PROTECTING CLIENT PRIVACY AND INFORMATION IN THE AGE OF DIVORCE

KENNETH G. RAGGIO
RAGGIO & RAGGIO, PLLC
3316 Oak Grove Avenue
Suite 100
Dallas, Texas 75204
214-880-7500

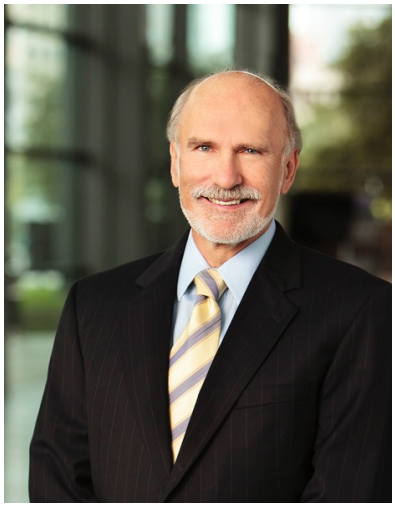
State Bar of Texas
FAMILY LAW TECHNOLOGY 360
December 4-5, 2014
AT&T Executive Education & Conference Center, Austin

CHAPTER 4

Kenneth G. Raggio

RAGGIO & RAGGIO
FAMILY LAW

3316 Oak Grove Avenue
Dallas, Texas 75204
214-880-7500
214-880-7506 Facsimile
www.raggiolaw.com
kenneth@raggiolaw.com



Ken Raggio is a shareholder of the Dallas firm Raggio Family Law and has been a certified Family Law specialist for 35 years. He first presented to the Texas Bar and to the Academy of Matrimonial Lawyers (AAML) on use of technology in family law in 1985 and has continually been in the forefront of applying technology to law practices and trials, including making presentations about technology-assisted opening statements. He was the first lawyer in Texas to use an Ipad to present evidence in a family law case. He most recently presented on the challenges of Electronically Stored Information (ESI) in a family law case to the AAML's 2013 spring meeting, moderated the 2013 Technology Symposium at the AAML's annual meeting, moderated the AAML's webinar on ESI and Ethics of Technology in 2014 and presented at the State Bar's 2012 Technology Conference and to the 2012, 2013, and 2014 Advanced Family Law Courses.

Ken combines his traditional matrimonial practice with resolutions by collaborative law divorce and by mediation when appropriate. He is known to have tremendous command of facts and figures, both in negotiations and in trials.

Ken is as vital in activities outside the courtroom and his law practice as within, winning gold medals in track events at the National Senior Olympics as well as age group wins in major stair climb races such as the Willis (Sears) Tower and the Empire State Building.

Ken practices at the firm with his two brothers, Grier and Tom, both AAML Academy fellows and with other attorneys. They strive to carry on the tradition of excellence, compassion, and professionalism exemplified by the founding members of the firm, the late Louise Raggio and Grier Raggio, Sr. Shareholder Barbara Van Duyne carries on Louise's feminist traditions in the firm.

Ken is a Past Chair of the American Bar Family Law Section and has chaired or vice chaired several committees with the AAML. He was the producer of the first Ultimate Trial Notebook for Family Law seminar while chair of the ABA Family Law Section. He is also a Fellow of the International Academy of Matrimonial Lawyers. He has been named to D Magazine's *Best Lawyers in Dallas* in 2014, and has been perennially listed in *Best Lawyers in America* and as a *Texas SuperLawyer*.

TABLE OF CONTENTS

I. INTRODUCTION

The Bedrock of the attorney client relationship is to protect client privacy and communications. Technology has placed new challenges on this principle.

Inadvertence may expose client – as well as firm data – to a whole world of watchers. This article highlights some perils and how to deal with them.

II. THE RULES

We have mandatory duties to keep client data and communication confidential.

A. The Texas Disciplinary Rules of Professional Conduct 1.05

The Texas Disciplinary Rules of Professional Conduct (Rules) provide that except as otherwise permitted or required, a lawyer shall not knowingly "reveal confidential information of a client or a 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." Confidential information includes both privileged information and unprivileged client information. Unprivileged client information means all information relating to a client, other than privileged information, acquired by the lawyer during the course of or by reason of the representation of the client. Comment 4 related to Rule 1.05 notes that the rule generally extends ethical protection to unprivileged information relating to the client or furnished by the client during the course of or by reason of the representation of the client.

B. Selected Texas Statutes

1. Tex. Bus. & Com. Code § 72.004, Disposal of Business Records Containing Personal Identifying Information: When a business disposes of a business record that contains personal identifying information of a customer of the business, the business shall modify, by shredding, erasing, or other means, the personal identifying information so as to make the information unreadable or undecipherable.

2. Tex. Bus. & Com. Code § 501.052, Privacy Policy Necessary to Require Disclosure of Social Security Number: A person may not require an individual to disclose the individual's social security number (SSN) to obtain goods or services from or enter into a business transaction with the person unless the person (i) adopts a privacy policy; (ii) makes the privacy policy available to the individual; and (iii) maintains under the privacy policy the confidentiality and security of the SSN disclosed to the person.

3. Tex. Bus. & Com. Code § 501.001-.002, Certain Uses of Social Security Numbers Prohibited: All persons and entities, excluding state agencies, are prohibited from (i) intentionally communicating or otherwise making available to the public an individual's social security number (SSN); (ii) displaying an individual's SSN on any card or tag required for the individual to access products or services; (iii) requiring an individual to transmit his or her SSN **over the Internet without encryption or a secure connection**; (iv) requiring an individual to use his or her SSN to access a website (unless a password or similar authentication device is also required); or (v) printing an individual's SSN on any mailed materials unless authorized by state or federal law. (**Bold** emphasis added)

4. Tex. Bus. & Com. Code, Ch. 521, the Texas Identity Theft Enforcement and Protection Act (ITEPA): Requires businesses to (i) implement and maintain reasonable procedures to protect from unlawful use or disclosure any sensitive personal information (SPI) collected or maintained by the business in the regular course of business; (ii) destroy or arrange for the destruction of customer records containing SPI (that are not to be retained) by shredding, erasing or otherwise making the information unreadable or undecipherable. Section 521.053 requires businesses that operate in Texas, and own or license computerized data that includes sensitive personal information, to disclose any breach of its system security (which means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data) to any person whose information was, or is reasonably believed to have been, acquired by an unauthorized person.

5. Texas Health & Safety Code, Chapter 181, the Texas Medical Records Privacy Act applies to health care providers; health plans; entities that process health insurance claims;

and individuals, businesses or organizations which obtain, store or possess protected health information (PHI) as well as their agents, employees and contractors (if they create, receive, obtain use or transmit PHI). Tex. Health & Safety Code § 181.001 (West 2010). In most instances, the Act prohibits these

"covered entities" from using or disclosing PHI without first obtaining an individual's authorization and requires covered entities to provide relevant compliance training for their employees. Tex. Health & Safety Code § 181.101 (West 2010).

Other State statutes deal with HIV and AIDS, but related federal statutes (HIPAA are more comprehensive.

C. Privacy Protection in Court Filings–State Courts

The Texas Supreme Court in Miscellaneous Docket Order No. 09-9153 instructs the Clerk of the Court to post redaction guidelines for electronic briefs and those are available at the court's website. These guidelines do not focus on what information to redact but rather on the process of redaction with the goal of aiding attorneys in preventing the accidental disclosure of information which they intend to redact from electronic briefs submitted to the court for posting on the court's website. The court's website includes the National Security Agency's primer on secure redaction. The approach NSA recommends as the safest approach calls for completely deleting sensitive information in the original word processing document, replacing it with innocuous filler (such as strings of XXes) as needed, and then converting it to a PDF document. The NSA primer also explains how to check for other potentially sensitive information that might be hidden in a document's metadata.
See www.txcourts.gov/media/124902/redactionguidelines.pdf.

Various District Clerks and Courts have adopted other variations for redaction, which has become somewhat more complicated with the integration of efiling into the local courts at various speeds, times, and with various systems.

III. THE COMING RULES–ABA MODEL RULE 1.1

A. ABA Model Rule 1.1 passes by ABA House of Delegates August 2012

Client-Lawyer Relationship
Rule 1.1 Competence

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

Comment 8 reads as follows:

Maintaining Competence

[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with relevant technology**, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (**Bold** Emphasis added)

B. Changing Ethics Rules- Competence in Social Media (North Carolina)

Not surprisingly, states have started to adopt some specific ethical rules dealing with cloud computing and other items dealing specifically with electronic storage or transmission of data. Of particular interest right now is the North Carolina 2014 Formal Ethics Opinion 5 dealing with a duty for the lawyer to counsel with the client about social media.

The opinion states:

"Lawyers must provide competent and diligent representation to clients. Rule 1.1 and Rule 1.3. To the extent relevant and material to a client's legal matter, **competent representation includes knowledge of social media and an understanding of how it will impact the client's case including the client's credibility**. If a client's postings on social media might impact the client's legal matter, the lawyer must advise the client of the legal ramifications of existing postings, future postings, and third party comments. Advice should be given before and after the law suit is filed." (Emphasis added)

The opinion also deals with advising clients on removing social media posts and spoliation:

"..., in general, relevant social media postings must be preserved....

"The lawyer therefore should examine the law on spoliation and obstruction of justice and determine whether removing existing postings would be a violation of the law."

Even though this opinion is from North Carolina, the Ethics opinion may have been prompted by the famous *Allied Concrete Co. v. Lester*, 736 SE 2d 699 (VA 2013).

C. California Ethics Opinion Dealing with ESI and Protection of Client Data.

California has dealt with protecting client confidentiality in a sweeping way in Formal Opinion Interim 11 – 0044. This opinion is in the context were a lawyer (who truly did not understand the breadth of a production request for ESI) agreed to a discovery order requiring production of his client's ESI, and foundout how ineffective a "clawback"of data would be. And how little a Judge wants to get into the middle of a discovery dispute, no matter what the cause. Relevant language includes:

"A fundamental duty of an attorney is '[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client.' [cite omitted] 'Secrets' includes 'information, other than that protected by the attorney-client privilege, that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client.' [cite omitted] Both 'secrets' and 'confidences' are protected communications. [cite omitted] 'A member shall not reveal information protected from disclosure by Business and Professions Code section 6068, subdivision (e)(1) without the informed consent of the client.'

"Similarly, an attorney has a duty to assert the attorney-client privilege to protect confidential communications between the attorney and client which are sought in discovery. [cite omitted] In a civil discovery setting, while the holder of the privilege is not required to take strenuous or 'Herculean efforts' to resist disclosure in order to preserve the privilege, the attorney-client privilege will protect confidential communications between the attorney and client in cases of inadvertent disclosure only if the attorney and client act reasonably to protect that privilege in the first instance. [cite omitted] A lack of reasonable care to protect against the disclosure of privileged and protected information when producing ESI can be deemed a waiver of the attorney-client privilege. See Kilopass Technology Inc. v. Sidense Corp. (N.D. Cal. 2012) 2012 WL 1534065 at *2-3 (attorney-client privilege deemed waived as to privileged documents released through e-discovery because screening procedures employed were unreasonable). [cite omitted]

"Accordingly, the reasonableness of an attorney's actions to ensure both that secrets and confidences, as well as privileged information, of a client remain confidential and that the attorney's handling of a client's information does not result in a waiver of any confidence, privilege, or protection, **is a fundamental part of an attorney's duty of competence**. Cal. State Bar Formal Opn. No. 2010-179. [Emphasis added]

D. Texas cannot be far behind

IV. CHALLENGES OF THE ELECTRONIC WORLD IN FAMILY LAW

A. A Laundry List

A short laundry list of challenges in the electronic world as it deals with our practices and family law and included at least the following:

- e-mail
- tape-recording
- videotape
- GPS and other tracking devices
- shared living quarters
- shared or co-owned vehicles
- a safe with confidential materials in a common habitation
- public wifi networks
- passwords
- forensic backup of computer and cell phone data
- encryption
- hacking
- data mining
- malware
- keystroke loggers
- remote access
- call spoofing
- leaving a computer on when unattended

B. Most information is now Electronic...

An example of how "simple" life was before the information age follows:

A client in a shared habitation only had to have a safe place – – a safety deposit box, or a safe bolted to the floor in the shared residence to protect the letters correspondence document etc. shared or communicated to and from the lawyer. One of the few possible breaches would be the quote other spouse unquote riding off to the safe company, swearing that they lost the code to their safe and getting it from the manufacturer.

Now virtually everything is digital; the "safe" must be expanded to allow for and protect and much wider range of data and information.

C. Email

We now routinely communicate with clients and with others via e-mail. It is wise to get the client written consent to such communications. An example clause from the Raggio and Raggio retainer letter is below:

Electronic mail is the Firm's preferred means of communication and is often more responsive to the client's needs, but may be less secure. Client _____ does [or] ____ does not wish to communicate with Attorney via e-mail, given the risks of inadvertent disclosure of privileged information.

D. "Free" Email-GMail

Gmail "mines" data in Gmail transmissions. If a lawyer chooses to use Google apps for business, there is even more data that Google mines. Please read your license agreement or EULA that you agreed to with Google – – and for that matter – – virtually every other electronic provider of services or software.

Does sending an unencrypted e-mail via Gmail potentially violate the duty to protect client confidences? The latest pronouncement, which may be relevant to a lawyer's duty, favors Google by not allows certification of a Class Action in *In Re Google Gmail Litigation* in US District Court for the Northern District of California.

E. Encryption of e-mail

One common way of dealing with some of the data mining and other issues is to encrypt e-mail as it is sent. Products such as PGP have "public keys" and "private keys" to unlock communications.

F. Virtru to Encrypt Gmail and Yahoo mail

Virtru secures email and attachments with end-to-end encryption, making it easy to send secure email from clients and your contacts. Virtru adds this new feature to Gmail, Yahoo! Mail, and outlook.com. It has other features such as message revoke, disable forwarding, and message expiration.

Virtru layers strong, end-to-end security atop email allowing end-users to send securely without the use of difficult to install encryption software like PGP, or the method within Outlook. Virtru therefore makes secure email accessible to all end-users. Virtru is based on the secured Trusted Document Format, a format used to secure sensitive information and give message senders the ability to control messages even after they have been sent. It is also supposed to work with the latest versions of major email services as well as email clients such as Apple Mail, Microsoft Outlook, Android, and iOS.

Easy email encryption could be the on the list for inclusion in the standard of practice in the foreseeable future.

G. Encryption of data files and documents

Fortunately, Adobe Acrobat Pro allows for the easy encryption of documents. While you wouldn't want to rely on this encryption to send the Coca-Cola secret it is a reasonable way to email documents to clients. WordPerfect and Word also have encryption features.

H. Passwords! Passwords! Passwords!

While the comments below are aimed at us lawyers, they are equally applicable to our clients. Do we need to discuss things like this with our client?

1. Password Retention and Change

The standard is to have different passwords, so that a hack of one password is not a hack into every account that one possesses.

It is not easy or fun to keep up with passwords.

One suggested way is to keep a listing of passwords in a password-protected document, and to keep the password to that document in a secure, hard-to-get-to location. (Like a safety deposit box.) In this manner, the password list can be updated with passwords as they change, or new accounts are added, but the password to open the list remains the same. So in effect the lawyer only needs to retain one password. Make sure it is a complex password – – perhaps using words and spaces– but make sure that those words are outside of the lawyer's, or client's, easily guessed vernacular.

Also, be sure to close the password document if it is your habit to leave your computer on when it is unattended or overnight for remote access to e-mail etc.

There are products – – 1Password for the iPhone is a good example – – that keep track of all your

passwords in a secure environment, requiring you to remember only the one password to access all your accounts.

2. Password Protection

Banks and brokerages have two-stage protection for their financial documents for customers. All of us are aware of the millions of accounts that are regularly hacked.

It is our duty to ensure that our data, including that on the cloud are protected. So protect the data with the passwords and protect the passwords in a secure way.

3. Health & Awareness: Can't Leave Your Data or Emails in an Unprotected State

Absent mindedly leaving your computer on or losing your cell phone can have obvious disastrous results, which may be equally catastrophic as a meltdown of data without a backup.

It is part of our job description at any age to be aware of our surroundings and not inadvertently expose our personal or client data to theft.

Have your IT people put "find my phone" or "lock my computer" software on your appropriate devices so that your negligence in losing a device – – or someone's active theft of a device – – does not operate to your or your client's peril.

Also, "log off" or "log out" when you leave your computer for a little while. This increases security, and doesn't slow you down when you start again.

Protecting your client's data also means taking reasonable steps to insure the trustworthiness of both staff and outside contractors and providers. Most offices require a signed confidentiality agreement for all staff and contractors.

V. CLOUD COMPUTING

A. What Is It?

A **simple definition** of cloud computing is the outsourcing of computer services software platform etc. to be hosted on a contractor servers and managed by the contractor. Cloud computing replaces the system where the lawyers and client data reside on the lawyer's computer or server in the lawyers office, or as the case may be, on the lawyers notebook computer.

A **more complete definition** of cloud computing by the National Institute of Standards and Technology ("NIST") is abbreviated as follows:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics are:
On-demand self-service.
Broad network access..
Resource pooling.
Rapid elasticity.
Measured service.

Service Models:
Software as a Service (SaaS).
Platform as a Service (PaaS).
Infrastructure as a Service (IaaS).

Deployment Models:
Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability

(e.g., cloud bursting for load balancing between clouds).

It is this last part of the NIST definition that affects us in our law practice and in our duties to maintain client privacy. IT is also why perhaps standards of practice for cloud computing are evolving and not set.

B. Texas Ethics Rules 1.05 (d) (1) and 5.03 (a)

Rule 1.05 (d) (1) deals with the fact that confidential information can be released if impliedly authorized by the client to carry out the representation. Rule 5.03 (a) deals with a lawyer responsibility with non-lawyer assistance and the duty to make reasonable efforts to ensure that nonlawyer subordinates and outside contractors conduct is compatible with the lawyers professional obligation.

Texas does not have a specific ethics opinion dealing with cloud computing.

C. Texas Ethics Opinion on Confidentiality and Third Parties

The Supreme Court of Texas Professional Ethics Committee Opinion Number 572, June 2006, addresses the use of an independent contractor, such as a copy service, hired by the lawyer to perform services in connection with the lawyer's representation of the client. The Committee concluded:

> A lawyer's delivery of materials containing privileged information to an independent contractor providing a service, such as copying, to facilitate the lawyer's representation of a client (and not for the purpose of disclosing information to others) does not constitute "revealing" such privileged information within the meaning of Rule 1.05, provided that the lawyer reasonably expects that the independent contractor will not disclose or use such items or their contents except as directed by the lawyer and will otherwise respect the confidential character of the information. In these circumstances, the independent contractor owes a duty of confidentiality both to the lawyer and to the lawyer's client.

Although not explicitly addressed by the Committee, use of independent contractors in the form of Internet- based services would not necessarily constitute revealing of privileged client information. However, attaining a reasonable expectation that Internet-based service providers will neither disclose nor use such privileged information, except as directed by the lawyer, may prove problematic.

D. Other states Cloud ethics opinions.

The American Bar Association has compiled a listing of the various states often very different opinions on cloud computing.
Access this listing at:
http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html .

E. There are real risks from using Cloud computing.

1. Human Error & Dishonesty - this is the single greatest security risk, just as it is outside of the cloud
2. Hacking and leaks through inadequate technical security measures
3. Death of the Delete Key – – data never really goes away
4. Loss of data or of data access – particularly if vendor goes out of business
5. Bring your own cloud ("BYOC") – Accelerating security risks & search impediments

F. Some Developing Trends in State Ethics Opinions

1. Investigation of vendor competence & trustworthiness – at times more thoroughly than any investigation of other outsourcing providers;

2. "Legally enforceable" vendor obligation to preserve confidentiality & make data available back to lawyer;

3. Lawyer's obligations may evolve based on technology developments

G. Some Security & Confidentiality Concerns

1. Geographic location of data servers – Privilege, Fourth Amendment, and other protections available under state & federal law but not under some non-U.S. laws;

2. Control of data and ability to retrieve at end of agreement or in event of bankruptcy or other demise

of provider;

3. Assurance that client data will not be negligently leaked and that you will get immediate notice if a leak is discovered;

4. Service Level Agreements – Guaranteed up-time; Redundancy; Firewall and anti-malware protection

5. Reliable Search and Production from the data base;

6. Assurance that at end of agreement no client data will be retained in backup, archive, or other format.

H. At least one solution.

Austin attorney W. Scott McCullough – while touting the services of his client described below, gave the following explanation on the Computer Law Section Listserv of why his client's Cloud service deals with most of the above issues:

[In response to a series of Cloud based questions]

"You are right to be concerned about where the servers are located. The federal law is unsettled, and state laws are all over the place. The federal government recently succeeded in securing an order requiring Microsoft to produce materials held in Ireland (appeal pending) by asserting that the holder (Microsoft) is in the US. I don't think the ECPA has this kind of extraterritorial reach, but so far a magistrate and a federal district judge have disagreed.

"Right now the most secure place in the world (in terms of protections against compelled production) to have your material is Switzerland, using a company without any situs in the US.

"But Texas is the most secure place in the US. While the applicable statutes are still very confusing and hard to penetrate (something we plan to fix this upcoming session; already have a Senate interim committee working), we did manage to amend state law [TX Code Crim Proc 18.02] to strictly require a warrant for all stored content, regardless of length of time it has been stored, whether is in draft form, and without regard to whether has been "opened."

"For those of us who don't want to have to travel abroad if you have a burning desire to go visit the machinery holding our data every once in a while, Texas is where it needs to be.

"You ask about companies. To be fair, I will start with the one I don't represent: Dell. They have two business cloud products. But note they have servers worldwide so might want to specify you require storage in Texas. I've heard good things about them.

...

"A family of recovering attorneys runs a group of Internet companies, with facilities in Austin (and in Houston, several states and over a hundred other countries). The old Texas.net (those of you who started early in dial-up will recall them; they were one of the first in 1995). They now run data centers under the name of Data Foundry (two locations in Austin, opening a new one in Houston soon). But they also have a Swiss-chartered company called Golden Frog that provides secure VPN (VyprVPN), solid encryption (OpenVPN, L2TP, PPTP and their own proprietary Chameleon that is awesome) and encrypted messaging (Cypher). See http://www.goldenfrog.com/vyprvpn. Their storage product is called Dump Truck. See http://www.goldenfrog.com/duptruck. They do not data mine. They contractually promise to never inspect. Their storage encryption lets you control your own key. I can't be very specific about particulars, but will say that they are very protective of user information and take every effort to not disclose or produce unless and until solid-lock compelled to do so. And if your stored information is encrypted with user-key only anything that is produced is gibberish, especially is the user locally encrypted first. I've been in their data centers many times, and they are beyond first class."

VI. THE NELSON-SIMEK PRACTICAL SECURITY TIPS

In their article, Preventing Law Firm Data Breaches, Nelson and Simek discussed security basics that every lawyer should know, including:

- Have a strong password of at least 12 characters. A strong 12-character password takes roughly 17 years to crack.
- Don't use the same password everywhere.
- Change your passwords regularly.
- Do not have a file named "passwords" on your computer.
- Change the defaults. Whether you are configuring a wireless router or installing a server operating system, make sure you change any default values.
- Laptops should be protected with whole disk encryption; no exceptions.
- Backup media should be encrypted. If you use an online backup service, make sure the data is encrypted in transit and while being stored. Also, be sure that employees of the backup

vendor do not have access to decrypt keys.
- Thumb drives should be encrypted.
- Keep your server in a locked rack in a locked closet or room. Physical security is essential.
- Most smartphones write some amount of data to the phone. Opening a client document may write it to the smart-phone. The iPhone is data rich. Make sure you have a PIN for your phone. This is a fundamental protection. Don't use "swiping" to protect your phone as thieves can discern the swipe the vast majority of the time due to the oils from your fingers. Also make sure that you can wipe the data remotely if you lose your phone.
- Solos and small firms should use a single integrated product to deal with spam, viruses and malware.
- Wireless networks should be set up with the proper security. First and foremost, encryption should be enabled on the wireless device. Whether using Wired Equivalent Privacy (WEP) 128-bit or WPA encryption, make sure that all communications are secure. WEP is weaker and can be cracked. The only wireless encryption standards that have not been cracked (yet) are WPA with the AES (Advanced Encryption Standard) or WPA2.
- Make sure all critical patches are applied. This may be the job of your IT provider, but too often this is not done.
- If software is no longer being supported, its security may be in jeopardy. Upgrade to a supported version to ensure that it is secure.
- Control access.
- Using cloud providers for software applications is fine, provided that you made reasonable inquiry into their security. Read the terms of service carefully and check your state for current ethics opinions on this subject.
- Be wary of social media applications, as they are now frequently invaded by cybercriminals. Giving another application access to your credentials for Facebook, as an example, could result in your account being hijacked. And even though Facebook now sends all hyperlinks through Websense first (a vast improvement), be wary of clicking on them.
- Consider whether you need cyber insurance to protect against the possible consequences of a breach. Most insurance policies do not cover the cost of investigating a breach, taking remedial steps or notifying those who are affected.
- Dispose of anything that holds data, including a digital copier, securely. For computers, you can use a free product like DBAN to securely wipe the data.
- Use wireless hot spots with great care. Do not enter any credit card information or login credentials prior to seeing the https: in the URL.
- For remote access, use a VPN or other encrypted connection.

See Sharon D. Nelson and John W. Simek, Preventing Law Firm Data Breaches, *Texas Bar Journal*, May 2012, p 364.

VII. SOME MORE TIPS IN CONCLUSION

1. Educate your client from the beginning consultation about vigilance to protect their data and communications.
2. Don't forget to mention their duty not to delete information or social media postings.
3. Get client's written consent to email communications.
4. Suggest that a client do an "audit" or "sweep" of their electronic devices – phones, computers, and even vehicles.
5. Get a grip on passwords, password retention, and password changes.
6. Turn it off when not using it. Or at least log off.
7. Have regular IT audits of your internal data security and backup systems.
8. Encrypt.

The hotlinks work better in the version at www.raggiolaw.com/privacy.pdf

GRIER H. RAGGIO (1988)
LOUISE B. RAGGIO (2011)
THOMAS L. RAGGIO*+
KENNETH G. RAGGIO*+
GRIER H. RAGGIO, JR.*
BARBARA G. VAN DUYNE
JEFFREY T. RAGGIO (2014)

Law Offices of
RAGGIO & RAGGIO, P.L.L.C.
3316 OAK GROVE AVENUE
DALLAS, TEXAS 75204
214/880-7500

FAX: 214/880-7506
Website: http://www.raggiolaw.com

*FELLOW
AMERICAN ACADEMY OF
MATRIMONIAL LAWYERS

+CERTIFIED SPECIALISTS
FAMILY LAW
TEXAS BOARD OF
LEGAL SPECIALIZATION

E-MAIL COMMUNICATION

As you are undoubtedly aware, there is a danger of unintended disclosure of confidential client information when you communicate with us or we communicate with your via e-mail as a result of inadvertent dissemination of e-mails. Thus, our office has developed a policy regarding e-mails, and it is set forth below. After you read the policy, we ask that you check the appropriate box at the end of this letter, sign the acknowledgment and return it to our office.

The e-mail policy of the firm is:

1. No one can guarantee the security of e-mail communications. We do not employ encryption methods. Any use of e-mail is at your own risk.

2. Do not send an e-mail from an address where you do not want a reply to be sent. We assume that, if we receive an e-mail communication from you, it is safe to send a reply message back to that address.

3. Do not rely upon e-mail for urgent matters. Please use the telephone to transmit urgent messages.

4. We may choose to respond to an e-mail received from you by telephone or regular correspondence at our discretion.

5. When the attorney working on your case is in court or unavailable, your e-mails may not be reviewed until the attorney returns to the office. Again, do not rely upon email for urgent matters.

6. You are billed for attorney and/or paralegal time for reviewing and responding to emails.

7. Do not e-mail particularly sensitive, confidential, or potentially embarrassing information. There is a risk, however slight, that your e-mail could be intercepted. There is also a risk that your e-mail could be misdirected, inadvertently disseminated, and read by others.

If you have any questions with regard to the foregoing, do not hesitate to contact our office. Again, we request that you check the appropriate box below and sign the acknowledgment below and return it to our office.

☐ I desire to include e-mail as a method of communication with Raggio & Raggio, P.L.L.C.
My email address is: _____

☐ I decline to communicate with Raggio & Raggio, P.L.L.C., via e-mail.

Dated: _____ Signature: _____

APPENDIX 1