com/news/uk-england-london-45440850

[2] Ponemon Institute Research Report: 2018 Study on Global Megatrends in Cybersecurity, February 2018

[3] Eric Lipton, David Sanger, Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.,* New York Times Dec. 13, 2016.

[4] ABA TechReport 2017. https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security.html

[5] https://www.marketwatch.com/story/equifax-stock-falls-breach-still-sapping-profit-2018-07-25.

[6] Alex Schiffer, *How a fish tank helped hack a casino,* Washington Post, Jul. 21, 2017.

Kingdom, impacting emergency rooms, medical procedures, and general patient care. US officials later publicly acknowledged that the ransomware was a North Korean government project.[7]

Not all hacks are financially motivated. On August 31, 2014, a collection of almost 500 private pictures of several nude celebrities, including Jennifer Lawrence, were posted on the imageboard 4chan, and later posted on websites and social networks such as Reddit and Tumblr. Apple later confirmed that the hackers had obtained the images using a "very targeted attack" on account information, such as passwords, rather than any specific security vulnerability in the iCloud service itself.[8] Hacking is not limited to credit cards and personal identification information.

Hackers are increasingly seeking confidential information that can be transformed into profits. In August 2015, the Securities and Exchange Commission announced fraud charges against two hackers who hacked into newswire services to obtain nonpublic information about corporate earnings announcements and then provided that information to traders who profited by the information. [9] The use of the non-public information garnered the traders over $100 million in profits. It is clear hackers are seeking to profit by non-public information and law firms that have a merger and acquisition practice are prime targets. Attorneys are targeted because their servers hold incredibly valuable information including client intellectual property, medical records, bank information, even government secrets. For hackers looking for information they can monetize, there is no better place to start.

In 2017, DLA Piper suffered a malware attack by the ransomware Petya that left the firm and its employees without phones and emails for three days.[10] In 2016 Cravath, Swaine & Moore and Weil Gotshal & Manges, two of the largest firms in the United States, got caught in a major cybersecurity breach later linked to a $4 million-plus insider-trading scheme.[11] Puckett & Faraj, a Washington-area firm, was hacked in 2012 by activists associated with the group Anonymous, who were angered by the firm's representation of a United States soldier involved in the death of 24 Iraqi civilians. [12]

While the risk of cybercriminals and hackers has increased, some of the most common threats to law firm data security come from attorneys who are sloppy or simply unaware of the risk and measures required to safeguard client information. A firm's records room was once a major source of vulnerability, but technology like smart phones, tablets, laptops and "smart" devices from coffee pots to thermostats have increased points of access into a firm's confidential information. Increasingly clients are demanding their counsel adopt the same strong security measures the client employs. In 2017 the Association of Corporate Counsel developed suggested security measures and controls for outside counsel.[13] The same year, The New York State Department of Financial Services promulgated 17 cybersecurity regulations which apply to regulated entities doing business in New York. [14]

In the increasingly complex area of cybersecurity even the most knowledgeable and well-trained experts cannot rely just on their training and expertise. The time worn trick of a checklist can help secure an attorney's environment and make sure they are prepared in case of a breach. This Article contains a number of helpful lists. Start with a review or an assessment of the current state of security, create a plan and implement it. Prepare a responsive list of actions in case of a breach. From an individual standpoint we all must secure (1) the devices we use, (2) the electronic communications we have, and (3) the storage we employ.

III. CYBERSECUITY FRAMEWORK

The technical details of cybersecurity implementation are beyond the scope of this paper. However, the NIST Cybersecurity Framework can provide context for reviewing and implementing a cybersecurity plan. The National Institute of Standards and Technology (NIST) developed the framework to help identify and mitigate cyber-risks that could potentially affect national and economic security.[15] The Cybersecurity Framework Version 1.1 was released this

---

[7] Tom Bossert, White House Briefing December 19, 2017; https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

[8] Apple – Press Info – Apple Media Advisory". Apple Inc. September 2, 2014

[9] SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases, 2015-163http://www.sec.gov/news/pressrelease/2015-163.html.

[10] Adam Janofsky, DLA Piper CIO on 'Petya' Attack: The Future of the Entire Business Was At Stake, Wall Street Journal, Dec. 18, 2017.

[11] Nicole Hong, Robin Sidel, Hackers Breach Law Firms, Including Cravath and Weil Gotshal, Wall Street Journal March 29, 2016.

[12] Julie Sobowale, *6 major law firm hacks in recent history*, ABA Journal, March 2017. http://www.abajournal.com/magazine/article/law_firm_hacking_history

[13] *See* https://www.acc.com/advocacy/upload/Model-Information-Protection-and-Security-Controls-for-Outside-Counsel-Jan2017.pdf

[14] https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf

[15] A download of the Framework is available at https://www.nist.gov/cyberframework/new-framework

year. Although developed for critical infrastructure such as banks and utilities it is a flexible and technology – neutral document that can be used by an organization of any size or sophistication. Lawyers and executives can use the Framework to assess how their firm or company's cybersecurity practices measure up. Expect courts to also take these standards into account in assessing liability for data and security breaches.[16]

The Framework is made up of three components: The Framework Core, Profiles, and Tiers. These components can be used to conduct a comprehensive review. The main component of the Framework is the Framework Core. The Core presents a variety of cybersecurity related activities and outcomes that are organized into five main groups: Identify, Protect, Detect, Respond and Recover.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

The Chart is a handy list of considerations that attorneys can use as a starting point in developing and implementing cybersecurity policies and procedures. Next we focus on the lawyer's ethical duties in relation to cybersecurity and tips to protect confidential information by securing your data, devices, and communication.

IV. LAWYERS ETHICAL DUTY OF TECHNOLOGY COMPETENCE

In addition to the motivation provided by the onslaught of hackers identified in the media, the American Bar Association's Model Rules of Professional Conduct were updated in 2012 to address the effect of technology upon the legal profession. Model Rule 1.1 Comment [8] provides that a lawyer

> **"should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."**[17] (Emphasis added).

An increasing number of states have imposed the duty of technology competence on lawyers. As the Arizona Bar stated in Opinion 09-04 (Dec. 2009) "[i]t is important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field".

Approximately 31 states have formally adopted the revised comment to Rule 1.1:

- Arizona, effective Jan. 1, 2015.
- Arkansas, approved June 26, 2014, effective immediately.
- Colorado, approved April 6, 2016, effective immediately.

[16] See FTC v. Wyndham Worldwide Corporation, 799 F.3d 236 (3rd Cir. 2015)

[17] ABA Model Rules of Professional Conduct, Rule 1.1, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence.html

- Connecticut, approved June 14, 2013, effective Jan. 1, 2014.
- Delaware, approved Jan. 15, 2013, effective March 1, 2013.
- Florida, approved Sept. 29, 2016, effective Jan. 1, 2017.
- Idaho, approved March 17, 2014, effective July 1, 2014.
- Illinois, approved Oct. 15, 2015, effective Jan. 1, 2016.
- Indiana, approved July 31, 2017, effective Jan. 1, 2018.
- Iowa, approved Oct. 15, 2015, effective Oct. 15, 2015.
- Kansas, approved Jan. 29, 2014, effective March 1, 2014.
- Kentucky, approved Nov. 15, 2017, effective Jan. 1, 2018.
- Massachusetts, approved March 27, 2015, effective July 1, 2015.
- Minnesota, approved Feb. 24, 2015.
- Missouri, approved Sept. 26, 2017, effective immediately.
- Nebraska, adopted June 28, 2017.
- New Hampshire, approved Nov. 10, 2015, effective Jan. 1, 2016.
- New Mexico, approved Nov. 1, 2013 (text of approved rules), effective Dec. 31, 2013.
- New York, adopted on March 28, 2015, by the New York State Bar Association.
- North Carolina, approved July 25, 2014. Note that the phrase adopted by N.C. varies slightly from the Model Rule: "… including the benefits and risks associated with the technology relevant to the lawyer's practice."
- North Dakota, approved Dec. 9, 2015, effective March 1, 2016.
- Ohio, approved Feb. 14, 2015, effective April 1, 2015.
- Oklahoma, approved Sept. 19, 2016, effective immediately.
- Pennsylvania, approved Oct. 22, 2013 (text of approved rules), effective 30 days later.
- Tennessee, adopted March 6, effective immediately.
- Utah, adopted March 3, 2015, effective May 1, 2015.
- Virginia, approved Dec. 17, 2015, effective March 1, 2016.
- Washington, approved June 2, 2016, effective Sept. 1, 2016.
- West Virginia, approved Sept. 29, 2014, effective Jan. 1, 2015.
- Wisconsin, approved July 21, 2016, effective Jan. 1, 2017.
- Wyoming, approved Aug. 5, 2014, effective Oct. 6, 2014.

Florida has taken the additional step of mandating not only tech competence but also mandating technology training. Florida requires that its lawyers complete three hours of CLE every three years in approved technology programs.[18] In April 2018, North Carolina's State Bar Council approved a proposed amendment mandating that one hour of CLE training be devoted to technology training. [19]

V. LAWYERS ETHICAL DUTY OF CONFIDENTIALITY

The duty of confidentiality is one of the foundations of the attorney-client relationship. Changes to ABA Model Rule 1.6 makes it clear that the "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."[20] The accompanying Comment identifies a safe harbor for unauthorized disclosure of confidential information if the lawyer has made "reasonable" efforts to prevent the access or disclosure. A number of factors are listed for consideration in determining the lawyer's reasonableness including:

- sensitivity of the information;
- likelihood of disclosure if additional safeguards are not employed;
- cost of employing additional safeguards;
- difficulty of implementing the safeguards;
- and the extent to which the safeguards adversely affect the lawyer's ability to represent clients.[21]

[18] https://www.floridabar.org/member/cle/cler-bscr-rules/

[19] Jason Tashea, North Carolina bar to propose mandatory technology CLE credit, ABA Journal, May 21, 2018. http://www.abajournal.com/news/article/north_carolina_bar_to_propose_mandatory_technology_cle_credit

[20] MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2016)

[21] ABA Model Rules at www.americanbar.org/contentdam/aba/administrative/ethics_2020/20120808 _house_ action_ compilation_redline_ 105a-f.authcheckdam.pdf.

The Commission examined the possibility of offering more guidance about specific measures lawyers should use, but decided technology changes rapidly and the corresponding measures lawyers should take will change with the advances in technology. According to the Commission, its "proposals are designed to help lawyers understand these risks so that they can take appropriate and reasonable measures when taking advantage of technology's many benefits."[22]

With the increasing risks associated with hacks and data loss there was a need to focus on what constitutes "reasonable efforts" to prevent inadvertent or unauthorized disclosure of, or unauthorized access to information relating to the representation of a client. The Standing Committee on Ethics and Professional Responsibility of the ABA concluded that adopting the language in the ABA Cybersecurity Handbook would illuminate the reasonable efforts standard:

> . . . rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts 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.[23]

A. Communicating with Clients: ABA Guidelines

Confidential information of clients is often hacked through email servers during the transmission of confidential information. In 1999, a good 5 years before the rise of the smart phone, the ABA issued formal opinion 99-413 that permitted a lawyer to transmit information relating to the representation of a client by unencrypted e-mail without violating the Model Rules of Professional Conduct because that mode of transmission afforded a reasonable expectation of privacy from a technological and legal standpoint. Recently the Committee recognized that updating was necessary. In May 2017, the ABA released its Formal Opinion 477R relating to secure communications with clients:

> A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

The opinion does not require encryption for all communications with attorneys. However, electronic communications through mobile applications or via unsecured networks may lack basic expectation of privacy afforded to email communications. Lawyers must, therefore, constantly analyze how they communicate electronically about client matters applying the Comment [18] factors to determine what is reasonable. In conjunction with its Opinion 477R the Committee provides common sense guidance.

[22] ABA Comm'n on Ethics 20/20, *Revised Draft Resolutions for Comment—Technology and Confidentiality*, Feb. 21, 2012, *available at* http://www.americanbar.org/content/dam/ aba/administrative/ethics_2020/20120508_ethics _20_20_final_resolution_and_report_technology_and_confidentiality_posting.authcheckdam.pdf.

[23] ABA CYBERSECURITY HANDBOOK, supra note 3, at 48-49.

Tips on Securing Client Communications

1. Understand the Nature of the Threat.
2. Understand How Client Confidential Information is Transmitted and Where It Is Stored.
3. Understand and Use Reasonable Electronic Security Measures.
4. Determine How Electronic Communications About Clients Matters Should Be Protected.
5. Label Client Confidential Information.
6. Train Lawyers and Nonlawyer Assistants in Technology and Information Security.
7. Conduct Due Diligence on Vendors Providing Communication Technology.

1. Understand the Nature of the Threat

There is a correlation between security threats and the value of the information; the more valuable the information, the higher the threat level. The lawyer must assess the risk when developing a security plan. Client information in areas such as "industrial designs, mergers and acquisitions or trade secrets, and industries like healthcare, banking, defense or education," may present a higher risk of data theft and greater effort at protection is warranted.[24]

2. Understand How Client Confidential Information is Transmitted and Where It Is Stored.

A lawyer should understand how their firm's communications are created, where client data resides, and how the information may be accessed. Every access point is a potential entry point for hackers. This is a complicated task in an environment where communications take place on multiple devices and data may be stored in multiple locations. Each access point, and each device, should be evaluated for security compliance.

3. Understand and Use Reasonable Electronic Security Measures.

Lawyers must make reasonable efforts to prevent inadvertent or unauthorized disclosure of or access to information relating to client representation. Making reasonable efforts "includes analysis of security measures applied to both disclosure and access to a law firms technology system and transmissions."[25] More specifically efforts could include security measures including using secure Wi-Fi, or a Virtual Private Network (VPN) in addition to "using unique complex passwords, changed periodically, implementing firewalls and anti-Malware/AntiSpyWare/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software."[26] Employing methods to remotely disable lost or stolen devices and destroy the data contained in those devices may be reasonable. Finally, encryption should be considered: "A lawyer should consider whether certain data should ever be stored in an unencrypted environment, or electronically transmitted at all". [27]

4. Determine How Electronic Communications About Clients Matters Should Be Protected.

Attorneys should have discussions with their clients at the beginning of their relationship about the level of security that will be necessary for communication. Communications to third parties containing protected client information requires analysis to determine what degree of protection is appropriate. If client information is of sufficient sensitivity, a lawyer should encrypt the transmission and determine how to do so to sufficiently protect it, and consider the use of password protection for any attachments.[28]Alternatively, lawyers can consider the use of a vetted and secure third-party cloud - based system to share and exchange documents normally attached to emails. Communicating with a client who uses computers or other devices subject to the access or control of a third party such as an employer or

[24] ABA Formal Opinion 477R
[25] Id.
[26] Id.
[27] Id.
[28] See Cal. Formal Op. 2010-179 (2010); ABA CYBERSECURITY HANDBOOK, supra note 3, at 121. Indeed, certain laws and regulations require encryption in certain situations. Id. at 58-59.

spouse presents special problems and likely will require other modes of communication. The client should always be cautioned about the risk of sending or receiving electronic communications using a computer or other device, or email account, to which a third party has, or may gain, access.[29] Depending on the sophistication and access a client has alternative non-electronic communications might be the most appropriate.

5. Label Client Confidential Information.

Privileged and confidential communications with clients should be marked as "privileged and confidential" to alert any inadvertent recipients that the information is intended to be privileged and confidential. In *Veteran Med. Prods. v. Bionix Dev. Corp.*, Case No. 1:05-cv-655, 2008 WL 696546 at *8, 2008 BL 51876 at *8 (W.D. Mich. Mar. 13, 2008), the following disclaimer (together with a confidentiality agreement) was sufficient to constitute a reasonable effort to maintain confidentiality.

> [T] his and any files transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient or the person responsible for delivering this email to the intended recipient, be advised that you have received this email in error and that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you have received this email in error, please notify me immediately.

Use of such a disclaimer may obligate the lawyer who receives such a missive to promptly notify the sending lawyer. *See* Model Rule 4.4(b). (requiring the return of inadvertently transmitted communications).

6. Train Lawyers and Nonlawyer Assistants in Technology and Information Security.

Because security breaches often occur through human error, it is critical that attorneys and their staff have periodic training. Policies and procedures for handling confidential and sensitive information and secure electronic communication must be established. Once established, vigilance is required to ensure that the policies are being followed. *See* Model Rule 5.1 (reasonable efforts to ensure that all lawyers conform to the Rules of Professional Conduct). *See* Model Rule 5.3 (conduct of nonlawyer assistants must be compatible with ethical duties of lawyers).

7. Conduct Due Diligence on Vendors Providing Communication Technology.

Cybersecurity issues are becoming more complex and are often beyond the expertise of a practicing lawyer. Outsourcing security, storage, communication, and information technology needs is often the best solution for law firms. Assistance from other lawyers or outside vendors may be necessary to evaluate the vendors. ABA Formal Opinion 08-451 identifies several factors to consider when selecting the outsource vendor, to meet the due diligence and duty of supervision obligations. Such factors may include:

- reference checks and 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 adversity; and
- the availability and accessibility of a legal forum for legal relief for violations of the vendor agreement.

After the issuance of ABA Opinion 08-451, Comment [3] to Model Rule 5.3 was added to address outsourcing, including "using an Internet-based service to store client information." This storage often takes place in the cloud which will be discussed in more detail below. Comment [3] provides that the "reasonable efforts" to ensure that the nonlawyer's services are provided in a manner that is compatible with the lawyer's professional obligations "will depend upon the circumstances." Comment [3] contains suggested factors that might be considered:

- the education, experience, and reputation of the nonlawyer;
- the nature of the services involved;
- the terms of any arrangements concerning the protection of client information; and

[29] *See* Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) (finding no reasonable expectation of privacy exists where the employer announces he can inspect workplace computers), United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (finding no reasonable expectation of privacy exists where the employer has a policy of auditing employees' computer use and the employee does not assert he was unaware of the policy),

- the legal and ethical environments of the jurisdictions in which the services will be performed particularly with regard to confidentiality.

Comment [3] further provides that when retaining or directing a nonlawyer outside of the firm, lawyers should communicate "directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer." When an attorney retains a non-lawyer outside the firm, there is a responsibility to monitor how the services of the vendor are being performed and that confidentiality is being maintained in the face of changing technology.

Due to the expense and the vast amount of email and data companies must often provide in litigation, clients are increasingly retaining outside vendors to assist in collecting and storing their information. When the client directs the selection of the outside firm, "the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer." MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. [4] (2017). In this situation the lawyer must remain aware of how the nonlawyer's services are being performed.

ABA Opinion 477R and accompanying commentary are a good place to start in assessing a lawyer's ethical duty in securing client communications. Texas also has issued an ethics opinion addressing client communications.

B. Communicating with Clients in Texas

In 2015, the Texas Center for Legal Ethics issued Opinion 648 (2015) that addressed whether a lawyer may communicate confidential information by email.[30] The question arose from lawyers that used unencrypted Gmail to communicate confidential information and who were concerned about hackers and the National Security Agency obtaining their transmissions without a search warrant. In response the Center referenced Rule 1.05(a) of the Texas Disciplinary Rules of Professional Conduct that provides:

> "a lawyer shall not knowingly:
>
> (1) Reveal confidential information of a client or former client to:
>
> (i) a person that the client has instructed is not to receive the information; or
> (ii) anyone else, other than the client, the client's representatives, or the members, associates, or employees of the lawyer's law firm."

According to the Center, whether a lawyer violates the Disciplinary Rules by sending an email with confidential information requires a case by case evaluation. The Center also noted that the concern about sending confidential information by email has been addressed by several ethics committees that have concluded that in general and except in certain special circumstances, the use of email, including unencrypted email is a proper method of communicating confidential information.[31] The Center further notes that "In some circumstances, however, a lawyer should consider whether the confidentiality of the information will be protected if communicated by email and whether it is prudent to use encrypted email or another form of communication."[32]

The examples given by the Center include:

1. communicating highly sensitive or confidential information via email or unencrypted email connections;
2. sending an email to or from an account that the email sender or recipient shares with others;
3. sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client's work email account, especially if the email relates to a client's employment dispute with his employer (see ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011));

[30] http://www.legalethicstexas.com/Ethics-Resources/Opinion/opinion-648.aspx

[31] See, e.g., ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (2018); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011); State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2010-179 (2010); Prof'l Ethics Comm. of the Maine Bd. of Overseers of the Bar, Op. No. 195 (2008); N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 820 (2008); Alaska Bar Ass'n Ethics Comm., Op. 98-2 (1998); D.C. Bar Legal Ethics Comm., Op. 281 (1998); Ill. State Bar Ass'n Advisory Opinion on Prof'l Conduct, Op. 96-10 (1997); State Bar Ass'n of N.D. Ethics Comm., Op. No. 97-09 (1997); S.C. Bar Ethics Advisory Comm., Ethics Advisory Op. 97-08 (1997); Vt. Bar Ass'n, Advisory Ethics Op. No 97-05 (1997).

[32] *Id.*

4. sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;
5. sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
6. sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer's email communication, with or without a warrant.

Certainly, it is appropriate for the attorney to caution the client as to the dangers inherent in sending or accessing emails from computers accessible to persons other than the client. "Additionally, a lawyer's evaluation of his email technology and practices should be ongoing as there may be changes in the risk of interception of email communication over time that would indicate that certain or perhaps all communications should be sent by other means."[33]

The Center's answer on whether you may use unencrypted email to transmit confidential information is "it depends". The answer depends on the facts of each case because a "knowing" disclosure can be based on actual or inferred knowledge. Thus "each lawyer must decide whether he or she has a reasonable expectation that the confidential character of the information will be maintained if the lawyer transmits the information by email".

Based on Ethics Opinion No. 648 it should be standard for attorneys to advise clients on the risks attendant with communication by unencrypted email. Furthermore, as encryption and file sharing become easier, alternatives to using web-based unencrypted email become much more appealing and efficient.

C. To Encrypt or Not to Encrypt Email?

Using unencrypted email for routine or low sensitivity communications may be appropriate, but as ABA Opinion 477R points out, the proliferation of cyberthreats and electronic communication devices together with the sensitivity of information may make the use of encrypted email a better choice. If you have clients that handle HIPAA personal information or financial institution clients you likely are using encrypted email in your communications with them. If you are doing business in New York then encryption of any transmission of Nonpublic Information may be required.[34] If you have clients that do business in Europe you may be required to encrypt emails if they contain personal or sensitive data. Rather than struggling with the type of email to send a client on a case by case basis, the most pragmatic solution for a firm may be to standardize to a communication process that provides a secure, encrypted channel for all case-related communications. Some knowledge of how email and encryption work is helpful in understanding the potential for a security breach.

Unencrypted email is not a secure way to share information. When you send an email, it goes from your device to a server and then passes through a number of servers on its way to the recipient's computer or mobile device. As the email passes through each server a copy of the email is deposited and anyone with access to one of the servers can read it unless the email is encrypted. Email can be intercepted or read while saved on remote servers. "Sending highly confidential or personal information via unencrypted email is like sending a postcard. There are many places that a postcard goes before it reaches its recipient – and can be read by anyone along the way."[35] Those that seek to intercept it include the government. Currently, prosecutors can obtain emails from email providers without alerting the owner of the emails.[36]

Encryption uses a formula to transform readable data into unreadable data. The formula is an algorithm (called a cipher), the readable data is called plaintext, and the unreadable data is called ciphertext. Decryption is the reverse process that uses a key to transform the encrypted data back to readable data. As long as the decryption key is protected, the data is unreadable and secure. Anyone who has access to encrypted data cannot read or use it without access to the decryption key. This may sound complex however, most email programs including Microsoft Outlook, can utilize encryption once the keys are set up. A number of third party vendors work seamlessly with Gmail and other email providers to provide encryption.

Gmail automatically encrypts your incoming and outgoing emails using Transport Layer Security (TLS), but this only works if the email providers of both the sender and the recipient always use TLS. G Suite enterprise users get an extra layer of encryption through S/MIME (Secure/Multipurpose Internet Mail Extensions) support. This supports encryption in transit and automatically encrypts outgoing emails whenever possible. Users can prevent messages from

[33] *Id.*

[34] DYS sec. 500.15

[35] Catherine Reach, *Easy Encryption for Email – Not an Oxymoron.* Slaw, August 12, 2013.

[36] Under the Stored Communicaions Act, prosecutors can obtain emails from third parties with less than the typical probable cause standard required. However, the recent Carpenter v. United States, 138 S.Ct. 2206 (2018) case, which dealt with cell-site records from wireless carriers, may require probable cause for obtaining emails in the future.

being sent or received unless they are S/MIME encrypted or signed, but this only works if both the sender and recipients have it enabled. End-to-end encryption can be added through "Pretty Good Privacy" better known as PGP. The software generates a public key that people can use to send you emails, and a private key that you use to decrypt them. If you want to use basic level Gmail or Yahoo accounts you can incorporate additional encryption by using an add-on like Virtru that sends messages that you can only read and access on the company's encrypted servers. Virtru offers a free basic version and Virtru-Pro by subscription.[37]

According to the 2017 ABA TechSurvey only 36% (up from 26% in 2016) attorneys encrypt their email. Most rely on confidentiality disclaimers on the email to protect the information. Encryption increases based on the size of the firm as shown in the chart below. With increasing pressure from clients and criminals, it is time for more lawyers to move to encryption. Encrypting the resting data in the phone and mobile devices will be addressed below.

Email Encryption by Firm Size	
Solo	24%
2-9 Attorneys	31%
10-49 Attorneys	41%
50-99 Attorneys	48%
100-499 Attorneys	51%
500+ Attorneys	61%

VI. SECURING DATA STORAGE

According to the Framework Core a key component to a cybersecurity program is data security. It includes identifying the location of the data and implementing appropriate security processes. A brief discussion of the location of data and the Federal Trade Commission's recommendations follow. Cloud computing is rapidly evolving. Cloud computing is a broad term that describes any technology that allows end users to store data and applications in shared data centers so they can share and access their data or run applications from any location with an Internet connection. The use of a smart phone or an iPad often involves "cloud computing" through products and services such as Google Drive, Facebook, or Dropbox. Approximately 54.4% of lawyers use online services for removable or external storage.[38]

Cloud providers increasingly offer access to more applications, operating systems and hardware as services.[39] Instead of using a personal computer to create documents and spreadsheets that are saved to the user's hard drive, a user can access Microsoft 365 over the internet and utilize the Microsoft Office tools and data protection controls. Applications such as Google Docs permit users to create and share documents and save to Google's server to access later. Data is created, edited, and shared entirely off-site.[40] Because the storage is in the "cloud" and off-site there are some concerns and ethical obligations that arise that will be discussed below.

Despite the ubiquitous nature of the cloud, there is a profound change coming due in large part to the growth of IoT. There is a shift from highly centralized resources and processing in the cloud to a distributed, decentralized architecture called Edge Computing. The "smart" device brings the computation, storage and network closer to the consumer level. This on-device approach helps reduce latency for critical applications, lower dependence on the cloud, and better manage the massive amount of data being generated by the IoT. An example is the Nest Cam IQ indoor security camera, which uses on-device vision processing to watch for motion, distinguish family members, and send alerts only if someone is not recognized or doesn't fit pre-defined parameters. By performing computer vision tasks within the camera, Nest reduces the amount of bandwidth, cloud processing, and cloud storage used versus the alternative of sending raw streams of video over the network. This introduces new complexities in securing data, because now data resides in your firm's and client's IoT. A discussion of IoT reveals additional security concerns.

---

[37] Top Email Encryption Software for 2017 – PCMag 2/14/2018. https://www.pcmag.com/business/directory/email-encryption

[38] *Room at the Top*, ABA Journal, November 2013 at p. 28.

[39] Alberto G. Araiza, Comment, *Electronic Discovery in the Cloud*, 2011 DUKE L. & TECH. REV. 8 (2011).

[40] *See* William Jeremy Robison, Note, *Free At What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1209–12 (2010).

A. The Internet of Things (IoT)

The installed base of hard-to-secure smart things, such as TVs, fridges, and security cameras, is expected to grow 31 percent this year to reach 8.4 billion devices, or around a billion more than the world's total population. [41] Consumer applications include connected entertainment, car, and smart home devices such as washer/dryers, refrigerators/freezers, ovens, robotic vacuums, heating systems, or air purifiers that use Wi-Fi for remote monitoring. Fitbit or Apple Watch, and medical device technologies contain significant personal data (including food consumption, exercise, sleep, physical states such as heart rate, mood, arousal, blood oxygen levels, and mental or physical performance). Automobiles now have built-in, computer-connected sensors that tell the operator to brake or get back into his or her lane, and we are not far from the day when highways will be filled with self-driving vehicles requiring minimal operator input. Industry IoT include oil field monitoring, connected road and signals, and wind turbines. Data is collected and processed in real time on the device but it also forwards refined data to the customer, or some other entity. If the information is confidential, the device and its data must be secured.

Unsecured IoT account for a number of security breaches. Simple factory resets, hardcoded passwords and easy-to-crack stock access credentials enable attackers to infiltrate IoT products. In many cases, users aren't even aware they've been compromised. In terms of IoT, the data on the device is of little importance, it is the ability to connect to a network or its usefulness as part of a distributed denial of service (DDoS) attack that is important to hackers.

Within the last few years a massive network of hacked devices was used to shut down Twitter and other websites. The increasing interconnectedness of our devices was examined by the FTC in their report *The Internet of Things – Privacy and Security in a Connected World* that discussed the privacy and security implications of internet-connected cars, appliances, health monitors, cameras, and other devices.[42] Despite the increasing use of Edge Computing on IoT devices, cloud storage and services are increasingly being used by attorneys.

B. Cloud Storage and Services

Cloud computing offers many advantages such as cost-efficiency, flexibility and scalability. Despite the numerous benefits that can be realized from migrating "into the cloud," some law firms remain reluctant to do so. Security, reliability, availability, and control over their own data are major concerns. According to the American Bar Association's 2017 Legal Technology Survey report, the many benefits of cloud computing have finally convinced the majority of lawyers to make the move to the cloud. This year's survey shows that after remaining stagnant at ~30% from 2013-15, and then increasing to 38% in 2016, there was a marked increase to 52% in the number of lawyers using cloud computing in 2017. [43] The 2017 Legal Technology Survey Report noted that attorneys are increasingly using "web-based software service or solution," including Software as a Service (SaaS). In practical terms, cloud computing includes software or services that can be accessed and used over the Internet using a browser (or, more commonly now, a mobile app), where the software itself is not installed locally on the computer being used by the lawyer accessing the service. Another common way to describe cloud services is to refer to "web services" or "hosted services." The data is processed and stored on remote servers rather than on local computers and hard drives.

Lawyers must be particularly aware of the ramifications of "off-site" storage of a client's data, and take appropriate precautions to prevent compromising client confidentiality. Security is the top consideration in choosing whether to move any data or productivity to the cloud. Electronic information storage and dissemination are covered by a myriad of laws and regulations that the attorney must understand before placing client information in the cloud.[44]

Certain categories of information (financial data, health-related information, *etc*.) are subject to specific laws and regulations that may dictate how and to what extent that information can be stored in the cloud. The Fair Credit Reporting Act, the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), Gramm Leach Bliley Act (GLBA), Family Educational Right to Privacy Act (FERPA), and the Federal Information Security Management Act (FISMA) have restrictions relating to data security. For example, HIPAA contains very explicit requirements for the storage of health-related personal information. Many of these legal obligations are non-delegable, meaning that even if the storage of the data is entrusted to a cloud services provider, the ultimate responsibility for compliance with the law rests with the company that "owns" the data.[45] Several states including Texas have additional requirements regarding information stored on the cloud and all states have breach notification

---

[41] Gartner, Inc. is a research and advisory firm providing information-technology-related insight for IT and other business leaders located across the world. https://www.gartner.com/smarterwithgartner/how-iot-impacts-data-and-analytics/

[42] FTC Report Internet of Things, www.ftc.gov/files/documents/reports/federaltrade-commision-staff-rep. January 2015.

[43] ABA Tech Report 2017 Cloud Computing: https://www.americanbar.org/groups/law_practice/publications/techreport/2017/cloud_computing.html

[44] Ryan, *The Uncertain Future: Privacy and Security in Cloud Computing*, 54 Santa Clara L. Rev. 497, 2014

[45] Mick Seals, *HIPAA in the Cloud: Technical Architectures that Render PHI As "Secured,"* SOGETI USA, INC. (October 2011), http://www.us.sogeti.com/what-we-do/PDF/HIPAA-in-the-Cloud-Whitepaper-Sogeti-v1.2.pdf.

laws.[46] Some cloud service providers have begun to specialize in storage of data that is covered by HIPAA, and have received certification of HIPAA compliance as further assurance to their customers that storage of health-related information in their cloud environment is a safe alternative to local storage.[47] As the cloud industry matures, more providers will become specialized in storage of other specific categories of information that are subject to legal or regulatory oversight.

Below is a brief summary of common regulations that may affect the storage and transmission of certain data:

The Act	What it Regulates	Entities Affected
HIPAA (Health Insurance Portability and Accountability Act)	Protects the privacy of individual patients.	Company or office that deals with healthcare data. That includes doctor's offices, insurance companies, business associates, and employers.
Sarbanes Oxley Act	Companies must have systems in place to protect against internal and external data tampering.	U.S. public company boards, management and public accounting firms
Federal Information Security Management Act of 2002 (FISMA)	Mandates that all federal agencies develop a method of protecting the information systems.	All Federal agencies fall under the range of this bill.
Gramm Leach Bliley Act (GLBA)	Financial Institution must protect consumer information they collet and inform consumers of their information sharing practices.	Defines "financial institutions" as: "…companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance."
Family Educational Rights and Privacy Act (FERPA)	Protecting student information.	Any postsecondary institution including universities, academies, colleges, seminaries, technical schools, and vocational schools.
Payment Card Industry Data Security Standard (PCI-DSS)	A set of 12 regulations designed to reduce fraud and protect customer credit card information.	Companies handling credit card information.

[46] The Texas Business & Commerce Code provides:

> Any person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

TEX. BUS. & COM. CODE ANN. § 521.053 (West Supp. 2011); State data Breach Notification Laws, National Conference of State Legislatures: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[47] *See* David Chernicoff, *Will Your Cloud Be HIPAA Compliant?*, ZDNET 2012; http://www.zdnet.com/blog/ datacenter/will-your-cloud-be-hipaa-compliant/1212?tag= search-results-rivers;item2.

C. Responsibility for Data Security in the Cloud

Companies from Amazon to Sony have learned the hard way that a breach in the security of sensitive customer information can have serious repercussions in areas of legal exposure and public relations.[48] The first question you should ask yourself—and the cloud provider you're considering—is: Who is responsible for which aspects of the security of your data? The perceived responsibility for protecting data in the cloud depends greatly on the type of cloud service you are using. In SaaS environments users believe that the cloud provider is primarily responsible for security while in IaaS and PaaS environments security is a shared responsibility.[49]

If your firm is considering offloading its storage to remote servers handled by vendors like Amazon or Rackspace there are a number of considerations to keep in mind. Although the vendor's website often promotes the security of data stored on its servers, the vendor's standard service level agreement usually reveals that the vendor disclaims responsibility and declares security the customer's responsibility.[50] Generally speaking, the cloud service provider is responsible for only the physical security of the datacenter and the server. The customer, on the other hand, is typically responsible for the security of the data stored on the server by, for example, maintaining adequate firewalls, data encryption software, and internal company controls to prevent data breaches from within. While some cloud companies may offer enhanced security services, you should assume that you, the customer, are responsible for all aspects of security other than the data center itself. Even experts can get this wrong.

On June 8, 2017, security researchers discovered a data repository on the Amazon Simple Storage Service (S3) that could be accessed by anyone on the Internet. The repository contained the names, addresses, account details and personal identification numbers (PINs) of up to 14 million Verizon customers. The Amazon account was owned by Nice Systems, a third-party vendor for Verizon. A Nice Systems engineer misconfigured the data repository to allow public access. A few days later, the same team of researchers discovered a similar issue with data compiled on behalf of the Republican National Committee (RNC). In that data leak, a firm called Deep Root Analytics misconfigured a data repository on Amazon S3, exposing the personal information of nearly 200 million American voters. More than 1.1 terabytes of sensitive data, including names, addresses, phone numbers, birthdates, party affiliation and other details, could be downloaded by anyone on the Internet. A class action lawsuit against Deep Root was filed by James McAleer but was subsequently dismissed.

> **TIP:**
> **Cloud service providers may be responsible for the security of their data center infrastructure, but customers are responsible for the data that's stored there.**

If the cloud services provider is responsible for data security, you should make sure the service level agreement provides you (or your client) with plenty of opportunity to verify the efficacy of the provider's security measures. You can also request the right to conduct your own inspection and audit of the provider's security measures—including both data security (where this is the provider's responsibility) and physical security of the facilities that house your company's data. Make sure that your agreement provides you the right to immediate termination in the event that the cloud provider's security measures are found to be materially deficient as a result of one of these audit procedures. You can also attempt to negotiate an indemnification from the provider for any losses or damage to your firm or clients as a result of the security of your data being compromised, as well as a corresponding carve-out from the section of the agreement that limits the cloud provider's liability under the agreement. However, again, this would only apply if the provider were responsible for the security of the data itself. Even where you, the customer, are responsible for the electronic security of your data, you can still ask the cloud provider to take responsibility for any breach of the physical security of the facility where your data is stored. As a practical matter, however, unless you have large storage needs

---

[48] *See* Roland L. Trope & Sarah Jane Hughes, *Red Skies in the Morning—Professional Ethics at the Dawn of Cloud Computing*, 38 WM. MITCHELL L. REV. 111, 181 (2011).

[49] *See* J. McKendrick, *Cloud Computing Improving But StillA Work In Progress Study Says*, Forbes Tech May 12, 2014,http://www.forbes.com/sites/joemckendrick/2014/05/12/cloud-security-improving-but-still-a-work-in-progress-study-says/

[50] *See id.* at 194–95 & n.248 (quoting the "Amazon Services Customer Agreement" and noting that the ultimate responsibility for security rests with the data customer). The Amazon Services Customer Agreement provides that Amazon "will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure." *Amazon Web Services Customer Agreement*, AMAZON WEB SERVICES, http://aws.amazon.com/agreement/ (last updated August 20, 2014). The agreement further provides, "You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content . . . ." *Id.*

it is unrealistic to expect major cloud providers such as Amazon or Rackspace to negotiate terms beyond their standard agreements without an increase in cost.

With Software-as-a-Service (SaaS), the cloud provider maintains the most control, with the customer only sharing responsibility for endpoint security and identity and access management (IAM). This type of service includes law firm management software like Clio, and file sharing like DropBox. You control the access to the account and the security to access and download information. Thus, password security and communication become critical to maintaining security and will be discussed below.

D. Other Important Issues

Relative to data security, other areas of concern for anyone considering cloud storage:

- Geographic Location of Data Storage. Where in the world is your data and what are the privacy and security rules that apply? There are numerous rules and statutes that relate to storing financial, health and education information that require additional security levels. In addition, The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.[51] It applies to all companies processing the personal data of subjects in the EU regardless where the company resides. If a company has European employees, or European clients whose personal information it processes – it needs to be aware of the new rules. The monetary penalty for infractions is substantial.
- Service Quality and Availability. How frequently can you get to your data and, more importantly, what happens if you cannot? Does the Service Level Agreement contain minimum uptime levels?
- Data Retention and Destruction. Will your data be backed up? When you delete your data is it "really" gone?
- Indemnification. If the provider makes a mistake, what is the liability?
- Contract Termination. How do you end the agreement? How do you migrate your data from the provider at the end of the contract? Are there fees associated with migration?

The reality is, however, that cloud computing contracts are often non-negotiable except for the largest customers.

TIPS For Cloud Storage

- Select a suitable provider
- Ensure the provider has technology to withstand any attempt to infiltrate
- Limit data to U.S. or understand consequences
- Take reasonable precautions to back up data and ensure its accessibility
- Implement electronic audit trail procedures to monitor who is accessing the data
- Create a plan to address security breaches
- Retain ownership of the data
- Require notification if the provider is requested to produce data to a third party
- Know the exit strategy if you terminate the agreement so you can obtain your data.
- Get Client Consent

E. Safe Data Security Practices

The FTC has launched an initiative to provide guidance on data security practices called Start with Security: A Guide for Business.[52] It includes 10 lessons, 9 of which are applicable to lawyers that assist companies in learning about data vulnerabilities and how to reduce the risks they pose.

[51] See GDPR Portal: https://www.eugdpr.org/

[52] Start With Security: A Guide for Business, www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business. (last reviewed 9-4-2018)

- **Collect only what is Necessary.** Companies should not collect data that is not needed and hold on to it only as long as it has a legitimate interest to do so.
- **Control Access to Data Sensibly.** Put limits on who can access sensitive information. Not everyone needs unrestricted access to the entire network and all the information in it.
- **Require Secure Passwords and Authentication.** Companies should require strong password practices among their employees. The passwords should be stored securely and not in clear text. Be mindful of backdoors and other means of avoiding password authentication.
- **Store Sensitive Personal Information Securely and Protect it During Transmission.** Companies should protect sensitive information throughout its life cycle including when the information is transmitted to others, downloaded to a laptop or other device or destroyed.
- **Segment Your Network and Monitor Who's Trying to Get In and Out.** Use firewalls to segment networks and limit access between devices on the network and between the network and the Internet. Implement intrusion detection and prevention tools to monitor networks.
- **Secure Remote Access to Your Network.** Employees with remote access rights need antivirus and firewall protection, and limit access to the information and resources necessary.
- **Make Sure Your Service Providers Implement Reasonable Security Measures.** Your security protection obligations include the vendors to whom you provide sensitive information. Make sure the providers have implemented appropriate security measures, including their security requirements in their contracts and monitor providers for compliance.
- **Put Procedures in Place to Keep Your Security Current and Address Vulnerabilities That May Arise.** Security is not a one-time analysis, and companies should be sure to apply security updates to third-party products on their networks and in their products and constantly monitor for new vulnerabilities to existing products.
- **Secure Paper, Physical Media and Devices.** Store and control access to paper files and devices. Laptops that contain sensitive information are vulnerable to theft or loss. Secure destruction of sensitive information is important and requires shredding and appropriate wipe technology.

VII. TEXAS ETHICS OF CLOUD COMPUTING

Having briefly examined the operation of the cloud and issues relating to security, we turn to some of the relevant ethical considerations. The advent of cloud computing, as well as the use of electronic devices such as cell phones that take advantage of cloud services, has raised serious questions concerning the manner in which lawyers and law firms handle client information, and this has been the subject of numerous ethical inquiries throughout the country.[53] A number of states have issued opinions on cloud storage.

All of the state and ABA opinions issued so far, deem the storage of confidential client information in the cloud to be ethical so long as proper precautions are taken by the attorney to assure that the materials remain confidential and they are protected from breaches, loss and other risks.[54] Interestingly, there are a number of requirements that differ among the jurisdictions. Nevada likens storage in the cloud to storage of paper documents in a warehouse and thus a client's consent to such storage was preferable but not required. New Hampshire seems to require consent to storage in the cloud based on the sensitivity of the documents while Massachusetts requires a client's express consent to cloud storage. Alabama requires the attorney to know how the provider will handle security of the stored information including confidentiality and the attorney should stay abreast of pertinent safeguards to be employed in cloud storage. California has a list of factors for an attorney to consider before using a particular form of technology based in part on the attorney's own competence.

Texas has not yet released a formal ethics opinion on the Cloud, but its Opinion 648 (2015) that addresses email provides some insight. Opinion 648 references with approval Opinion 572 (2006) that provides:

> Under the Texas Disciplinary Rules of Professional Conduct, unless the client has instructed otherwise, a lawyer may deliver materials containing privileged information to an independent contractor, such as a copy service, hired by the lawyer in the furtherance of the lawyer's representation of the client if the lawyer

[53] *See* Roland L. Trope & Sarah Jane Hughes, *Red Skies in the Morning—Professional Ethics at the Dawn of Cloud Computing*, 38 WM. MITCHELL L. REV. 111, 144, 161–63 (2011) (reviewing ethics opinions from the New York State Bar, California State Bar, and the American Bar Association). The ABA has a map that keeps track of states issuing ethics opinions at https://www.americanbar.org/groups/departments_offices/legal_tehnology_resources/resources/charts_fyis/cloud-ethics-chart.html.

[54] For an interactive map of cloud ethics opinions go to: www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.

> reasonably expects that the confidential character of the information will be respected by the independent contractor.[55]

Thus, by implication just as a lawyer can hire a copy service to hold client confidential information, the attorney may select a cloud vendor but only if she does due diligence to determine the vendor has adequate security.

An attorney using cloud computing is under the same obligation to maintain client confidentiality as is the attorney who uses on-site document management. While no Texas Disciplinary Rule of Professional Conduct specifically addresses cloud computing, the following, *inter alia*, may be implicated: Rule 1.01 (Competent and Diligent Representation), Rule 1.05 (Confidentiality of Information); Rule 1.14 (Safekeeping Property); and Rule 5.03 (Responsibilities Regarding Non-Lawyer Assistants). [56]

Rule 1.01 requires that "[i]n representing a client, a lawyer shall not . . . neglect a legal matter entrusted to the lawyer. . . . '[N]eglect' signifies inattentiveness involving a conscious disregard for the responsibilities owed to a client or clients."[57] Failing to ensure that a cloud services provider has implemented adequate safeguards to maintain confidentiality may implicate Rule 1.01. Likewise, under Comment 8 to the Rule, a lawyer "should strive to become and remain proficient and competent in the practice of law." As the use of technology increases in the practice of law, lawyers must become knowledgeable about the technology that they and their client's use.

Rule 1.05 states that "a lawyer shall not knowingly . . . reveal confidential information of a client or former client to [anyone] other than the client, the client's representatives, or the members, associates, or employees of the lawyer's firm."[58] However, "A lawyer may reveal confidential information . . . when the lawyer has been expressly authorized to do so in order to carry out the representation [or when] the client consents after consultation."[59] Comments [1]–[5] to Rule 1.05 explain the importance of the confidential relationship... It is vital that a client's personal information or information related to a case is kept private and protected. Comment [1] explains the reasoning behind the confidential attorney-client relationship: "The ethical obligation of the lawyer to protect the confidential information of the client not only facilitates the proper representation of the client but also encourages potential clients to seek early legal assistance."[60]

Rule 1.14 requires that client property should be "appropriately safeguarded." Client property generally includes files, information, and documents, including those existing electronically. Appropriate safeguards will vary depending on the nature and sensitivity of the property.[61] Rule 1.14 provides in relevant part: "A lawyer shall hold . . . property belonging in whole or in part to clients . . . separate from the lawyer's own property." In the days of paper discovery and tangible property, assuring this level of protection for the client's property was a straightforward process. File cabinets and folders maintained the separation among clients and the attorney's personal information. With the move to electronic rather than paper documents and the switch from boxes to the cloud, the separation of attorney and client materials becomes less clear.

Rule 5.03 provides:

> With respect to a nonlawyer employed or retained by or associated with a lawyer: (a) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and (b) a lawyer shall be subject to discipline for the conduct of such a person that would be a violation of these rules if engaged in by a lawyer if: (1) the lawyer orders, encourages, or permits the conduct involved; or (2) the lawyer: (i) is a partner in the law firm in which the person is employed, retained by, or associated with; or is the general counsel of a government agency's legal department in which the person is employed, retained by or associated with; or has direct supervisory authority over such person; and (ii) with knowledge of such misconduct by the nonlawyer knowingly fails to take reasonable remedial action to avoid or mitigate the consequences of that person's misconduct.

---

[55] Tex. Comm. on Prof'l Ethics, Op. 572, 69 TEX. B.J. 793, 794 (2006).

[56] Texas Disciplinary Rules of Professional Conduct (reprinted, Tex. Gov't Code Ann., Tit.2, Subtit.G App. A-1(Tex. State Bar R. Art. X, sec,9 (West)).

[57] Tex. Disciplinary Rules Prof'l Conduct R. 1.01(b), *reprinted in* TEX. GOV'T CODE ANN., tit. 2, subtit. G, app. A (West 2005) (Tex. State Bar R. art. X, § 9).

[58] Tex. Disciplinary Rules Prof'l Conduct R. 1.05(b)(1).

[59] *Id.* R. 1.05(c)(1)–(2).

[60] *Id.* R. 1.05 cmt. 1.

[61] *See* Tex. Disciplinary Rules Prof'l Conduct R. 1.14.

At its essence, cloud computing can be seen as an online form of outsourcing subject to Rule 5.03's governance of the supervision of those who are associated with an attorney. Therefore, a lawyer must make reasonable efforts to ensure that the cloud provider entrusted with confidential client information is competent and trustworthy.

VIII. SECURE THE DEVICES

We have examined the ethical and practical necessity of securing confidential client information in the cloud. The FTC guidelines provide practical ways to reduce the risk of a security breach. We now turn to the devices, that contain data and could provide the means of infiltrating a company network. Laptops and Mobile devices including phones, tablets, e-readers, lap tops and jump drives may contain sensitive client information. Despite the media attention directed to hacking retail operations, perhaps the most widely experienced security breach is caused by owner error and it is the loss of their mobile devices.

A. Protect Against Loss

The single most stolen items in airports are laptops and tablets. Roughly 10 percent of all cell phones (some 30 million) go missing each year. A full 40% of armed robberies include smartphones.[62] Keep your eyes on your devices at all times. Do not leave your device charging outside of your view. Make sure you have a tracking program on and tape a note on the back with your email address or work number. If you cannot locate your phone quickly push the erase button.

B. Encryption

We previously discussed Encryption as it pertains to email. But information stored on devices and hard drives (data at rest) should also be encrypted. All personal computers and mobile devices (the stored data) should be encrypted. Once the device is encrypted, all user-created data is automatically encrypted before committing it to disk. Encryption is enabled on any Apple iOS device (iPad, iPhone) merely by configuring a lock code. The iOS operating system provides full device encryption by setting a PIN or password. Older Android devices need to have encryption enabled through the setting menu. Newer Android models are encrypted by default with a password. There are a variety of specialty thumb drives like IronKey which come preloaded with encryption software. External drives such as Maxtor, WD and Seagate come with disk encryption.

Attorneys' laptops often contain confidential and privileged information of their clients. Encrypting your hard drive will protect you and the information if your laptop falls into the wrong hands, because without the encryption key, the information on the disk is unreadable. If someone steals your laptop and your disk is not encrypted your files can be easily viewed. It doesn't matter that your computer is password - protected, the thief can simply boot to a new operating system or remove the disk and put it in a different computer. Bear in mind, however, disk encryption only secures your computer from attackers that have physical access to your computer. It does not make your computer free from attack over a network. Malicious websites and hackers can still attack you through your web browser. You can also encrypt individual files.

Windows and Mac encryption vary but are not difficult to implement.[63] Remember the key or you will be as locked out as any potential thief. All modern Macs (since about 2003) have a feature called FileVault that encrypts your entire system drive. Just open your Mac's System Preferences, head to Security & Privacy and select the FileVault tab. Click the "Turn On FileVault" button to create a password and begin the encryption process. Store your key in a safe place (not on that computer) in case you ever get locked out.

If you have a Windows laptop, there are options. Some Windows 10 devices come with encryption turned on by default, and you can check this by going to Settings > System > About and scrolling down to "Device Encryption." You'll need to log into Windows with a Microsoft account in order for this feature to work, but if your laptop offers it, it's an easy and free way to protect your data.

If your laptop doesn't support Device Encryption, you can use Windows' other built-in encryption tool: BitLocker. BitLocker is available only on Professional versions of Windows and above but it's easy to set up. Go to Windows' Control Panel > System and Security > Manage BitLocker. Select your operating system drive and click the "Turn On BitLocker" button, following the prompts to create a password that will function as your encryption key. Be sure to store your BitLocker key in a safe place and not on that computer.[64]

There is also a free program called VeraCrypt that can encrypt your entire hard drive, requiring your password when you boot your computer. It's not quite as simple and seamless as Windows' Device Encryption and BitLocker.

---

[62] 11Tips to Safeguard Clients' Digital Information, Jill Fernandez, coloradosupremecourt.com, Winter 2014.

[63] Micah Lee, Encrypting Your Laptop Like You Mean It, April 27, 2015; https://firstlook.org/the intercept/2015/04/27encrypting-laptop-like-mean/

[64] Whitson Gordon, *The One Thing That Protects a Laptop After It's Been Stolen*, NYTimes March 13, 2018.

> TIP: If you encrypt – you must remember your password. It will be impossible for you to access data if you forget your password or key.

C. Tips for Securing Mobile Phones and Tablets

Tablets are increasingly being used in place of the laptop. But their hybrid use as an entertainment device and professional tool create issues with security. Attorneys often store and communicate confidential information using their tablets. You may also access your law firm network using the devoce. But if you use your iPad for a law practice tool, you must keep kids, spouse and neighbors from using it for entertainment. The following are tips to secure your tablet.

- Label your device with your name and a phone number to make it easy to return
- Set a strong passcode. The 4-digit code is inadequate if you use the device out of the office. Create a password with at least 8 characters or enable touch technology.
- Set an idle timeout that will automatically lock the device when not in use
- Keep all software up to date, including the operating system and installed "Apps". Many of the updates include fixes for security bugs. Delete old apps you are not using anymore and turn off the location tracker.
- Turn off WIFI when not using it so it doesn't automatically sign you in to a free but unsafe Wi-Fi.
- Disable Bluetooth for pairing devices when not in use. Hackers can use this easily to enter your phone.
- Obtain your apps only from trusted sources like AppleiTunes store, Google Play or the Amazon App Store for Android.
- Enroll your device in a managed environment if permitted.
- Enroll your device in Find my Phone service.
- Regularly back up data
- Individually password protect client information with an application password.
- Do not let your spouse or your children play with your work tablet or phone.

D. Bring Your Own Device (BYOD)

BYOD was a growing trend until significant security threats lessened the attraction. By allowing employees to use their own devices companies lowered costs and helped employees balance work and life interests and increased their productivity but significant pitfalls including cybersecurity and ediscovery present tough issues. While BYOD may be attractive from a cost standpoint it creates a myriad of problems without strong policies and technology to back it up. The Sedona conference has weighed in on BYOD. [65] Before launching BYOD, an organization should consider the sensitivity of the information that would be accessed or stored on the devices as well as the organization's legal obligations to restrict disclosure or use of the data. For many firms, the security issues are too great. For others, the cost benefit and the ability to build the appropriate infrastructure including technical support weigh in favor of such a program.

IX. SECURE THE COMMUNICATION

New forms of electronic communications such as texting, tweeting, social networking through a myriad of sites, and instant messaging are creating additional challenges to the existing issues with email communications. Not only is it becoming difficult to keep information confidential, there is increasing risk of waiver of attorney – client privileged matter. Clients have new expectations regarding communications with their counsel, and attorneys must keep abreast and manage those expectations. If attorneys don't understand the new modes of communication it will be difficult for them to take the necessary precautions to make sure their communications remain confidential.

A. Secure Email

We previously covered Email and how unencrypted email is not secure. Not surprisingly law firms rely on email more than any other tool to collaborate with clients and third parties. Because of the lack of security, the ABA and

[65] THE SEDONA CONFERENCE COMMENTARY ON BYOD: PRINCIPLES AND GUIDANCE FOR DEVELOPING POLICIES AND MEETING DISCOVERY OBLIGATIONS A Project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1)

other jurisdictions are beginning to question the wisdom of sending confidential information by unencrypted email. As noted previously, several regulations that impose security requirements may require the transmission of confidential information through end to end encryption. To secure your email effectively, you should encrypt three things: the connection from your email provider, your actual email messages; and your stored, cashed, or archived email messages.[66] End to end encryption means that your data is encrypted when it leaves your device and travels through various servers to your intended recipient.

Hacking a communication in transit is just one way to obtain confidential emails. There are at least three ways a hacker can access your email: (1) through a security flaw within the email system that gives the hacker access to messages; (2) through guessing or brute-forcing your password; and (3) the hacker tricks you into voluntarily providing login information through phishing or malware. Phishing occurs on mobile devices as well as office computers and is a major source of security breaches.

1. Phishing

Phishing is a cyber-attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something the recipient wants or needs — a request from their bank, an email from a potential client, or an email from a boss — and to click a link or download an attachment. The attackers pose as a trusted entity of some kind, often a real or plausibly real person, or a client or customer. Generally, phishing's goal is to (1) get you to hand over sensitive information belonging to you or a client or (2) download malware including ransomware. When attackers craft a message designed to appeal to a specific target it is called "spear" phishing. Attackers use LinkedIn, Facebook, and other available information to send emails that look like they come from co-workers or even their boss. [67]

2. Smishing

Text message or SMS phishing—also called "smishing"—occurs when scam artists use deceptive text messages to lure victims into providing their personal or financial information. The scam artists that send smishing messages often impersonate a government agency, bank, or other company to lend legitimacy to their claims. Smishing messages typically seek usernames and passwords, credit and debit card numbers, PINs, or other sensitive information that scam artists can use to commit fraud.

3. Prevention

Tips to avoid phishing and smishing:

- Think before you click. Do not click on links in random emails and instant messages. If it is from a bank or financial institution go their website directly.
- Install an anti-phishing toolbar. Most browsers have this feature and will alert you if you are visiting a known phishing site.
- Stay up to date about new phishing scams.
- Verify a Site's Security – Before submitting information make sure the site's URL begins with "https". Check the site's security certificate. Never download files from suspicious emails or websites.
- Check your online accounts regularly
- Keep your browser up to date
- Use firewalls
- Pop-ups are often phishing attempts, block pop-ups.
- Use antivirus software.
- Never share personal or financially sensitive information over unencrypted email.

B. Using a Secure Client Portal

If encrypting your email is too cumbersome, a less difficult alternative to communicate with your client is through a secure client portal. These are becoming more common in both large and small firms particularly those that deal with HIPAA and GLBA security requirements. The portal is an encrypted location where all communication takes place, rather than using email to send documents and information back and forth. The client portal also eliminates the size limitation inherent in some email systems. To access the portal clients generally must create a user name and password

[66] Eric Geier, PC World, How to Encrypt Your Email, April 25, 2012.

[67] Lehigh University maintains a website that publishes recent phishing examples: https://lts.lehigh.edu/phishing/examples

that will allow them access to all the information relating to their matter.[68] Features of a client portal may include document sharing, bill sharing, task sharing, ease of ending client access and contact retention. Several case management software applications, including Clio and MyCase, already have portals built into the application. Alternatively, the firm could partition a secure portion of its network that permits access to your client. The benefit is that the server is located in your office and not in the cloud. From the client's perspective a portal is easier to navigate and ensures the communication is secure and available 24/7. Both clients and staff will need training on the portal's use.

C. File Sharing

File sharing services allow you to store information on remote servers and access it through the Internet. The communication and files are placed in encrypted cloud storage and that allows third parties or the client to have password-protected access to them. Rather than emailing attachments, the client receives a link to the securely stored data. File sync and share ("FSS") is shorthand for sharing files among multiple users and devices, and synchronizing the shared files to retain file integrity. File sharing is gaining importance in law firms. Approximately 50% of law firms have used free commercial file sharing services to transmit privileged information.[69] One of the most popular services is DropBox[70], free, simple and easy to use. However, free, consumer based file sharing services may not be secure enough for storing confidential information. There are a number of file sharing services that offer more secure and robust services including: DropBox Business, Citrix, Box, EMC and Accellion.

D. HTTP vs. HTTPS

HTTP (hypertext transfer protocol) is the way a Web server communicates with browsers like FireFox. HTTP lets visitors view a site and send information back to the Web server. HTTPS (hypertext transfer protocol secure) is HTTP through a secured connection. Communications through an HTTPS server are encrypted by a secure certificate known as an SSL. The encryption prevents third-parties from eavesdropping on communications to and from the server. It does not guarantee the website is safe to use, it only assures you of the identity of the website based on information provided by the certifying organization. Most organizations are moving to HTTPS in their transactions. You should too.

E. Texting Tips

Issues with client texting:

- Short messages are misconstrued
- Text messages are not secure
- Text messages are not easily preserved
- Text message may encourage constant contact and access to the attorney

Although the ABA and other state ethics commissions have not objected to attorneys' text messaging clients, attorneys should consider carefully whether to use texts to communicate privileged information to clients. The concern includes the ownership of the cell phone to which you are communicating and access to third parties. Does your client have a reasonable expectation of privacy? Although texting can be fast and easy, the most common form of texting, SMS, is not sufficiently secure to use to transmit personal information in the healthcare environment.[71] SMS text messages are sent and stored on servers in plain text and can be intercepted during transit.[72] There are some services that provide a more secure text environment including Signal ad Zip Whip. Although texting clients may be appropriate in some

[68] Donna Seyle, Expand Your Solo or Small Firm Practice Using Client Portals, Law Practice Today, December 2011http://www.americanbar.org/content/dam/aba/publications/law_practice_today/expand-your-solo-or-small-firm-practice-using-client-portals.authcheckdam.pdf.

[69] LexisNexis, Law Firm File Sharing in 2014

[70] DropBox Business has more robust security but there is a charge for the service.

[71] The Joint Commission forbids the use of SMS for the transmission of electronic protected health information under HIPAA regulations.

[72] Nathan Collier, Keep Text Messaging Secure, For the Record Vol 27 No. 3 P. 25, March 2015.

circumstances, save long conversations for some other communication method. Client portals serve as more secure communication sites and will satisfy client needs.

F. Wireless Communications

Wireless networks have become ubiquitous. Coffee shops, hotels, airports, homes and businesses all use wireless (Wi-Fi) networks to enable their laptops and other devices to access the Internet. If the network doesn't have a password, don't use it unless you have a secure VPN (virtual private network). Otherwise, use Skype, or What's App to communicate.

Most of us have wireless routers at home or the office that provides access to the internet. The wireless "router" is connected to a broadband Internet service via a modem that is attached to the cable or telephone network. While

Tips

- Use HTTPS for secure browsing. If you have sensitive data wait until you are at a secure site.
- Use a VPN (virtual private network)
- Turn off wi-fi when you are not using it
- Use what's app or skype to transmit your information
- Turn off automatic wifi

Wi-Fi provides many benefits, unprotected networks can result in unauthorized use and theft of information. Unauthorized users may be able to access your private information, view the transmissions, download your content and infect your devices. There are steps you can take to secure your wireless transmissions.[73] The FCC has published the following guidelines:

1. **Turn Encryption On**
   Turn your wireless router's encryption setting on and use WPA2 encryption. Use a strong wireless network password.
2. **Turn the Firewall On**
   Wireless Routers generally contain built-in firewalls, but are sometimes shipped with the firewall turned off. Make sure the firewall is turned on.
3. **Change the Default Passwords**
   Most wireless routers come with preset passwords for administering the devices settings. Change the router device's password as soon as it is installed.
4. **Change the Default Name of the Network**
   A network's name is known as its SSID (service set identifier). When a computer searches for a wireless network the SSID nearby are displayed. Manufacturers usually give the router a default SSID so it is a good practice to change it.
5. **Turn Network Name Broadcasting Off**
   Wireless routers may broadcast the name of the SSID to the general public. This might be useful for commercial operations that want to offer wireless access to customers but unnecessary for a private network. Turn this feature off.
6. **Use the MAC address Filter**
   Every device that can connect to a Wi-Fi network has a unique ID called the MAC (media access control) address. You can set your wireless network to accept connections only from devices with MAC addresses that the router is set to recognize. Make sure the router activates its MAC address filter to include only your devices.

[73]FCC Guide, Protecting Your Wireless Network, Benefits and Risks of a Wireless Network

In addition to securing home and office networks, remember to turn off "share." Many of us share files, printers, music and data when we are at home. When you are on a public wireless service you must turn off sharing or anyone can access your data.

X. DISPOSAL OF CONFIDENTIAL INFORMATION

Once you upgrade to the next smart phone or tablet, be careful how you dispose of your older version.[74] In Texas, the Texas Information Disposal Act governs the disposal of business records, including electronic records, containing personal identifying information. In a recent study by Deloitte,[75] researchers were able to recover personal email content (30%), corporate email content (15%) on factory-wiped phones. On encrypted devices, recovery was not possible. The lesson: encrypt your device. Do not rely on the factory wipe. Perhaps the best advice is to use a certified vendor for file and data destruction.

There is other data that is retained on devices that you should consider disposing of: When you link your phone to a rental car, make sure you disconnect when you finish and delete the data. Lots of information can be saved when you connect your phone to a car:

- GPS history.
- Device name.
- Address book.
- In-car internet search history.
- Music-streaming login, such as Spotify or Pandora.
- Call log and text messages if you use hands-free calling.
- WiFi identifiers.

The car companies do not delete your information. You should. Go to system settings, or the Bluetooth setup menu, and delete your device from the paired phones list. A more thorough way to clear data is by finding the factory reset option in the menu. Car-rental agencies, and even travel groups, continue to place responsibility on the customer. "AAA advises consumers to disconnect their synced phones upon returning their rental cars and to become familiar with rental car companies' privacy policies,"

XI. TEXAS CYBERSECURITY LEGISLATION

Texas has been at the forefront in addressing cybersecurity and data privacy issues. From its Data Notification statute to the Texas Cybersecurity Act and Cybercrime Act enacted in 2017, a comprehensive approach toward Cybersecurity is emerging. The Texas Cybersecurity Act establishes certain cybersecurity requirements for all state agencies, adds cybersecurity as an element of the sunset review process, creates a cybersecurity council and requires that certain agencies conduct studies and reports related to cybersecurity threats and responses. In addition to the internal requirements for state agencies, Texas institutions of higher education are affected. (Tex. Gov't Code § 2054.517.). They must adopt and implement a policy for websites or mobile applications operated by the institution to ensure that the privacy of individuals and their information is protected. The Open Meetings Act was amended to permit governmental bodies to conduct closed meetings to deliberate network security assessments and issues. (Tex. Gov't Code §551.089.).

The Cybercrime Act is an attempt to clearly define offenses related to cyberattacks including denial of service attacks, ransomware, and intentional deceptive data alteration. The Cybercrime Act creates the offense of "Electronic Access Interference," a third-degree felony. A person commits this offense by intentionally interrupting or suspending access to a computer system or network without the effective consent of the owner. (Tex. Penal Code § 33.022(a-b).) Importantly, the definition of this crime includes a defense to prosecution if the person who took an action described above did so with the intent to facilitate lawful access to a computer network or system for a legitimate law enforcement purpose. (Tex. Penal Code § 33.022(c).) The offense of Electronic Data Tampering applies to a person who intentionally alters data as it transmits between two computers through deception and without a legitimate business purpose; or intentionally introduces ransomware onto a computer network or system through deception and without a legitimate business purpose. (Tex. Penal Code § 33.023(b-c).)

The Student Privacy Act is based on a model student privacy law enacted by several other states. It prohibits the sale or rental of any student's data (Tex. Educ. Code § 32.152), bans targeted advertising to students based upon their use of educational services, and prohibits the use of a student's data to build a student profile for any purpose other than an educational purpose. Educational technology operators are also required to implement and maintain reasonable

[74] See Texas Information Disposal Act Section 72.004, Tex. Bus. & Comm. Code.
[75] www.2.deloitte.com/content/dam/Deloitte/Risk/mobile _device_security_risk.pdf.

security procedures and practices designed to protect student data from unauthorized access, deletion, use, modification, or disclosure. (Tex. Educ. Code § 32.155.) Lastly, an operator must delete student data whenever a school or school district requests that the data be deleted, unless the student or student's parent consents to the operator's continued maintenance of the student's data. (Tex. Educ. Code § 32.156.) The Student Data Privacy Act also specifies for what purposes an operator may use a student's data, which is essentially limited to educational purposes and to improve educational products, but only if no data will be associated with an identifiable student. (Tex. Educ. Code § 32.154.)

XII. RESPONDING TO A DATA BREACH

This section will briefly discuss response plans to data breaches with a focus on Texas notification action. This is just an overview of some of the issues that should be addressed. Once there is a data breach a number of regulations may require notification to a governmental agency and the affected individual. The nature of the data and where it is stored will govern the type of response.

A. FTC Guide

The FTC is at the forefront of data protection for consumers and businesses. Its guide to responding to data breaches: Data Breach Response: A Guide for Business,[76] is a good place to start with an overview of a response plan:

1. Immediate Steps

    a) Fix Vulnerabilities
    b) Assemble a team of experts

        (1) Identify a data forensics team
        (2) Consult with legal counsel

    c) Secure physical areas
    d) Stop additional data loss
    e) Remove improperly posted information from the web
    f) Interview people who discovered the breach
    g) Do not destroy evidence

2. Next Steps

    a) Think about service providers
    b) Check your network segmentation
    c) Work with your forensics experts
    d) Have a communications plan

3. Send Notification

    a) Determine your legal requirements
    b) Notify Law Enforcement
    c) Did the breach involve electronic health information?

        (1) Health breach resources

            a) Notify affected businesses
            b) Notify individuals

[76] Federal Trade Commission, Data Breach Response: A Guide for Business, https://www.ftc.gov/system/files/documents/plainlanguage/pdf-0154_data-breach-response-guide-forbusiness.pdf.

B. Identify Data and Location

We have previously identified a variety of federal regulations that apply to specific industries and data. In addition, all 50 states and 3 territories have data notification rules that may apply to data located in their jurisdictions.[77] Texas has robust notification requirements if the data includes personally identifiable information (PII). If it is personal health information, PHI, then federal HIPAA and HITECH laws as well as state law may be impacted. Customer data from financial institutions would be covered under GLBA. Payment card information is governed by the standards of the Payment Card Industry. Based on the identity of the data and/or its location you may be required to notify federal entities, state governmental entities and agencies and individuals whose information was accessed or stolen. Each state's notification law is different with some requiring disclosure to the state's attorney general while others require pre-notice of a breach which means private companies must provide advance disclosure to their state attorney general or other state agency before notifications are provided to the affected persons. Reviewing all of the states' disclosure laws is beyond the scope of this article. The following is a brief summary of the Texas notification law. [78]

The Texas Identity Theft Enforcement and Protection Act section 521.053 sets forth the notification required following a breach of security of computerized data. Texas Bus. & Comm. Code § 521.053. It provides in part:

> A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made as quickly as possible, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Sensitive personal information is often referred to as "sensitive personal information". Its definition under the Act is specific and includes "an individual's first name or first initial and last name in combination with any one or more of the following items, if the name in the items are not encrypted:" Sec. 521.002 (a)(2). The following items include Social Security number, driver's license number, government-issued identification number or account number or credit or debit card number in combination with code or password that would permit access to the person's financial account. In addition, the items can include an individuals physical or mental records.

The notification requirement is broad. Arguably notification must be made to "any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Sec. 521.053(c). Thus the duty of disclosure extends to non-residents. For persons who conduct business in Texas and own or license computerized data that includes sensitive personal information, the disclosure shall be made as quickly as possible if the information was or is reasonably believed to have been acquired by an unauthorized person, except as required by law enforcement or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Any person who maintains computerized data (non-owner) that includes sensitive personal information shall notify the owner or license holder of the information immediately after discovering the breach, if there is a slight difference in treatment between owners of computerized data and those who maintain computerized data.

C. Penalty

Section 521.151 provides for a civil penalty for failing to comply with the notification requirement of up to $100.00 per individual per day for the delayed time but is not to exceed $250,000 for a single breach. Issues that arise include whether a breach as opposed to an incident has occurred.

---

[77] State data Breach Notification Laws, National Conference of State Legislatures: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx: Baker Hostetler, Data Breach Charts (last visited Sept. 3, 2018); https://www.bakerlaw.com/files/uploads/documents/data%20breach%20documents/data_breach_charts.pdf ;

[78] For a deeper discussion of Texas notification law see Shawn E. Tuma, *Guide to Responding to Data Breach Incidents and Reporting to Law Enforcement and Governmental Regulators*, 16th Annual Advanced in-Houst Counsel, August 17-18, 2017.

D. Additional Guidance

The NIST is at the forefront in developing standards and has created a *Security Incident Handling Guide* that assists organization in establishing computer security incident response capabilities and handling incidents efficiently and effectively. [79] It is extremely helpful and practical in setting up an appropriate response process.[80]

XIII. CONCLUSION

This week, yet again, one of my credit cards was used by someone in Florida despite the fact the card is in my purse and I haven't been to Florida in years. Cyber crooks and hackers are prolific. The purpose of this article, in part, is to sound the alarm that an active and robust cybersecurity plan is required of all attorneys. It is not only an ethical duty, but a smart response to increasing security threats. For most attorneys, retaining a qualified expert may be the easiest way to implement a plan. But individual attorneys must participate and be knowledgeable enough to assess a security plan and actively participate. Don't become a hacker's access point into your client's information.

[79] National Institute of Standards and Technology, Computer Security Incident Handling Guide, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[80] For additional practical guidance on reporting See Shawn E. Tuma, *Guide to Responding to Data Breach Incidents and Reporting to Law Enforcement and Governmental Regulators*, State Bar of Texas 16th Annual Advanced In House Counsel 2017.