USING A COMPUTER FORENSIC EXPERT

Kathryn Murphy

Goranson Bain, PLLC
6900 N. Dallas Parkway, Suite 400
Plano, Texas 75024

Aimee Pingenot

Goranson Bain, PLLC
8150 N. Central Expressway, Suite 1850
Dallas, Texas 75206

R. Lance Fogarty

Protegga LLC
730 East Park Blvd., Suite 210
Plano, TX 75074

December 13, 2012

Family Law Technology Course: No Tech to High Tech in Two Days

Austin, Texas

Table Of Contents

I. INTRODUCTION

As each year passes, people are becoming more technologically advanced and increasingly rely on computers, cell phones and other electronic media. As such, family law practitioners must frequently identify, analyze, and utilize evidence from such media in their cases. Text messages, emails and computer searches commonly become pivotal exhibits in discovery, settlement and trial. However, understanding how to locate and use such evidence is often beyond the scope of the family law practitioner and as such, we must rely on computer forensic experts to not only interpret but also to identify where we may find such critical evidence. This paper focuses on understanding the role computer forensics plays in our practice as well as outlining the developing case law that addresses this issue for clients and attorneys.

II. WHAT IS COMPUTER FORENSICS?

Computer forensics is the identification, preservation, extraction, interpretation and presentation of computer-related evidence. Computer forensics focuses on three different categories of data: active data, latent or ambient data and archival data. Active data consists of the current files on the computer which are still visible in directories and available to applications. Much active data can be easily understood and examined using simple translation techniques such as plain text files, but will more often need to be viewed using a computer program to be useful. Such programs may include email programs or database program like Excel or word processing programs such as Microsoft Word. Active data also includes system data in the recycle bin, history fields, temporary internet directory, system registry files and data caches. Latent or ambient data are deleted files and other data, including memory dumps that may still be retrieved. This data resides on the hard drive or other storage media and slack space. The recovery of latent data is what is most commonly associated with computer forensics. Archival data is data that has been transferred or backed up to secondary media such as zip disks, network servers or CDs.

Computer forensics, where once limited to personal computers, now extends to all manner of electronic devices holding electronically stored information. This includes external hard drives, thumb drives, Ipads, cell phones, and cameras. As technology continues to expand, computer forensics expands and evolves in tandem. Computer forensics also differs from electronic discovery, another burgeoning issue in family law. Electronic discovery addresses the electronically stored information available to litigants, while computer forensics addresses the electronically stored information available to forensic experts.

III. WHAT IS THE ROLE OF COMPUTER FORENSICS IN FAMILY LAW?

If electronic evidence is going to be important to your case, it is often necessary to hire a professional to collect data and information, to properly preserve the data, to analyze the data and to present the data to the Court. A forensic expert can review the data on computer hard drives, cell phones and other electronic equipment. The expert can interpret data on a hard drive and evaluate whether a website was actually visited by the user or the hit simply reflects a popup or some other program placed on the computer without the knowledge of the user. The expert can also help draft the appropriate discovery requests for electronic discovery issues.

Other roles for an expert include reconstructing previously deleted files from a computer hard drive and searching the producing party's system for occurrences of particular terms and phrases. Companies specializing in data retrieval can search and seek all types of data from "deleted" information to broken hard drives. Experts may also assist in electronic searches. This may become particularly useful because when a file is deleted, the operating system simply deletes the reference to the data in the master index for the disk. The data itself remains intact until overwritten by new data. Software tools can be

employed to search the disk for remaining fragments of the deleted file. While a novice may attempt this task, he or she runs the risk of accidentally overwriting the remaining data and losing the validity of such data.

Additionally, the forensic computer expert can testify as to the reliability of the computer, its processes, and the data that is produced by those processes pursuant to TRE 901(b)(9). A forensic computer expert is likely the only witness that can authenticate the data that is located on the computer hard drive. However, even with a testifying computer expert, evidentiary problems may still arise with regard to the internet. A computer expert cannot alleviate the hearsay problem that accompanies any data received over the internet. The expert can authenticate any data as to its presence on the computer but cannot authenticate any data as from an outside source or prove the truth of the matters asserted in the data. The expert also cannot authenticate photographs on the computer for the truth of the matters depicted in the photographs. In *MySpace v. Sanford Wallace dba FreeVegasclubs.com*, 498 F.Supp. 2d 1293(C.D.CA. 2007), an individual who was qualified to testify as an engineer at an aerospace corporation gave no testimony that he had any foundational knowledge of how MySpace operated, other than that MySpace.com users can only send messages to users on their "friends" list. Therefore, the trial court gave no weight to the expert. *See also Burleson v. State*, 802 S.W.2d 429 (Tex. App.—Fort Worth 1991)(Court found programmer was sufficiently qualified to testify as an expert).

IV. HOW TO SELECT A COMPUTER FORENSIC EXPERT?

A common way to locate and hire a computer forensics expert is to ask other lawyers and judges who they have used and would recommend. Even in such situation, it is advisable to contact a professional association for computer forensic examiners such as the High Technology Crime Investigation Association (www.HTCIA.org) to obtain the names of nearby members. The Electronic Evidence Information Center (www.e-evidence.info) is another place to look for information on leading computer forensic practitioners. In addition to merely identifying a potential computer forensic expert, there are numerous factors to consider.

A. Private Investigations Licensure

In Texas, a forensic expert must be a licensed private investigator. If a company engages in the business of securing, or accepts employment to secure, evidence for use before a court, that company is required to have a Private Investigator's License, according to Texas Occupations Code § 1702.104. The code specifically states:

INVESTIGATIONS COMPANY. (a) A person acts as an investigations company for the purposes of this chapter if the person:

(1) engages in the business of obtaining or furnishing, or accepts employment to obtain or furnish, information related to:

(A) crime or wrongs done or threatened against a person, state, or the United States;

(B) the identity, habits, business, occupation, knowledge, efficiency, loyalty, movement, location, affiliations, associations, transactions, acts, reputation, or character of a person;

(C) the location, disposition, or recovery of lost or stolen property; or

(D) the cause or responsibility for a fire, libel, loss, accident, damage, or injury to a person or to property;

(2) engages in the business of securing, or accepts employment to secure, evidence for use before a court, board, officer, or investigating committee;

(3) engages in the business of securing, or accepts employment to secure, the electronic tracking of the location of an individual or motor vehicle other than for criminal justice purposes by or on behalf of a governmental entity; or

(4) engages in the business of protecting, or accepts employment to protect, an individual from bodily harm through the use of a personal protection officer.

(b) For purposes of Subsection (a)(1), obtaining or furnishing information includes information

obtained or furnished through the review and analysis of, and the investigation into the content of, computer-based data not available to the public. The repair or maintenance of a computer does not constitute an investigation for purposes of this section and does not require licensing under this chapter if:
(1) the review or analysis of computer-based data is performed only to diagnose a computer or software problem;
(2) there is no intent to obtain or furnish information described by Subsection (a)(1); and
(3) the discovery of any information described by Subsection (a)(1) is inadvertent.

Computer forensics investigations fall well within the State of Texas's definition of an investigative service. As stated in the Private Security Act, a person acts as an investigator, if they engage in the business of obtaining or furnishing information related to the identity, habits, business, occupation, knowledge, efficiency, loyalty, movement, location, affiliations, associations, transactions, acts, reputation, or character of a person or engage in the business of securing evidence for use before a court, board, officer, or investigating committee.

B. Computer Forensics Certification

There is not a specific certification that denotes someone as a computer forensic expert, but there are an increasing number of organizations that offer certification in computer forensics. Global Information Assurance Certification (GIAC) currently has over 1700 certified analysts and is accredited under the ANSI/ISO.IEC 17024 personnel Certification Program. The IACRB (Information Assurance Certification review Board) sponsors the Certified Computer Forensics Examiner (CCFE) certification. These candidates must pass a multiple choice exam with a score of 70% or higher. Candidates that ass the multiple choice exam are then given mock evidence files in the form of a computer image and they must analyze these files and then submit a report to be graded on such image. The IACIS (International Association of Computer Investigative Specialists) has offered a computer forensics certification since 1994, now known as the Certified Forensic Computer Examiner (CFCE).

Other computer forensic software companies offer product specific certifications, such as the Encase Certified Examiner (EnCE) certification and the AccessData ACE certification. The Certified Information System Security Professional certification (CISSP) is a highly respected security certification that certifies that an individual has a mastery of international standards of information security.

The International Association of Computer Investigative Specialists offers training and certifications previously only offered to those in the law enforcement community but which are now available to anyone. The primary certification offered is the Certified Forensic Computer Examiner (CFCE) which is a two week certification course that teaches forensic imaging, examination, reporting and ethics as well as legal issues in the area of computer crimes.

Another well respected program is sponsored by the International Information Systems Forensic Association (IISFA) and is called the Certified Information Forensics Investigator (CIFI). The CIFI program has an adherence to high standards of ethical conduct and knowledge requirements and expertise. The CIFI maintains vendor neutrality and is independent of dependence requirements such as sponsored training, purchasing a product or requirements other than ability.

An additional question to consider when selecting a computer forensics expert is how much of the individual's practice is devoted to computer forensics. Some potential experts divide their practice between forensics, repair, installation, programmer and private investigator. While it might be feasible for a computer firm to have a wide range of specialties, it should give the potential client pause for concern if a solo practitioner practices a wide range of attributes. Instead, when hiring a potential forensics expert, it is best to hire one who focuses his or her practice on forensics.

Additionally, when interviewing a potential computer forensic experience, it is

important to investigate whether or not the expert has experience testifying in court. Many times in family law, forensic investigators must testify in court and need to understand how to communicate technical concepts and jargon without losing the judge or jury.

IV. WHAT CAN A COMPUTER FORENSIC EXPERT DO?

Computer forensics experts are generally hired to acquire, authentic and analyze data in legal cases. Each of the steps is explained in depth below. while there are numerous other technical aspects of the forensic practice, the following is intended to merely be a brief overview for the family law practitioner to best understand the process when hiring an evaluator to evaluate a specific media.

A. Acquisition

Once a forensic expert is hired, he or she works from a copy of the electronic media. The process of obtaining the forensic copy or forensic image is called the "acquisition phase" of the examination. This process involves making a forensic copy of the hard drive. The common practice is for the examiner to make a physical image, or exact duplicate of the drive. This is often referred to as a "bitstream" copy by forensic examiners. The acquisition process allows the examiner to gather information independent of the operating system and ensure that all data from the drive to be examined is obtained. The forensic image of the drive is commonly obtained in the form of E01 files, which is a proprietary file format that stores the contents of an acquired drive. Using the files, the examiner can then reconstruct the drive for analysis. "E01 files" are commonly called "evidence files" by examiners. When acquiring electronic media, a "write blocker' is used. A write blocker is a piece of hardware that prevents the operating system of the examiner's machine from making changes to the original media.

B. Authentication

Once the electronic media has been acquired, the examiner must verify that he or she has made an accurate copy. To do this, the examiner will "hash" the drive or media. Hashing may be thought of as "bates labeling" in computer forensics. Hashing is taking the sequence of data and running it against a hashing algorithm with the result being a unique code. See http://www.nsrl.nist.gov/Documents/hash-selection.pdf. Two files with the same data should then result in the same code being generated by the algorithm. Texas courts have addressed hashing and have found it to be a reliable means of verifying that a sequence of data has not been changed. *See Williford v. State*, 127 S.W.3d 309, 312–13 (Tex.App.-Eastland 2004, pet. ref'd) (finding testimony about EnCase and hashing was reliable in child pornography case). In the authentication process, it is relatively simple to determine that a valid copy was made of the drive as the hash value of the original should be the same as compared to the copy. In a report, you will see the term "acquisition hash" and "verification hash."

C. Analysis

After an examiner has forensically authenticated the piece of electronic evidence, analysis begins. An evaluation may often use a variety of tools to analyze the data. Forensic tools have several features in common; the ability to acquire and image the drive along with verification of the image as well as the ability to create E01 files, and they allow for file viewing at the disc level and automated searching and filtering functions, logging functions and annotation of the findings. There are many forensic tools available and often an examiner will use a combination of tools to conduct the examination as one tool may be better at a particular function than others. Some examiners are more comfortable with a particular forensic tool or may have received more training and have more experience with a particular tool. If

possible, find out what your examiner uses and prefers and their experience level with the tools. Most of the current tools, including write block devices have been evaluated by the National Institute of Standards and their computer tool testing section. The NIST reports are helpful in understanding forensic tools in general and their capabilities and limitations.

VI. THE LAW AND COMPUTER FORENSICS

Before engaging a computer forensic expert, family law practitioners need to be aware of the federal and state laws concerning the collection, storage and dissemination of electronic evidence. Additionally, attorneys must educate their clients on what information they have an ability to obtain or monitor and the consequences for deviating from established rules. Each of the relevant rules and commiserate case law will be addressed below.

A. Federal Wiretap Statute

1. Background

The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act of 1986 (ECPA). The ECPA updated the Federal Wiretap Act of 1968. The older Wiretap Act had been written to address interception of conversations using "hard" telephone lines. The onset of computer and other digital and electronic communications prompted the need to make the update. The USA PATRIOT Act and subsequent federal enactments have clarified and updated the ECPA in light of the ongoing development of modern communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases.

2. General Provisions

The ECPA, as amended, protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically. ECPA has three titles:

Title I of the ECPA, which is often referred to as the Wiretap Act, prohibits the intentional actual or attempted interception, use, disclosure, or "procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." Title I provides exceptions for operators and service providers for uses "in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service" and for "persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act (FISA) of 1978." 18 U.S.C. § 2511. It provides procedures for Federal, State, and other government officers to obtain judicial authorization for intercepting such communications, and regulates the use and disclosure of information obtained through authorized wiretapping. 18 U.S.C. § 2516-18. A judge may issue a warrant authorizing interception of communications for up to 30 days upon a showing of probable cause that the interception will reveal evidence that an individual is committing, has committed, or is about to commit a "particular offense" listed in § 2516. 18 U.S.C. § 2518. Title I also prohibits the use of illegally obtained communications as evidence. 18 U.S.C. § 2515. The Wiretap Act imposes criminal and civil liability for intentional “interceptions” of electronic communications. 18 U.S.C.A. §2511. Actual and punitive damages are recoverable. Minimal liquidated damages of $10,000.00 may be imposed for violations of the Wiretap Act. 18 U.S.C.A. §2500.

Title II of the ECPA, which is called the Stored Communications Act (SCA), protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses. 18 U.S.C. §§ 2701-12.

Title III of the ECPA, which addresses

pen register and trap and trace devices, requires government entities to obtain a court order authorizing the installation and use of a pen register (a device that captures the dialed numbers and related information to which outgoing calls or communications are made by the subject) and/or a trap and trace (a device that captures the numbers and related information from which incoming calls and communications coming to the subject have originated). No actual communications are intercepted by a pen register or trap and trace. The authorization order can be issued on the basis of certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the applicant's agency.

3. *Amendments*

The ECPA was significantly amended by the Communications Assistance to Law Enforcement Act (CALEA) in 1994, the USA PATRIOT Act in 2001, the USA PATRIOT reauthorization acts in 2006, and the FISA Amendments Act of 2008. Other acts have made specific amendments of lesser significance.

a. Federal Wiretap Act-Relevant Portions of the Statute

The Federal Wiretap Act (Title 18, U.S.C.A. §§2510-3127) is set forth in relevant part as follows:

18 U.S.C. Section 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who–

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when–

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors 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 in violation of this subsection;

(d) intentionally uses, or endeavors 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 in violation of this subsection; or shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(d) 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 one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious action in violation of the Constitution or laws of the United States or of any State.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person-
(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;...
(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.
(5)(a)(ii) In an action under this subsection –
(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal
Government shall be entitled to appropriate injunctive relief; and (B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.
(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

b. 18.U.S.C. Section 2510. Definitions.

(1) "wire communication" means any aural transfer made in whole or in part through the use of
facilities for the transmission of communications be the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;
(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;
(4) "intercept" means the aural or other acquisition
of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.
(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than–
(a) any telephone or telegraph instrument, equipment or facility, or any component thereof,
(i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;
(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;
(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence or any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include–
(A) any wire or oral communication;
(B) any communication made through a toneonly paging device;
(C) any communication from a tracking device (as defined in section 3117 or this title); or
(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;
(14) "electronic communication system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic

equipment for the electronic storage of such communications;
(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;
(17) "electronic storage" means–
(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;
(18) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception;"

c. 18 U.S.C. Section 2515. Prohibition of use as evidence of intercepted wire or oral communications

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

d. 18.U.S.C. Section 2520. Recovery of civil damages authorized

(a) In General. – Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.
(b) Relief. – In an action under this section, appropriate relief includes – (1) such preliminary and other equitable or declaratory relief as may be appropriate; (2) damages under subsection (c) and punitive damages in appropriate cases; and (3) a reasonable attorney's fee and other litigation costs reasonably incurred.
(c) Computation of Damages.--
.....
(2) In any other action an action under this section, the court may assess as damages whichever is the greater of –
(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or (B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000. Note: The language in Section 2520 of the Wiretap Act was changed from "shall be entitled to damages" to a court "may" assess damages. Most courts have viewed the change to mean that awarding damages is discretionary and will not award damages for *de minimis* violations of Title I. *See Goodspeed v. Harman*, 39 F.Supp. 2d 787, 791 (N.D. Tex. 1999).)(*cf. Robinson v. Fulliton*, 140 S.W.3d 312 (Tenn.Ct.App. 2003)(holding that the intention of the statute was that an award for damages is not discretionary, but rather is mandatory).
(e) Limitation. – A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

B. Texas Law Regarding Interception of Communication

Texas also has statutory prohibitions against electronic interception. Ch. 123, Tex. Civ. Prac. Rem. Code; Ch. 16.02, Tex Pen. Code, and Sec. 1820, Tex Code Crim Proc.

1. Texas Civil Practice and Remedies Code

Chapter 123.001 of the Texas Civil Practice and Remedies Code provides as follows:
Chapter 123. Interception of Communication Section 123.001. Definitions.
In this chapter:
(1) "Communication" means speech uttered by a person or information including speech that is transmitted in whole or in part with the aid of a wire or cable.

(2) "Interception" means the aural acquisition of the contents of a communication
through the use of an electronic, mechanical, or other device that is made without the consent of a party to the communication, but does not include the ordinary use of:
(A) a telephone or telegraph instrument or facility or telephone and telegraph equipment;
(B) a hearing aid designed to correct subnormal hearing to not better than normal;
(C) a radio, television, or other wireless receiver; or
(D) a cable system that relays a public wireless broadcast from a common antenna to a receiver.
Section 123.002. Cause of Action
(a) 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.
(b) This section 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.
Section 123.004. Damages
A person who establishes a cause of action under this chapter is entitled to:
(1) an injunction prohibiting a further interception, attempted interception, or divulgence or use of information obtained by an interception;
(2) statutory damages of $10,000 for each occurrence;
(3) all actual damages in excess of $10,000;
(4) punitive damages in an amount determined by the court or jury; and (5) reasonable attorney's fees and costs.

See Collins v. Collins, 904 S.W.2d 792 (Tex. App. -Houston [1st Dist.] 1995), writ denied, 923 S.W.2d 569 (Tex. 1996) (per curiam); *Kotrla v. Kotrla*, 718 S.W.2d 853, 855 (Tex. App. – Corpus Christi 1986, writ ref'd n.r.e.).

C. Texas Penal Code

Section 16.02 of the Texas Penal Code prohibits the unlawful interception, use, or disclosure of wire, oral or electronic communications, either personally or by hiring another person to take such actions. Section 16.02 of the Texas Penal Code provides that:

1. Section 16.02. Unlawful Interception, Use, Or Disclosure of Wire, Oral, or Electronic Communications.

(a) In this section, "computer trespasser," "covert entry," "communication common carrier," "contents," "electronic communication," "Electronic, mechanical, or other device," "immediate life-threatening situation," "intercept," "investigative or law enforcement officer," "member of a law enforcement unit specially trained to respond to and deal with life-threatening situations," "oral communication," "protected computer," "readily accessible to the general public," and "wire communication" have the meanings given those terms in Article 18.20, Code of Criminal Procedure.
(b) A person commits an offense if the person:
(1) intentionally intercepts, endeavors to intercept, or procures another person to intercept a wire, oral or electronic communication;
(2) intentionally discloses or endeavors to disclose to another person the contents of a wire, oral or electronic communication if the person knows, or has reason to know, the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
(3) intentionally uses or endeavors 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 in violation of this subsection;
(4) knowingly or intentionally effects a covert entry for the purpose of intercepting wire, oral,

or electronic communications without court order or authorization; or (5) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when the device:
(A) is affixed to, or otherwise transmits a signal through a wire, cable, or other connection used in wire communications; or (B) transmits communications by radio or interferes with the transmission of communications by radio.
(c) It is an affirmative defense to prosecution under Subsection (b) that:
.....
(4) a person not acting under color of law intercepts a wire, oral, or electronic communication, if:
(A) the person is a party to the communication; or
(B) one of the parties to the communication has given prior consent to the interception, unless the communication is intercepted for the purpose of committing an unlawful act;
.....
(f) An offense under this section is a felony of the second decree, unless the offense if committed under Subsection (d) or (g), in which event the offense is a state jail felony.

D. Definitions in Texas Code of Criminal Procedure.

The definitions of some of the words in Section 16.02 of the Texas Penal Code are found in Article 18.20 of the Texas Code of Criminal Procedure as follows: "Wire Communication" means an aural transfer
made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception, including the use of such a connection in a switching station, furnished or operated by a person authorized to engage in providing or operating the facilities for the transmission of communications as a communications common carrier. The term includes the electronic storage of a wire communication. *Tex. Code Crim. Proc. Art. 18.20(1).*
"Oral communication" means an oral communication uttered by a person exhibiting an expectation that the communication is not subject to interception under circumstances justifying that expectation. The term does not include an electronic communication. *Tex. Code Crim. Proc. Art. 18.20(2).*
"Intercept" means the aural or other acquisition of the contents of a wire, oral, or electronic communication through the use of an electronic, mechanical or other device. *Tex.*
Code Crim. Proc. Art. 18.20(3).
"Electronic communication" means a transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo-optical system. The term does not include:
A. A wire or oral communication; B. A communication made through a tononly paging device; or
C. A communication from a tracking device.

E. Case Law-Wiretap Act

1. General

Provisions of the Federal Wiretap Act clarify that Congress did not intend to regulate the entire field of wiretapping when it enacted the law. 18 U.S.C. §2516(2)(1994). Because the Act gives only the minimum protection against illegal interception, states may regulate the wiretapping field by passing stricter legislation if the state wants to offer its citizens more protection**.** *Id.* However, states are not required to pass wiretapping statutes and may rely solely on the provisions of the Federal Wiretap Act. *See Commonwealth v. Vitello*, 327 N.E. 2d 819, 833 (Mass. 1975). When determining which statute will apply in a given case, the courts must first decide whether the federal wiretapping statute preempts the state statute. Courts have held that the federal statute will preempt a state statute that "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."

Id. at 835. To avoid this preemption, states will adopt statutes that are either more stringent or similar to the federal statute. *See Id.*

Several federal opinions have been written regarding the Federal Wiretap Act, which is closely related to the Texas wiretap statute. In the case of *O'Brien v. O'Brien*, 899 So. 2d 1133 (Florida 2005), the Court held that the wife illegally intercepted her husband's electronic mail and instant messaging communications with another woman, and the communications were properly excluded from evidence. In *O'Brien*, the wife installed a spyware program called Spector on her husband's computer. The Spector spyware secretly took snapshots of what appeared on the computer screen, and the frequency of the snapshots allowed Spector to capture and record all chat conversations, instant messages, e-mails sent and received, and the websites visited by the user of the computer. The husband received an injunction preventing the wife's disclosure of the communications and preventing her from engaging in the behavior in the future. The wife argued that the electronic communications did not violate the Florida wiretap statute as the communications were retrieved from storage and therefore not "intercepted communications." The Florida statute, which was modeled after the Federal Wiretap Act, subjects a person to criminal penalties for violating the statute.

The Court in *O'Brien* held that the issue was whether the electronic communications were "intercepted." The Court noted that the federal courts have consistently held that electronic communications, in order to be intercepted, must be acquired contemporaneously with transmission and that electronic communications are not intercepted within the meaning of the Federal Wiretap Act if they are retrieved from storage. *Citing Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3d Cir. 2003); *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir.), *cert. denied*, 543 U.S. 813, (2004); *United States v. Steiger*, 318 F.3d 1039 (11th h Cir.), *cert. denied*, 538 U.S. 1051, 123 S.Ct. 2120 (2003); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002), *cert. denied*, 538 U.S. 1193, 123 S. Ct. 1292 (2003); *U.S. v. Szymuszkiewicz*, 622 F.3d 701 (2010). E-mail in storage after completion of the transmission cannot be intercepted and is not protected by the Wiretap Act. *Fraser v. Nationwide*, 352 F.3d 107(3rd Cir. 2003). The Spector spyware program that the wife installed on the computer used by her husband in *O'Brien* intercepted and copied the electronic communications as they were transmitted. Therefore, the Court held this method constitutes interception with the meaning of the Florida wiretap statute.

To be considered an interception under the Federal Wiretap Act, the communication must be acquired by an electronic, mechanical, or other device during its transmission. *United States v. Meriwether*, 917 F.2d 955(6th Cir. 1990). In *Meriwether* the Sixth Circuit held that an FBI agent did not unlawfully intercept a text message sent by the defendant to a pager that he had lawful possession of. The agent merely acquired the text message visually and did not use a device other than the pager that received the communication. As such, he was actually a party to the communication. The Court held that no intercept occurred once the message was received by the pager because the transmission was complete before the agent read the message. *Id.* at 960.

It has been held that "intercepting" an e-mail can occur only while the email is in transit, and not after it has been received by the recipient's internet service provider. *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002); *United States v.Steiger*, 318 F.3d 1039 (11th Cir. 2003). Therefore, the Federal Wiretap Act prohibits only acquisitions of e-mail that are contemporaneous with transmission. As noted by one author, the window of prohibited activity for e-mail lasts only a few seconds, or even mili-seconds – the time it takes for a newly - composed e-mail message to travel from the sender to the receiver's internet service provider. Jarrod J. White, *E-Mail @Work.com: Employer Monitoring of Employee E-mail*, 48 Ala. L. Rev. 1079, 1083 (1997). Keystroke loggers or spyware programs that capture e-mail messages

in transit, or "re-routing software" that surreptitiously sends duplicate copies of a sender's email to a third person would fit the contemporaneous requirement of the Federal Wiretap Act. In *United States v. Steiger*, 318 F.3d 1039 (11th Cir.), *cert. denied*, 538 U.S. 1051, 123 S. Ct. 2120 (2003), an individual was able to hack into the defendant's computer via a Trojan horse virus that allowed the hacker access to pornographic materials stored on the hard drive. The court held that because the Trojan horse virus simply copied information that had previously been stored on the computer's hard drive, the capture of the electronic communication was not an interception within the meaning of the Federal Wiretap Act. The court indicated, however, that interception could occur if the virus or software intercepted the communication as it was being transmitted and copied it. The Court in *Steiger*, stated: "[T]here is only a narrow window during which an E-mail interception may occur – the seconds or mili-seconds before which a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible." *Steiger*, 318 F.3d at 1050 (quoting Jarrod J. White, EMail@Work.com: Employer Monitoring of Employee EMail, 48 Ala. L. Rev. 1079, 1083 (1997); *See Brown v. Waddell*, 50 F.3d 285 (4th Cir. 1995)(cell phones).

Text messages on a cell phone are not protected under the Federal Wiretap Act or the Stored Communications Act. *U.S. v. Jones*, 451 F. Supp. 2d 71 (D.D.C. 2006) (Court held that police officers did not have to follow protocol of wiretapping statutes in getting cell phone text messages during an investigation because they were not covered under the statute).

F. The Stored Communications Act

1. The Federal Stored Communications Act.

E-mail has essentially replaced traditional letters and even telephone calls as the primary choice for communication. Access to e-mail and voicemail by private parties is primarily regulated under Title II of the ECPA. Title II regulates access to "stored electronic communications", and is commonly known as the Stored Communications Act. *See* 18 U.S.C.A. §§ 2701-2711. The Act prohibits any person from "intentionally accessing without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system...." 18 U.S.C. § 2701. Under the USA PATRIOT ACT (the Patriot Act) amendments to the ECPA, voicemail is treated as e-mail. The Stored Communications Act protects against unauthorized "access" to "electronic communication while it is in electronic storage." 18 U.S.C.A. § 2701. This Act provides protection for private communication
only during the course of transmission.

a. 18 U.S.C. Section 2701. Unlawful access to stored communications

(a) Offense.– Except as provided in subsection (c) of this section whoever --
(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.
(b) Punishment.– The punishment for an offense under subsection (a) of this section is – (1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State –

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and (B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and
(2) in any other case – (A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and (B) a find under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section. (c) Exceptions.– Subsection (a) of this section does not apply with respect to conduct authorized – (1) by the person or entity providing a wire or electronic communications service;
(2) by a user of that service with respect to a communication of or intended for that user; or ...
"Electronic storage" under the Act is defined as:
A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.
"Electronic communication service" under the Act is defined as any service that provides users the ability to send or receive wire or electronic communications.

2. Texas Penal Code – Unlawful Access to Stored Communications

Penal Code Section 16.04. Unlawful Access to Stored Communications
(a) In this section, "electronic communication," "electronic storage," "user," and "wire communication" have the meanings assigned to those terms in Article 18.21, Code of Criminal Procedure.
(b) A person commits an offense if the person obtains, alters, or prevents authorized access to a wire or electronic communication while the communication is in electronic storage by: (1) intentionally obtaining access without authorization to a facility through which a wire or electronic communications service is provided; or (2) intentionally exceeding an authorization for access to a facility through which a wire or electronic communications service is provided. (c) Except as provided by Subsection (d), an offense under Subsection (b) is a Class A misdemeanor. (d) If committed to obtain a benefit or to harm another, an offense is a state jail felony. (e) It is an affirmative defense to prosecution under Subsection (b) that the conduct was authorized by: (1) the provider of the wire or electronic communications service;
(2) the user of the wire or electronic communications service; (3) the addressee or intended recipient of the wire or electronic communication; or (4) Article 18.21, Code of Criminal Procedure.

3. Case Law – Stored Communications Act

Title II of the ECPA (the Stored Communications Act) prohibits unauthorized access to an electronic communication while it is in "electronic storage." *See 18 U.S.C.A. § 2701(a)(2).* The Texas statute in the Texas Penal Code is closely related to the federal Stored Communications Act. *Tex. Pen Code § 16.04.* Messages that are in post-transmission storage after transmission is complete are not covered under the definition of "electronic storage." Therefore, retrieval of a message from post-transmission storage is not covered by the Stored Communications Act. The Stored Communications Act provides protection only for messages while they are in the course of transmission. *Fraser v. Nationwide Mutual Insurance Co.*, 135 F. Supp.2d 623 (E.D. Pa 2001). Therefore, there is no violation of the Stored Communications Act in cases where spouses access e-mail stored on the hard drive of the computer in the family home. These provisions govern access to e-mail held in electronic storage for the recipient at an Internet Service Provider (ISP). Thus, the statutes draw a distinction between interception of e-mail while in transmission and access to that same communication once it has reached its destination and is held in the recipient's mailbox. Once e-mail is received and stored in a computer system, it is regulated exclusively under The Stored Communications Act (Title II). Accessing stored e-mail is not an "interception" of an electronic communication under the Federal Wiretap Act (Title I). *Steve*

Jackson Games v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994); *Konop v. Hawaiian Airlines*, 262 F.3d 972 (9th Cir. 2001).

To violate the Stored Communications Act, the communication must be in temporary, intermediate storage or backup storage. Temporary, intermediate storage is construed in the statute as those communications held on the system of the service provider pending delivery to the intended recipient of the communication. An e-mail, for example, is sent through the electronic communications service provider, which stores the communication until the recipient downloads the e-mail from the provider. After the recipient downloads the e-mail, temporary immediate storage ends and the e-mail enters post transmission storage on the computer of the recipient. At this point the communication is no longer under temporary, intermediate storage, and access of electronic communication that is in post transmission storage on the personal computer of the recipient is not a violation of the Stored Communications Act. *Fraser v. Nationwide Mutual Insurance Co.*, 135 F. Supp. 2d 623 (E.D. Pa.2001).

The Stored Communications Act applies to information stored with a phone company internet service provider, or electronic bulletin board system. *United States v. Steiger*, 318 F.3d 1039 (11th Cir. 2003). The Stored Communications Act provides for criminal punishment, 18 U.S.C. § 2701(b), and civil damages, 18 U.S.C. § 2707, but it contains no rule of exclusion that would prohibit the use of such evidence in trial. See *United States v. Smith*, 155 F.3d 1051, 1057 (9th Cir. 1998). The Eleventh Circuit held that while the Federal Wiretap Act makes it illegal to intercept electronic communications, it does not provide a basis for excluding unlawfully intercepted electronic communications from evidence. *United States v. Steiger*, 318 F.3d 1039 (11th Cir. 2003). Under this view, illegal interceptions of wire (i.e. telephone) and oral interceptions are excluded from evidence, but illegal interceptions of e-mail are not excluded from evidence. *See also, United States v. Meriwether*, 917 F.2d 955, 960 (6th Cir. 1990); *United States v. Reyes*, 922 F.Supp. 818, 837 (S.D.N.Y. 1996). The New Jersey statute contains language that tracks the federal Stored Communications Act. In *White v. White*, 344 N.J. Super. 211, 781 A.2d 85 (N. J. Super. Ct. App. Div. 2001), the court evaluated the applicability of state and federal statutes to interspousal access to e-mail stored on a computer in the family home. The court held that the wife did not unlawfully access stored electronic communications in violation of the New Jersey Wiretap Act. In *White*, although a divorce petition had been filed, the husband and wife lived in the same house. He occupied the "sun room" of the home with the family computer, television and stereo. The husband and the children of the parties often used the sun room to utilize the computer, watch television and adjust the stereo. After the wife discovered a letter from the husband to his girlfriend, allegedly in plain view, she hired a computer detective and copied his e-mails that were stored on the hard drive. The court held there was no violation of the New Jersey Wiretap Act for two reasons. First, the e-mail was not in "electronic storage" when it was accessed; and second, access to the e-mail was not "without authorization" as meant by the Act. In *White*, the court adopted the accepted technical description of transmission of e-mail. E-mail typically involves three stages of storage, intermediate, back-up and protected storage and "post transmission storage." Post transmissions storage was not "electronic storage" within the meaning of the Wiretap Act. The Act protected only electronic communications which are "in the course of transmission or are backup to that course of transmission." In *White*, the court also concluded that access of the e-mail was not "without authorization" as that concept is meant under the Act. Without authorization was limited to prohibited use of a computer or unauthorized use of someone's password. Because the husband in *White* had consented to his wife's access to access the computer network, her "roaming in and out of different directories on the hard drive" was not "without authorization." *Id.* at 221.

Courts have addressed the definition of "backup storage" under the Stored Communications Act. *Fraser v. Nationwide*

Mutual Insurance Co., 352 F.3d 107(3rd Cir. 2003), *Quon v. Arch Wireless Operating Co.*, 309 F. Supp.2d 1204 (E.D. Ca. 2004). One court found that such e-mails, although not in temporary, intermediate storage because transmission had been completed, were held by the electronic communication service provider for the purposes of backup protection of the communications. *Theofel et al. v. Farey-Jones et al.*, 359 F.3d 1066 (9th Cir. 2003). As such, the e-mails were in electronic storage and therefore were protected by the Stored Communication Act. The Court noted that the obvious purpose of storing the message on an internet service provider's server after transmission is to enable the recipient to download the message again if needed, and the provider is protecting the message for the benefit of the recipient. *Theofel*, at 1075. The Court also rejected the argument that all electronic storage with the provider ended with transmission, since that would render the "backup storage" portion of the definition of electronic storage to be meaningless. *Id.* The Court further pointed out that emails permanently retained by a provider would not qualify as being in backup storage, and any saved e-mail's backup status would end when the underlying e-mail expired in the normal course. *Id.; but see Fraser v. Nationwide Mutual Insurance Co.*, 135 F.Supp.2d 623(E.D.PA. 2001) (Court found that backup storage ended after the completion of the transmission to the recipient of the communication, and therefore access to such communications cannot be violation of the Act). An exception to the Stored Communication Act allows a person or entity that provides a wire or electronic communication service to perform searches of those communications stored on its system. In *Fraser*, an employee's e-mails were accessed by the employer from that employer's server. Since the employer was an entity providing the electronic communication service, it was authorized under the Act to seize e-mails on its system. *Id.*

G. EXCLUSION OF EVIDENCE UNDER THE WIRETAP AND STORED COMMUNICATIONS ACT

The Wiretap Act (Title I) has a strict exclusionary rule. The Wiretap Act provides that "whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial...." 18 U.S.C. § 2515. "Wire communication" is defined as "any aural transfer made in whole or in part through the use of facilities or the transmission of communications by the aid of wire, cable, or other like connection. . . ." 18 U.S.C. § 2510(1). An aural transfer involves the ear, and so has been interpreted by federal courts to include live conversations between people, and voice mail messages, but not email.

The Eleventh Circuit held that while the Federal Wiretap Act makes it illegal to intercept electronic communications, it does not provide a basis for excluding unlawfully intercepted electronic communications from evidence. *United States v. Steiger*, 318 F.3d 1039 (11th Cir. 2003). Under this view, illegal interceptions of wire (i.e., telephone) and oral interceptions are excluded from evidence, but illegal interceptions of e-mail are not excluded from evidence. *See also, United States v. Meriwether*, 917 F.2d 955, 960 (6th Cir. 1990); *United States v. Reyes*, 922 F.Supp. 818, 837 (S.D.N.Y. 1996); *O'Brien O'Brien*, 899 So.2d 1133 (Florida 2005) (court agreed with reasoning of *Steiger* court and concluded that the intercepted electronic communications in the case were not excludable under the Florida Act, which is an identical statute, however, the court held that the trial court did not abuse it discretion in refusing to admit the evidence as it was illegally obtained). The Stored Communications Act applies to information stored with a phone company internet service provider, or electronic bulletin board system. *United States v. Steiger*, 318 F.3d 1039 (11th Cir. 2003). The Stored Communications Act contains no rule of exclusion that would prohibit the use of such

evidence in trial. See *United States v. Smith*, 155 F.3d 1051, 1057 (9th Cir. 1998).

There is no exception for the use of illegally obtained communications under the Wiretap Act in civil cases for impeachment of witnesses, as there is in criminal cases. *United States v. Wuliger*, 981 F.2d 1497(6th Cir. 1994). Under the Texas wiretap statute, there is no statutory exclusion from use as evidence for illegally intercepted communications. *Kotrla v. Kotrla*, 718 S.W.2d 853, 855 (Tex. App.–Corpus Christi 1986, writ ref'd n.r.e.); *Allen v. Mancini*, 170 S.W.3d 167 (Tex. App.–Eastland 2005, no pet.)(court stated that the Texas wiretap statute does not address the admissibility of intercepted communications at trial and there was no violation of the statute because one party consented to the intercept). However, case law authority does exist for exclusion illegally obtained communications in Texas Courts. In *Collins v. Collins*, 904 S.W.2d 792, 796-98 (Tex. App.–Houston [1st Dist.] 1995, *writ denied*, 923 S.W.2d 569 (Tex. 1996), the Court notes that although there is no exclusionary rule under Texas law for illegally intercepted communications, the provisions for criminal penalties and a cause of action for disclosing illegally obtained communications and the availability of an injunction to prevent such disclosure is sufficient to rebut the presumption of admissibility under TRE 402. *Id.* at 799. The Court held that it was an abuse of discretion for the trial court to admit illegally attained recordings of communications, as to allow otherwise would make the court a participant in the illegal activity of disclosing the content of the illegal intercepts. *Id.*

H. MISCELLANEOUS PROVISIONS IN THE TEXAS PENAL CODE

The Texas Penal Code provides that it is a crime for a person to access a computer, computer network or computer system without the effective consent of the owner. This offense can be found in Title 7 of the Texas Penal Code under "Offenses Against Property," Chapter 33 "Computer Crimes," Section 33.02. The statute states:

Section 33.02. Breach of Computer Security.
(a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.
(b) An offense under this section is a Class B misdemeanor unless in committing the offense the actor knowingly obtains a benefit, defrauds or harms another, or alters, damages, or deletes property, in which event the offense is:
(1) a Class A misdemeanor if the aggregate amount involved is less than $1,500;
(2) a state jail felony if:
(A) the aggregate amount involved is $1,500 or more is less than $20,000; or (B) the aggregate amount involved is less than $1,500 and the defendant has been previously convicted two or more times of an offense under this chapter;
(3) a felony of the third degree if the aggregate amount involved is $20,000 or more but less than $100,000; (4) a felony of the second degree if the aggregate amount involved is $100,000 or more but less than $200,000; or (5) a felony of the first degree if the aggregate amount involved is $200,000 or more. *See Mitchell v. State*, 12 S.W.3d 158 (Tex. App.–Dallas 2000, no pet.)(evidence showing that the defendant knowingly accessed her employer's computer files without consent was sufficient to support conviction of breach of computer security arising from defendant's corruption of computer files on her last day of employment; defendant was not authorized to corrupt her employer's files, and defendant admitted to police that she corrupted the files, insinuating that she did so in revenge for how her employer treated her).

I. INVASION OF PRIVACY

1. Right to Privacy

Most states have recognized a tort right to privacy in common law. The common law privacy intrusion tort is violated if someone intentionally intrudes upon the private affairs, seclusion or solitude of another person by means that would be highly offensive to a person or ordinary sensibilities. *Boyles v. Kerr*, 855

S.W.2d 593 (Tex. 1993)(defendant's secret videotaping of himself and plaintiff engaging in intercourse that was later aired for third parties was an invasion of plaintiff's privacy); *Texas State Employees Union v. Texas Dep't of Mental Health and Mental Retardation*, 746 S.W.2d 203 (Tex. 1987). In cases where wiretap acts are not violated, the common law invasion of privacy tort may apply to the forms of surveillance that have been discussed in this paper. A violation of the invasion of privacy tort might result in an award for compensatory damages, but it would not be a basis for excluding evidence in divorce or custody proceedings. If the retrieved messages were stored on a home computer to which both spouses have equal access there is most likely no violation. Texas recognizes a cause of action for willful invasion of privacy, which is a person's right to be left alone in his or her own affairs. *Billings v. Atkinson*, 489 S.W.2d 858 (Tex. 1973). The Texas Constitution protects personal privacy from unreasonable intrusion and guarantees the sanctity of the home and person against unreasonable intrusion. *Texas State Employees Union v. Texas Dep't of Mental Health and Mental Retardation*, 746 S.W.2d 203 (Tex. 1987).

2. Elements of Tort of Right to Privacy

To recover on a claim for invasion of privacy, the complainant must show:
1. Conduct in the nature of an intrusion;
2. Private nature of the thing or place intruded upon; and
3. The intrusion was substantial and the conduct highly offensive or objectionable to the reasonable person. *Thomas v. Allsip*, 836 S.W.2d 825, 828 (Tex. App.–Tyler 1992, no writ); *see also* Restatement (Second) of Torts 752B, cmt. A. Liability for invasion of privacy does not depend on any publicity given to the person whose interest is invaded or to his affairs. *Clayton v. Richards*, 47 S.W.3d 149 (Tex. App.–Texarkana 2001, no pet.)(defendant was found liable for videotaping the plaintiff's bedroom without the plaintiff's permission); *Kramer v. Downey*, 680 S.W.2d 524, 525 (Tex. App.–Dallas 1984, writ ref'd n.r.e.)(defendant who continuously stalked, followed and spied on plaintiff invaded plaintiff's right to privacy); *see also* Restatement (Second) of Torts 752B, cmt. A. When assessing the offensive nature of the invasion, courts require the intrusion to be unjustified or unwarranted. *Billings*, 489 S.W.2d at 860. This type of invasion of privacy is generally associated with either a physical invasion of a person's property, eavesdropping on another's conversation with the aid of wiretaps, microphones, or spying. *Clayton v. Wisener*, 190 S.W.3d 685, 696 (Tex. App.–Tyler 2005, pet. denied). The core of the tort of invasion of privacy is the offense of prying into the private domain of another, and the tort is not limited to unmarried individuals. *Clayton v. Richards*, 47 S.W.3d 149 (Tex. App.–Texarkana 2001, no pet.). In *Vaughn v. Drennon*, 202 S.W.3d 308 (Tex. App.–Tyler 2006, no pet.), the Court held that claim of neighbor's behavior through invasion of privacy by watching plaintiffs through binoculars from defendant's property did not violate the Texas Constitution's guarantee of sanctity of the home and person from unreasonable intrusion.

3. Accessing E-mails

If there is no claim for a violation of the Federal Wiretap Act, the Texas wiretap statute or Stored
Communication Act, there may be a claim against another for invasion of privacy. The court in *White v. White*, 344 N. J. Super.211, 781 A.2d 85 (N.J. Super. Ct. App. Div. 2001), rejected the plaintiff's claim that accessing stored email constituted a violation of the common law privacy intrusion tort. The court stated that the plaintiff must have a reasonable expectation of privacy in the area or information that is accessed and the means of access must be "highly offensive" for a tortious invasion of privacy to occur. In that case, the husband did not have a reasonable expectation of privacy in e-mail on the hard drive of the home computer. The court analogized the computer to an office file cabinet in a room that both spouses had complete access to.

4. Damages for Invasion of Privacy

A plaintiff can recover the following types of damages for the tort of invasion of privacy.

1. Actual Damages – Generally, the actual damages resulting from an invasion of privacy claim are personal injury damages. There are two common types of damages which fall under this category: mental anguish and loss of earning capacity. With an invasion of privacy claim, unlike claims for other torts, a plaintiff can recover for mental anguish without proving physical injury. *Motor Express, Inc. v. Rodriguez*, 925 S.W.2d 638, 639 (Tex. 1996).

2. Nominal Damages – A plaintiff will be limited to recovery of only nominal damages if the plaintiff cannot prove actual loss or injury as a result of the invasion. *K-Mart Corp. v. Trotti*, 677 S.W.2d 632, 637 (Tex. App.–Houston 1st Dist.] 1984), writ ref'd n.r.e., 686 S.W.2d 593 (Tex. 1985).

3. Exemplary damages – Exemplary damages are available under a claim for invasion of privacy if the plaintiff successfully proves by clear and convincing evidence that the defendant acted with malice. One case upheld a punitive damages award of $1,000,000 (21% of defendant chiropractor husband's net worth) where the defendant had bugged telephones of his wife's attorneys and engaged in other outrageous conduct. *Parker v. Parker*, 897 S.W.2d 918, 930 (Tex. App.–Fort Worth 1995, writ denied) overruled on other grounds by *Formosa Plastics Corp. USA v. Presidio Engineers & Contractors, Inc*., 960 S.W.2d 41.

4. Equitable Relief – A permanent injunction may be obtained to protect against invasions of privacy. *Kramer v. Downey*, 680 S.W.2d 524, 525 (Tex. App.–Dallas 1984, writ ref'd n.r.e.)("The right to be left alone from unwanted attention may be protected, in a proper case, by injunctive relief.")

5. Interest – A plaintiff may recover prejudgment and postjudgment interest in an action for invasion of privacy.

6. Court Costs – A plaintiff may recover court costs in an action for invasion of privacy.

VII. CRIMINAL RISK TO LAWYERS FOR USE AND ETHICAL CONSIDERATIONS

Lawyers should be aware that the state and federal wiretap statutes bring criminal and civil sanctions to bear not only against one who makes illegal interceptions, but also one who merely uses them. *See United States v. Wuliger*, 981 F.2d 1497 (5th Cir. 1992). This is especially dangerous for attorneys since merely disclosing information that was attained by violation of the Federal Wiretap Act and the Texas wiretap statute by itself can subject the attorney to both criminal and civil liability. In the *Wuliger* case, an attorney was convicted with an offense under the Federal Wiretap Act. The husband had intercepted and recorded phone conversations of the wife at the marital residence without the wife's knowledge. The attorney had used the tape recordings of phone conversations in depositions and in a divorce trial, asking questions of the wife from information attained from the tapes. The Court held that the government must show that the attorney had reason to know that the recordings were illegally obtained. *Id.* Unless the attorney was aware of evidence that showed the tapes were illegally obtained, the attorney could rely on the representation of the client that the recordings were legally obtained. The application of the Federal Wiretap Act was exhaustively examined in *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158 (5th Cir. 2000). Among other things, *Peavy* indicates that a client's disclosure of the content of illegally-made tapes to an attorney is prohibited by the statute, but an exception is recognized for attorney-client discussions that occur in the context of a suit or prosecution over the tapes in question.

In addition to criminal and civil liability, attorneys should be aware of additional requirements imposed on their conduct by professional ethical codes. Although the ABA Formal Ethics Committee has issued an opinion that a lawyer may secretly record telephone conversations with third parties without violating ethical structures so long as the law of the jurisdiction permits, state ethical opinions

have differed on the subject. ABA Formal Ethics Opinion 01-422 (2001).

VIII. CASE LAW REGARDING COMPUTER FORENSICS

To date, there are only a very few cases in Texas that directly address the use of computer forensic experts and the roles that they may play in cases and the limits on what may or may not be discoverable. Below follows the two key cases that address these issues.

B. *In re Honza*, 242 S.W.3d 578 (Tex.App.–Waco, 2008, no pet.)

The Waco Court of Appeals in *Honza* first addressed the rules for forensic examination of electronic data. The case involved the issue of a real estate contract and whether it had been amended after the terms had been agreed to. The first trial ended in a mistrial and before the second trial, A&W requested access to Honza's hard drive to examine it for "metadata." The trial court authorized access and Honza filed a mandamus. After looking at federal and state law in the area, the Waco Court of Appeal announced a 5 prong test as follows: Step 1: The party seeking discovery selects a forensic expert to make a mirror image of the computer hard drive at issue. *Honza* at 582. Step 2: The expert is required to perform an analysis subject to the terms of a protective order, generally prohibiting the expert from disclosing confidential or otherwise privileged information other than under the terms of the discovery order. *Id*. Step 3: The expert is required to compile the documents analyzed and provide copies to the party opposing the discovery. *Id*. Step 4: The opposing party then reviews the documents and produces those that are responsive to the discovery request and creates a privilege log for this documents which are withheld. *Id*. Step 5: The trial court then conducts an incamera review should any disputes arise regarding entries in the privilege log. *Id*. See, *Electronic Discovery in the Age of Honza and Weekley by* Kristal Cordova Thomson, State Bar of Texas, 33rd Annual Marriage Dissolution Institute, May 6-7, 2010.

When the Waco Court of Appeals applied its own test to the trial court's order, it denied the mandamus and concluded that the trial court had limited access to two documents, had found the forensic expert to be well qualified for the task, the protective order of the trial court provided that the forensic examination would not constitute a waiver of privileged or confidential information if such information was obtained and any violation of the order would subject the parties, counsel and expert to contempt. *Id*.

B. In *re Weekley Homes, L.P.*, 295 S.W.3d 309 (Tex. 2009).

The Texas Supreme Court examined the issue of computer forensics in *In re Weekley Homes, L.P.*, 295 S.W.3d 309 (Tex. 2009) and this was the Texas Supreme Court's first opportunity to establish the rules regarding discovery of evidence contained in electronic storage. The Texas Supreme Court relied heavily on the Federal Rules of Civil Procedure and federal case law. The Texas Supreme Court granted mandamus relief to Weekley due to the trial court's order to turn over its four hard drives for a number of reasons. First, it found the search of the hard drives to be "highly intrusive" and the subject matter "sensitive" and the failure to properly qualify the forensic expert regarding his or her expertise as to knowledge, characteristics of the electronic storage devices, its' operating system and that the proposed methodology (protocol) would work. *Id* at 1.

The holding in *Weekley* meant that since Texas Rules of Civil Procedure 196.4 does not provide guidance for the discovery of electronic evidence, the court must look to the Federal Rules for guidance. *Id* at 5. Additionally, the holding meant that a trial court's granting access to electronic storage is the same as giving access to a file cabinet for general perusal and is therefore "particularly intrusive and should be generally discouraged." *Id* at 6. While Texas Rules of Civil Procedure do not impose a "good cause" requirement for obtaining evidence not readily accessible or available, Federal Rules of Civil Procedure *26(b)(2)(B)* does and should be followed. See Federal Rules of Civil Procedure *26(b)(2)(B)* :

(2) Limitations on Frequency and Extent.
(B) Specific Limitations on Electronically Stored Information. A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.
(C) When Required. On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:
(i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;
(ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

The court additionally held that such requests must be examined pursuant to a balancing act test. As there was such a long span of time from when the emails were generated to the time of the discovery request, such request may outweigh the benefit versus the intrusion. The protocol for requesting and obtaining hard drive electronic evidence is explained as follows:
a. The party seeking to discover electronic information must make a specific request for that information and specify the form of production. TEX.R.CIV. P. 196.4.
b. The responding party must then produce any electronic information that is "responsive to the request and ...reasonably available to the responding party in its ordinary course of business."
Id.
c. If "the responding party cannot-through reasonable efforts-retrieve the data or information requested or produce it in the form requested," the responding party must object on those grounds." *Id.*
d. The parties should make reasonable efforts to resolve the dispute without court intervention. TEX.R. CIV. P. 191.2. See TRCP 191.2 below:
191.2 Conference.
Parties and their attorneys are expected to cooperate in discovery and to make any agreements reasonably necessary for the efficient disposition of the case. All discovery motions or requests for hearings relating to discovery must contain a certificate by the party filing the motion or request that a reasonable effort has been made to resolve the dispute without the necessity of court intervention and the effort failed.
e. If the parties are unable to resolve the dispute, either party may request a hearing on the objection, TEX.R. CIV. P. 193.4(a), at which the responding party must demonstrate that the requested information is not reasonably available because of undue burden or cost, TEX.R.CIV. P. 192.4(b).
f. If the trial court determines the requested information is not reasonably available, the court may nevertheless order production upon a showing by the requesting party that the benefits of production outweigh the burdens imposed, again subject to Rule 192.4's discovery limitations.
g. If the benefits are shown to outweigh the burdens of production and the trial court orders production of information that is not reasonably available, sensitive information should be protected and the least intrusive means should be employed. TEX.R. CIV. P. 192.6(b). The requesting party must also pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information. TEX.R. CIV. P. 196.4.
h. Finally, when determining the means by which the sources should be searched and information produced, direct access to another

party's electronic storage devices is discouraged, and courts should be extremely cautious to guard against undue intrusion. See, *Weekley* at 322.

Honza is not overruled but distinguished, as in *Honza* the electronic data was produced but not the metadata and therefore the intrusion was limited to the file and not the file cabinet and unlike *Weekley* the expert in *Honza* was well qualified to conduct the examination.

IX. CONCLUSION

As computer forensics continues to gain importance in family law, practitioners need to remain aware of the myriads uses in cases as well as the pitfalls and legal traps for the unwary. Case law and statutes must and will continue to develop and address issues as individuals become more reliant on technology in their daily lives.