USE OF “NEW AGE” DISCOVERY TOOLS
IN FAMILY LAW CASES

KEVIN T. SEGLER
KoonsFuller, PC
5700 W. Plano Parkway, suite 2200
Plano, Texas 75093
Email: Kevin@KoonsFuller.com

State Bar of Texas
FAMILY LAW 101
July 31, 2016
San Antonio

CHAPTER 3
Kevin T. Segler  
KoonsFuller, PC  
5700 W. Plano Parkway, Suite 2200, Plano, Texas 75093  
P: (972) 769-2727      F: (972) 769-0313  
Kevin@KoonsFuller.com

EDUCATION/LICENSES
B.A., University of Oklahoma, 2006  
J.D., University of Oklahoma College of Law, 2009  
State Bar of Texas, 2009  
Certified Mediator, 2010  
United States District Court, Northern District of Texas, 2010  
Board Certified – Family Law, Texas Board of Legal Specialization, 2014  
United States Supreme Court, 2015

PROFESSIONAL ACTIVITIES
Member, Texas Academy of Family Law Specialists  
Member, Dallas Bar Association  
Member, Dallas Association of Young Lawyers  
Dallas Association of Young Lawyers, Leadership Class, 2011  
Co-Chair, DAYL Social Committee, 2011  
Member, College of the State Bar of Texas, 2013 – Present  
Member, Annette Stewart Inn of Court, 2014 - Present  
Co-Chair, DAYL Assisting Lawyers in Transition Committee, 2015, 2016  
Fellow, DAYL Foundation  
Member, Texas Trial Lawyers Association  
Volunteer Mediator, Dallas County Dispute Resolution Center

LAW RELATED ARTICLES, PUBLICATIONS & PRESENTATIONS
10 Ways to Harness the Power of the PDF, Article, Dallas Bar Association HEADNOTES, Law & Technology Issue, December 2013, Co-Author: Jessica H. Janicek.  
Courtroom Technology, Presentation, Dallas Bar Association Family Law Section Bench Bar Conference, February 2014, Co-Presenter: Austin Jones.  
The UCCJEA, Presentation, North Dallas Bar Association, January 2016 Meeting.  
Marking the Most Effective Case to the Court in the Era of Time Limits, Article, Dallas Bar Association HEADNOTES, Criminal Law/Trial Skills Issue, April 2016.
# TABLE OF CONTENTS

1. SCOPE OF ARTICLE ............................................................................................................................................ 1

2. COMMON ELECTRONIC INFORMATION IN FAMILY LAW CASES .................................................................... 1

3. “NEW AGE” DISCOVERY TOOLS ..................................................................................................................... 1
   a. Consumer Level Tools ...................................................................................................................... 1
   b. Advanced Tools ............................................................................................................................... 2
   c. Appropriate Use of “New Age” Tools ................................................................................................ 3

4. ETHICAL ISSUES - RELEVANT STATUTES AND CASES ............................................................................. 3
   a. Federal Wiretap Act .......................................................................................................................... 3
   b. Texas Wiretap Act ............................................................................................................................ 4
   c. Federal Stored Communications Act ................................................................................................ 4
   d. Texas Stored Communications Act .................................................................................................. 4
   e. Chapter 33 of Texas Penal Code – Computer Crimes ........................................................................ 5
      i. Breach of Computer Security ........................................................................................................... 5
      ii. Online Impersonation ........................................................................................................................ 5
   f. Texas Statutory Civil Claims and Remedies ....................................................................................... 5
   g. Common Law Claim – Invasion of Privacy .......................................................................................... 6
   h. Miscellaneous Torts .......................................................................................................................... 6
   i. Texas Occupations Code – Private Investigators ............................................................................... 7
   j. Spoliation ........................................................................................................................................ 7

5. PRACTICE TIPS .................................................................................................................................................... 8

6. CONCLUSION ....................................................................................................................................................... 9

APPENDIX ................................................................................................................................................................... 11
USE OF “NEW AGE” DISCOVERY TOOLS IN FAMILY LAW CASES

1. SCOPE OF ARTICLE

This article attempts to provide a broad overview of some of the “new age” tools available to obtain, gather, and use electronic information. Further, the article provides a summary of legal and ethical pitfalls that a practitioner should be aware of, and looking out for, when using technology and acquiring, using, and disclosing electronic information.

The purpose of this article is not to provide an in depth analysis of all the legal topics discussed herein. Rather, this article is meant to be a synopsis of potential issues that may arise when dealing with technology and electronic information so as to help the practitioner spot these issues, and address them appropriately, before they become problems. While this article aims to help the practitioner know what issues to look for, the practitioner will certainly need to look outside this article to competently research and analyze those issues.

Many of the legal issues touched on in this paper are extremely complex, nuanced, and important. Each of these issues are (and should be) the subject of other books and articles solely devoted to that particular subject matter. The brief discussions of these various important topics in this article are not intended to minimize their importance and significance. The discussions herein are not, and are not intended to be, comprehensive.

It should be noted that these areas of the law are extraordinarily complex and involve a number of federal and state criminal statutes, civil statutes, and common law claims. The laws and cases related to these issues are also constantly changing and being applied to new sets of facts. Further, each of these laws can potentially overlap and, whether or not a violation exists, can be heavily fact dependent. Ultimately, the practitioner should understand these concepts but conduct a more detailed, case/fact specific, analysis each time these issues arise. In sum, this article is a starting point for practitioners to be able to identify these important issues but, thorough research must be done elsewhere once these issues are spotted.

2. COMMON ELECTRONIC INFORMATION IN FAMILY LAW CASES

As the lives of family law clients become more and more digital, so does the evidence that practitioners use in their cases. Much of the electronic evidence used in family law cases is fairly common and often include:

- Text Messages
- Emails
- Photos
- Videos
- Social Media (Facebook, Twitter, Snapchat, etc.)
- Computer Hard Drives
- Web Browser Histories
- Cell Phone Data/Cell Phone Apps
- iTunes Accounts
- GPS Data
- Web Accounts

Sometimes acquiring and using this information is simple and straight-forward. For instance, having the client take a screenshot of a text message or a social media post.

On the other hand, acquiring and using this information may not be as easy. Particularly, if the electronic information is not in your client’s possession or control. Further, acquiring the electronic information may require expert technical assistance and/or the manner in which you acquire or use the electronic information may create a sticky ethical situation for both the attorney and the client.

3. “NEW AGE” DISCOVERY TOOLS

With the growth of electronic information, and the need to use it as evidence, there has also been a growth in the number of tools available to acquire this information. The tools and software programs available to acquire electronic information are extensive and also range in their level of sophistication from basic, convenient consumer level tools to highly advanced, expert level programs and hardware.

a. Consumer Level Tools

Consumer level tools can be extremely useful for attorneys because they are usually relatively inexpensive and can provide a quick, efficient way to pull electronic information off a mobile device or computer. For example, instead of getting numerous emails with multiple screenshots of a text message conversation from your client, these tools can help you download the entire text message conversation directly to a PDF. Some of these helpful, consumer level tools are:

- **iMazing.** This is a complete iOS management software and works on iPhones, iPads, and iPods. Available on Mac and PC. Gives ability to transfer files between Mac and PC, backup and restore data from devices, create a complete archive of the device, copy, save, and manage iOS data, pictures and videos, extract and save text
messages to text or PDF format. Cost ranges between $34.99 - $64.99.1

• **iBackup Viewer.** This is an iPhone data management and extraction tool. Available on Mac and PC. Gives ability to backup and extract data from iPhones and iCloud backups, including iOS app data and raw data files, create a complete archive of the device, export text messages, WhatsApp messages, photos, videos, etc. to another device and save text messages to PDF format. Cost ranges between free and $39.95 for the Pro version.2

• **iPhone Transfer.** This is an iPhone data management and extraction tool. Available on Mac and PC. Gives ability to transfer files between Mac, PC, and any iOS device, backup and restore data from devices, create a complete archive of the device, copy, save, and manage iOS data, pictures and videos, extract and save text messages to text or PDF format. Cost is free.3

• **MobileGo.** This is an Android phone data management, extraction, and recovery tool. Available on PC. It allows you to not only, add, delete, import, export, backup, recover, download, and sync data to your Android device but claims to be able to permanently delete data, transfer content between other devices, and to convert and import video and audio to other devices. Cost is free.4

• **Vibosoft Android Mobile Manager.** This is an Android phone management, extraction, and recovery tool. Available on Mac and PC. It allows you to manage all of the data on your Android phone, use your phone apps through the computer, as well as importing, exporting, backing up, recovering data, and extracting text messages to text format. Cost is $35.95.5

These software programs are merely a few of the many, many similar applications and programs available. A simple internet search will yield numerous results depending on the type of device and operating system. Many of these applications are free but vary in reliability and capability but it is certainly not difficult to find the right application for a reasonable cost.

b. **Advanced Tools**

While the consumer level tools can be very helpful and convenient in a variety of situations, sometimes it is necessary to recover deleted data, sort through complex technical data, collect vast amounts of electronic information, or try to collect electronic information that is not easy to locate or collect. In these situations, some of the more advanced electronic information gathering tools can prove extraordinarily helpful. However, it should be noted that a licensed computer forensics expert should be hired to deploy these tools in a lawful, ethical manner and so that they can testify about how the electronic information was appropriately acquired and prepared for use in the case. Some of these more advanced tools include:

• **Cellebrite.** Cellebrite offers an extraordinary range of hardware and software that can be used to extract and analyze electronic data, even deleted data, from a myriad of mobile electronic devices and cloud services. It is commonly used by law enforcement professionals in criminal investigations. It is a very sophisticated tool and generally a computer forensics expert is needed to properly operate the device and analyze the data provided.6

• **X1.** This is a product suite that includes a variety of products such as X1 Search (which helps search, and obtain data from computers files, network files, emails, attachments, sharepoint data, etc.), and X1 Social Discovery (which can search the internet for social media content for a particular user or users as well as searching through webmail). Not only do these products search through vast amounts of data on computers, networks, and the internet, they are able to retain and save the relevant data discovered in usable formats for court purposes.7

• **Oxygen Forensics.** A package of hardware and software to extract and analyze mobile devices, enterprise computer networks, cloud storage, and computers. It works on a wide range of devices and is able to export data to PDF, text, or spreadsheet format. It can also find passwords to encrypted backups, disable lock screens, and provide common locations of the device users.8

• **EnCase Forensics.** A powerful computer forensics software that provides for a complete imaging of a computer’s hard drive and files, data search and extraction functions, and sophisticated analytical capabilities. It can also create a specific evidence file that

---

1 [www.imazing.com](http://www.imazing.com).
2 [www.imactools.com](http://www.imactools.com).
3 [www.iphone-transfer.wondershare.net](http://www.iphone-transfer.wondershare.net).
4 [www.wondershare.net/ad/mobilego/all.html](http://www.wondershare.net/ad/mobilego/all.html).
6 [www.cellebrite.com](http://www.cellebrite.com).
7 [www.x1.com](http://www.x1.com).
8 [www.oxygen-forensic.com](http://www.oxygen-forensic.com).
Use of “New Age” Discovery Tools in Family Law Cases

Chapter 3

The unfortunate truth is that there are a myriad of state and federal statutes (criminal and civil), state and federal cases (criminal and civil), common law claims and administrative regulations that come into play when trying to determine whether the acquisition, use, or disclosure of electronic information is lawful or not. Many of the statutes involved are very technical and have precise definitions for certain terms and what types of behavior or activities may satisfy those definitions. Moreover, making any generalized assertions about what situations may violate one or more of these laws would be misguided because of strict statutory definitions and the need for a very specific, case-by-case fact analysis.

As such, this article does not provide an in-depth analysis of these laws but merely aims to provide a bird’s-eye-view of the relevant laws that may be applicable in assessing how to acquire, use, and disclose electronic information in a lawful manner. The laws discussed below provide a solid starting point for your assessment but, ultimately, the practitioner will need to analyze further based on the specific set of circumstances in question.

4. ETHICAL ISSUES - RELEVANT STATUTES AND CASES

The unfortunate truth is that there are a myriad of state and federal statutes (criminal and civil), state and federal cases (criminal and civil), common law claims and administrative regulations that come into play when trying to determine whether the acquisition, use, or disclosure of electronic information is lawful or not. Many of the statutes involved are very technical and have precise definitions for certain terms and what types of behavior or activities may satisfy those definitions. Moreover, making any generalized assertions about what situations may violate one or more of these laws would be misguided because of strict statutory definitions and the need for a very specific, case-by-case fact analysis.

As such, this article does not provide an in-depth analysis of these laws but merely aims to provide a bird’s-eye-view of the relevant laws that may be applicable in assessing how to acquire, use, and disclose electronic information in a lawful manner. The laws discussed below provide a solid starting point for your assessment but, ultimately, the practitioner will need to analyze further based on the specific set of circumstances in question.

a. Federal Wiretap Act

The Federal Wiretap Act provides both criminal penalties and civil remedies for the interception, use and disclosure of wire, oral, or electronic communications. First, the Federal Wiretap Act makes it unlawful for a person to intentionally intercept, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communications.

Second, the Federal Wiretap Act makes it unlawful for a person to intentionally disclose, or endeavor to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication.

Third, the Federal Wiretap Act makes it unlawful for a person to intentionally use, or endeavor to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication.

Criminal penalties for violation of the Federal Wiretap Act can range from a fine, to imprisonment for up to five years, or both. Civil remedies for violation of the Federal Wiretap Act can include injunctions, actual damages, statutory damages, punitive damages, and attorney’s fees.
One significant exception to the Federal Wiretap Act is a person is a party to the intercepted communication or a party to an intercepted communication gives prior consent to the interception. The Federal Wiretap Act states that:

“It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception…”

This is often referred to as the “one-party consent” rule. This means that only one party to the communication needs to consent to the interception, even if the person consenting is doing the intercepting. The “one-party consent” rule is the federal rule and it is also the rule in a number of other states, including Texas.17

However, there are still a handful of other states that have an “all-party consent” rule, which means that all parties to a communication must give consent. It is important to note that when a communication crosses state lines, the state with the more restrictive rule applies.

Also, there is no exception for spouses under the Federal Wiretap Act (or under the Texas Wiretap Act).18 The simple fact that people are married does not permit a person to intercept their spouse’s communications that would otherwise be a violation of the Federal Wiretap Act.

b. Texas Wiretap Act

The Texas Wiretap Act, a criminal statute, largely tracks the Federal Wiretap Act in prohibiting the interception, use, and disclosure of communications, but with a few notable differences.19

First, the Texas Wiretap Act also makes it unlawful for a person to knowingly or intentionally effect a covert entry for the purpose of intercepting wire, oral, or electronic communications.20

Second, the Texas Wiretap Act makes it unlawful for a person to intentionally use, endeavor to use, or procure any other person to use or endeavor to use any electronic, mechanical, or other devise to intercept any oral communication.21

Third, the Texas Wiretap Act makes it unlawful for a person to intentionally use or endeavor to use the contents of a wire, oral, or electronic communication if the person knows or is reckless about whether the information was obtained through the interception of a wire, oral, or electronic communication.22 Thus, the Texas Wiretap Act does not necessarily require proof that a person has actual knowledge that they were using unlawfully intercepted communications but proof that a person was reckless about their use of the intercepted communications can constitute a violation of the Texas Wiretap Act.

A violation of the Texas Wiretap Act is either a second degree felony or a state jail felony.23

c. Federal Stored Communications Act

The Federal Stored Communications Act (“FSCA”) provides both criminal penalties and civil remedies for unauthorized access to stored communications or exceeding authorized access to stored communications.24

First, the FSCA makes it unlawful to intentionally access, without authorization or in excess of authorization, a facility through which an electronic communication service is provided and to thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such a system.25

Notably, the FSCA differs from the Federal Wiretap Act in that the Federal Wiretap Act focuses on the interception of a communication while in transmission, whereas the FSCA deals with accessing electronic communications that are being stored.26

Criminal penalties for violation of the FSCA can range from a fine, to imprisonment for up to five years or ten years, or both, depending on the purpose of the violation (i.e. if it was malicious, used for commercial gain or advantage, etc.) and whether or not it was a person’s first offense.27 Civil remedies for violation of the FSCA can include administrative discipline, injunctions, actual damages, statutory damages, punitive damages, and attorney’s fees.28

d. Texas Stored Communications Act

The Texas Stored Communications Act (“TSCA”), a criminal statute, is largely the same as the Federal Stored Communications act.29 The TSCA provides for

---

17 See 18 U.S.C. §2511(2)(d); See also Tex. Penal Code §16.02(c)(4)(B).
21 See Tex. Penal Code §16.02(b)(5).
22 See Tex. Penal Code §16.02(b)(3) (emphasis added).
23 See Tex. Penal Code §16.02(f).
criminal penalties ranging from a Class A misdemeanor to a state jail felony (if the offense was committed to obtain a benefit or harm another). 30

e. Chapter 33 of Texas Penal Code – Computer Crimes

Chapter 33 of the Texas Penal Code sets forth a variety of computer crimes under Texas law including “Breach of Computer Security” and “Online Impersonation.” 31

i. Breach of Computer Security

A person commits the offense of “Breach of Computer Security” if a person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner. 32

The criminal penalties for “Breach of Computer Security” range from a Class C misdemeanor to a first degree felony depending on the intent of the breach, the type of information obtained, and the amount of monetary damage caused by the unlawful breach. 33

ii. Online Impersonation

A person commits the offense of “Online Impersonation” if a person, without obtaining the other person’s consent and with the intent to harm, defraud, intimidate, or threaten any person, uses the name or persona of another person:

1) to create a web page on a commercial social networking site or other internet website; or
2) posts or messages on or through a commercial social networking site or other internet website, other than on or through an electronic mail program or message board program. 34

A person also commits the offense of “Online Impersonation” if a person sends an electronic mail, instant message, text message, or similar communication that references a name, domain address, phone number, or other item of identifying information belonging to any person:

1) without obtaining the other person’s consent; and
2) with the intent to cause a recipient of the communication to reasonably believe that the other person authorized or transmitted the communication; and

3) with the intent to harm or defraud any person. 35

The criminal penalties for “Online Impersonation” range from a Class A misdemeanor to a third degree felony. 36

When interpreting the Chapter 33 of the Texas Penal Code it is important to pay attention to the wide variety of statutory definitions set forth in the Chapter 33, particularly in Section 33.01, which provides definitions applicable to all computer crimes listed in the Chapter 33 of the Texas Penal Code. 37

f. Texas Statutory Civil Claims and Remedies

While the Texas Penal Code, in Chapters 16 and 33, sets forth criminal statutes and penalties for unlawful interception of communications, unlawful access of stored communications, and other computer crimes, the Texas Civil Practice & Remedies Code sets forth civil causes of actions for these crimes.

Chapter 123 of the Civil Practice and Remedies Code, the Intercepted Communications Act (“ICA”), provides a civil cause of action for unlawful interception of communications. 38 Chapter 143 of the Civil Practice and Remedies Code, the Harmful Access by Computer Act (“HACA”), provides a civil cause of action for violations of Chapter 33 of the Texas Penal Code. 39

Under the ICA, a party to a communication may sue a person who:

1) intercepts, attempts to intercept, or employs or obtains another to intercept or attempt to intercept the communication;
2) uses or divulges information that he knows or reasonably should know was obtained by interception of the communication; or
3) as a landlord, building operator, or communication common carrier, either personally or through an agent or employee, aids or knowingly permits interception or attempted interception of the communication. 40

The ICA does not apply to a party to a communication if an interception or attempted interception of the communication is authorized by Title 18, United States Code, Section 2516. 41

The remedies available for violations of the ICA can include injunctions, statutory damages of $10,000 for each occurrence, all actual damages in excess of

30 See Tex. Penal Code §16.04(c)-(d).
31 See generally Tex. Penal Code §33.01-07.
32 See Tex. Penal Code §33.02(a).
33 See Tex. Penal Code §33.02(b-2).
34 See Tex. Penal Code §33.07(a).
35 See Tex. Penal Code §33.07(b).
36 See Tex. Penal Code §33.07(c).
37 See Tex. Penal Code §33.01.
$10,000, punitive damages, reasonable attorney’s fees, and costs.42

Under the HACA, a person who is injured or whose property has been injured as a result of a violation under Chapter 33 of the Texas Penal Code has a civil cause of action if the conduct constituting the violation was committed knowingly or intentionally.43

The remedies available for violations of the HACA can include actual damages and reasonable attorney’s fees and costs.44

g. Common Law Claim – Invasion of Privacy

A common law right to privacy exists under Texas law.45 The Texas Constitution also protects personal privacy from unreasonable intrusion.46 Nothing in the Texas Constitution or in Texas common law suggests that the right of privacy is limited to unmarried individuals.47

Texas recognizes several forms of invasion of privacy including intrusion upon a person’s seclusion and public disclosure of private facts.48 The elements of a claim for invasion of privacy by intrusion upon a person’s seclusion are:

1) An intentional intrusion upon the seclusion, solitude or private affairs of another, which
2) Would be highly offensive to a reasonable person.49

The core of this claim is the offense of prying into the private domain of another, not publication of the results of such prying.50 Further, the intrusion must be unjustified or unwarranted.51 This type of invasion of privacy is generally associated with either a physical invasion of a person’s property or eavesdropping on another’s conversation with the aid of wiretaps, microphones, or spying.52 A spouse’s actions, whether personally or through an agent, in making a surreptitious recording of the other spouse, who believes she is in a state of complete privacy, could be an invasion of privacy.53 The videotaping of a person without consent or awareness when there is an expectation of privacy goes beyond the rights of a spouse because it may record private matters, which could later be exposed to the public eye.54 The fact that a recording can be retained, reproduced, and distributed may be considered in determining whether an invasion of privacy occurred.55 Importantly, while the ICA creates a statutory cause of action for an individual whose communications are intercepted in violation of the ICA, there is nothing in the ICA that precludes a common law claim for invasion of privacy for communications not covered by the ICA.56 The right of privacy is a right distinct in itself and not incidental to some other recognized right for breach of which an action for damages will lie.57 A violation of the right is a tort.58

h. Miscellaneous Torts

While not necessarily applicable to all situations, it is possible for a client to open themselves up to a variety of other miscellaneous torts depending on the nature and extent of their acquisition, use, and disclosure of electronic information and communications. For instance, it is possible for a client to open themselves up to the following tort claims:

1) Misappropriation of Trade Secrets;
2) Tortious Interference with Business Relations;
3) Business Disparagement; and
4) Defamation.59

Ultimately, when a person engages in unlawfully obtaining, using, and disclosing electronic information it can trigger a wide range of potential criminal and civil repercussions—both for them and their attorney—depending on the extent and severity of the acquisition, use and disclosure of the information.
i. Texas Occupations Code—Private Investigators

If a client or an attorney hires private investigator (which includes forensic computer experts and investigators) to obtain certain electronic information, it is imperative that the expert be licensed by the Texas Department of Public Safety to perform such work. In addition to creating issues with the potential admissibility of evidence, the person hiring an unlicensed investigator may be subjected to civil or criminal liability.

Under the Texas Occupations Code, a private investigator is, among other things, a person who engages in the business of obtaining or furnishing, or accepts employment to obtain or furnish, information related to the identity, habits, business, occupation, knowledge, efficiency, loyalty, movement, location, affiliations, associations, transactions, acts, reputation, or character of a person. This includes information obtained or furnished through the review and analysis of, and the investigation into the content of, computer-based data. A private investigator is required to obtain a license to operate as a private investigator in the state of Texas.

A person who contracts with or employs a person who is required to hold a license under §1702 of the Texas Occupations Code knowing that the person does not hold the required license, commits a Class A misdemeanor and/or may be assessed a civil penalty in an amount not to exceed $10,000 for each violation.

j. Spoliation

Spoliation, and the preservation of potential valuable and material evidence, is important on two fronts. First, it is important for the client and their attorney to be aware of their duty to preserve potential evidence and avoid liability or sanctions for spoliating evidence. Second, it is important to inform the opposing side of their duty to preserve evidence and to clarify certain items that need to be preserved, particularly if it may not be immediately obvious that certain information may be needed in the case.

A party may be entitled to a remedy for spoliation of evidence when (1) the party destroyed or failed to produce evidence had a duty to preserve it; (2) the party either negligently or intentionally breached that duty by destroying the evidence or rendering it unavailable; and (3) the breach prejudiced the nonspoliating party. Spoliation is an evidentiary concept, not a separate cause of action.

The standard governing the duty to preserve resolves two related inquiries: when the duty is triggered, and the scope of that duty. A duty to preserve arises only when a party knows or reasonably should know that there is a substantial chance that a claim will be filed and that evidence in its possession or control will be material and relevant to that claim. A “substantial chance of litigation” arises when “litigation is more than merely an abstract possibility or unwarranted fear.”

If a party possesses a duty to preserve evidence, it is inherent that a party breaches that duty by failing to exercise reasonable care to do so. Otherwise, the nonspoliating party would have no legitimate reason to seek a spoliation remedy. Spoliation of evidence can occur either when it is due to negligence or intentional acts.

Spoliation is essentially a form of discovery abuse and can be sanctioned as such, under Rule 215 of the Texas Rules of Civil Procedure, by awarding attorney’s fees or costs to the harmed party, exclusion of evidence, striking a party’s pleadings, or even dismissing a party’s claims. Further, the trial court also has discretion to craft other remedies it deems appropriate in light of the particular facts of an individual case, including the submission of a spoliation instruction to the jury. However, the remedy must have a direct relationship to the act of spoliation and may not be excessive. The remedy crafted by the trial court must be proportionate when weighing the culpability of the spoliating party and the prejudice to the nonspoliating party. This logically follows from the remedial purpose undergirding the imposition of a spoliation remedy under Texas law, which is to restore the parties to a

61 See Texas Occupations Code §1702.104(b).
64 See Tex. Occ. Code §1702.381(b).
65 Brookshire Bros., Ltd. v. Aldridge, 438 S.W.3d 9, 19 (Tex. 2014); See also Trevino v. Ortega, 969 S.W.2d 950, 955-58 (Tex. 1998).
66 See Trevino v. Ortega, 969 S.W.2d 950, 952 (Tex. 1998).
67 Brookshire Bros., Ltd. v. Aldridge, 438 S.W.3d 9, 20 (Tex. 2014);
68 Id. (citing Wal-Mart Stores, Inc. v. Johnson, 106 S.W.3d 718, 722 (Tex. 2003)).
69 National Tank Co. v. Brotherton, 851 S.W.2d 193, 204 (Tex. 1993).
70 Brookshire Bros., Ltd. v. Aldridge, 438 S.W.3d 9, 20 (Tex. 2014).
71 Id.
72 See Id.; See also Trevino v. Ortega, 969 S.W.2d 950, 952 (Tex. 1998).
73 Id. at 21.
74 Id.
75 TransAmerican Natural Gas Corp. v. Powell, 811 S.W.2d 913, 917 (Tex. 1991).
rough approximation of their positions if all evidence were available.\textsuperscript{77} The body of federal and state case law, as well as academic articles and writings, in the area of spoliation is extensive. This area of the law has particularly grown in so much as it relates to electronic data. While the intricacies of spoliation law and the duty to preserve electronic data is not within the scope of this particular article, it is briefly discussed herein because:

1) Electronic information is becoming more and more prevalent in everyday life and, thus, is the type of evidence that needs to be preserved for use in court;
2) The various types and categories of electronic information are ever-growing and, to many, can seem very technical and confusing;
3) Handling, storing, and preserving electronic information is different than dealing with paper documents because even the simple act of saving an electronic file to a different device can change the underlying electronic data, thereby potentially destroying pieces of information;
4) It is clear that clients (and opposing parties) have at least some duty to preserve relevant and material information, documents, and data in their case;
5) Attorneys also have a duty not to destroy evidence and, at minimum, advise their client of their duty to take reasonable measures to preserve and safeguard information that may be relevant and material to the case;\textsuperscript{78} and
6) Attorneys should be prudent in taking steps toward ensuring the opposing party is preserving relevant information to protect their ability to represent their client effectively and, if necessary, secure an appropriate remedy for spoliation of evidence.

5. PRACTICE TIPS

When dealing with new age discovery tools, electronic information and advising clients on the same, consider the following practical tips:

a. Provide a spoliation notice letter to YOUR client as soon as you are hired.
b. Send a spoliation letter to the opposing attorney (or party, if unrepresented) as early in the case as possible.
c. Use extreme caution when advising your client on whether or not employing "self-help" methods of acquiring electronic information is appropriate or advisable. At minimum, you should do the following:
   i. Conduct thorough legal research with a focus on what specifically it is your client wants to do and pay very close attention to the statutory language and definitions applicable to any relevant statute.
   ii. Consider other methods you could use to obtain the information that would not involve putting yourself and/or your client in jeopardy.
   iii. Consider whether the methods your client employs to obtain certain information, even if legally above board, may make them look worse in the eyes of the court than then information they may or may not uncover about the other party.
   iv. Consider if and how you would be able to get any information your client acquires into evidence (i.e. is your client going to have to admit to a crime under oath in order to get a text message into evidence?)

d. Consider the use of a third party expert who is licensed and experienced in dealing with electronic information and computer forensics. Using an expert can provide insulation from liability for both you and your client. The following situations are indicative that an expert should be used:
   i. When you need to recover deleted data;
   ii. When you need to recover/access data from the opposing party, or a third party’s, electronic devices;
   iii. When you need a neutral person with specialized knowledge to collect, analyze, and produce electronic evidence;
   iv. When you need an expert to attest to the processes and procedures used to collect, analyze, and produce electronic evidence; and
   v. When you do not know what you are looking for precisely, an expert can assist in reviewing the facts of your case and advise on what to look for and how to move forward.

e. Some situations where an expert may not be necessary are as follows:

\textsuperscript{78} See Id.
i. When you just need an easy and convenient way to get text messages, videos, emails or voicemails off of YOUR client’s device;
ii. When you do not need analytical or technical information or meta-data;
iii. When you do not need to recover “deleted” from an electronic device; or
iv. When you do not need to have a third party testify about or authenticate the electronic information (i.e. your client can generally prove up a text message that they received).

6. CONCLUSION

This article is not—and is not intended to be—an exhaustive or comprehensive discussion of the various laws and potential ethical pitfalls mentioned herein. It is intended to be an overview of new age discovery tools and aid in identifying the potential legal and ethical problems that can arise in using those tools and dealing generally with electronic information. At best, this article is a mere introduction to the enormously intricate and complex laws and ethical issues that a family court practitioner should look out for when advising their clients and handling cases involving the acquisition, use and disclosure of electronic information.

The aim of this article is to help make attorneys aware of potential sticky ethical situations so they can identify them in advance, further analyze the relevant law as it may be applicable in their specific situation, and avoid disciplinary action, civil liability, and criminal penalties.

The author also wishes to thank Robert Heller of CKC Consulting, LLC for his valuable input and consultation in preparing this article.
<table>
<thead>
<tr>
<th>LAW/STATUTE</th>
<th>PROHIBITED ACTIONS</th>
<th>CRIMINAL PENALTIES</th>
<th>CIVIL REMEDIES</th>
</tr>
</thead>
</table>
| **Federal Wiretap Act** (18 USC §2511) | 1) Unlawful for a person to intentionally intercept, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication.  
2) Unlawful for a person to intentionally disclose, or endeavor to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication.  
3) Unlawful for a person to intentionally use, or endeavor to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication. | Fine, Imprisonment for up to 5 years, or both | Injunctions, actual damages, statutory damages, punitive damages, attorney’s fees and costs |
| **Texas Wiretap Act** (Tex. Penal Code §16.02) | Similar to Federal Wiretap Act, but also:  
1) it unlawful for a person to knowingly or intentionally effect a covert entry for the purpose of intercepting wire, oral, or electronic communications.  
2) unlawful for a person to intentionally use or endeavor to use the contents of a wire, oral, or electronic communication if the person knows or is reckless about whether the information was obtained through the interception of a wire, oral, or electronic communication | Second degree felony or state jail felony | N/A (see ICA below) |
<p>| <strong>Federal Stored Communications Act</strong> (18 USC §2701) | Unlawful to intentionally access, without authorization or in excess of authorization, a facility through which an electronic communication service is provided and to thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such a system. | Can range from a fine, to imprisonment for up to five years or ten years, or both, depending on the purpose of the violation | Administrative discipline, injunctions, actual damages, statutory damages, punitive damages, and attorney’s fees |
| <strong>Texas Stored Communications Act</strong> (Tex. Penal Code §16.04) | Similar to Federal Stored Communications Act | Class A misdemeanor or state jail felony | N/A |</p>
<table>
<thead>
<tr>
<th>LAW/STATUTE</th>
<th>PROHIBITED ACTIONS</th>
<th>CRIMINAL PENALTIES</th>
<th>CIVIL REMEDIES</th>
</tr>
</thead>
</table>
| **Texas Computer Crimes (Tex. Penal Code §33)** | **Breach of Computer Security:** if a person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.  
**Online Impersonation:** if a person, without obtaining the other person’s consent and with the intent to harm, defraud, intimidate, or threaten any person, uses the name or persona of another person:  
1) to create a web page on a commercial social networking site or other internet website; or  
2) posts or messages on or through a commercial social networking site or other internet website, other than on or through an electronic mail program or message board program.  
**AND**  
if a person sends an electronic mail, instant message, text message, or similar communication that references a name, domain address, phone number, or other item of identifying information belonging to any person:  
1) without obtaining the other person’s consent;  
2) with the intent to cause a recipient of the communication to reasonably believe that the other person authorized or transmitted the communication; and  
3) with the intent to harm or defraud any person | **Class A misdemeanor to third degree felony** | **N/A (see HACA below)** |
<table>
<thead>
<tr>
<th>LAW/STATUTE</th>
<th>PROHIBITED ACTIONS</th>
<th>CRIMINAL PENALTIES</th>
<th>CIVIL REMEDIES</th>
</tr>
</thead>
</table>
| Texas Intercepted Communications Act ("ICA") (CPRC §123) | Allows civil suit against a person who:  
1) Intercepts, attempts to intercept, or employs or obtains another to intercept or attempt to intercept the communication;  
2) Uses or divulges information that he knows or reasonably should know was obtained by interception of the communication; or  
3) As a landlord, building operator, or communication common carrier, either personally or through an agent or employee, aids or knowingly permits interception or attempted interception of the communication | N/A | Injunctions, statutory damages of $10,000 for each occurrence, all actual damages in excess of $10,000, punitive damages, reasonable attorney’s fees, and costs |
| Texas Harmful Access by Computer Act ("HACA") (CPRC §143) | A person who is injured or whose property has been injured as a result of a violation under Chapter 33 of the Texas Penal Code has a civil cause of action if the conduct constituting the violation was committed knowingly or intentionally | N/A | Actual damages, reasonable attorney's fees and costs |
| Invasion of Privacy (Common Law) | 1) An intentional intrusion upon the seclusion, solitude or private affairs of another, which  
2) Would be highly offensive to a reasonable person | N/A | Damages available for common law torts |
| Hiring Unlicensed Private Investigator (Tex. Occupations Code §1702.04) | Contracting or employing a person who is required to hold a license under §1702 of the Texas Occupations Code knowing that the person does not hold the required license. | Class A misdemeanor | Civil penalty not to exceed $10,000 for each violation |
| Spoliation (Common Law but NOT Independent COA) | Either negligently or intentionally destroying, or failing to preserve, information/evidence material to a case when the party has a duty to preserve the same and this breach prejudiced the nonspoliating party. | N/A | Remedies available under Rule 215 for discovery abuse (attorney’s fees, exclusion of evidence, striking pleadings, dismissal of claims); Jury instruction against spoiliating party; Other proportionate remedies available at discretion of judge depending on circumstances |