

**SPY VS. SPY**

**THE LEGALITY OF USING WIRETAPS, SPYWARE, GPS AND  
OTHER EAVESDROPPING TECHNOLOGIES**

**REGINALD A. HIRSCH  
1980 Post Oak Boulevard  
Suite 2210  
Houston, Texas 77056  
(713) 961-7800  
[reghir@hirschfamilylaw.com](mailto:reghir@hirschfamilylaw.com)**

**STATE BAR OF TEXAS  
SOAKING UP SOME CLE COURSE  
May 20-21, 2010  
South Padre Island, Texas**

**CHAPTER 11**

**REGINALD A. HIRSCH**  
Law Office of Reginald A. Hirsch  
1980 Post Oak Boulevard, Suite 2210, Houston, Texas 77056  
(713) 961-7800 FAX: (713) 961-3453 E-Mail: reghir@hirschfamilylaw.com

**BIOGRAPHICAL INFORMATION**

**DATE OF BIRTH:** February 24, 1947, Houston, Texas

**MARRIED:** Patricia Wicoff, Attorney at Law; Child: Sarah Lauren Hirsch, Age 23

**EDUCATION:** Lamar High School, Houston, Texas, 1965  
B.S., University of Houston, 1970  
J.D., University of Houston, 1973  
Chief Justice Student Court, University of Houston Student Court, 1972-1973  
Student Regent to the University of Houston Board of Regents, 1972-1973

**PROFESSIONAL EMPLOYMENT:**

Assistant Attorney General for State Bar of Texas, Environmental Division, 1973-1974  
Balasco, Clark, Hirsch and Stern, 1974 - 1979  
Lipstet & Hirsch, 1979 - 2008  
Law Office of Reginald A. Hirsch, 2008-

**PROFESSIONAL LICENSES:**

State Bar of Texas, 1973  
U.S. District Court, Southern District of Texas, 1974  
U.S. Court of Appeals, Fifth Circuit, 1974

**PROFESSIONAL ACTIVITIES:**

Board Certified in Family Law, 1974-2009  
President, Harris County Young Family Lawyers Association, 1977  
President, Family Law Section, Houston Bar Association, 1980-1981  
Member, State Bar of Texas, Family Law Counsel, 1985-1989  
Chairman, Houston Volunteer Lawyers Association, 1983-1984  
Director, The Association of Trial Lawyers of America, 1985  
President Family Law Forum, 1983-1985  
Director, Association of Gulf Coast Family Law Specialists, 1989-1990  
President, Gulf Coast Legal Foundation, 1986  
Texas Association of Family Law Specialists  
International Society of Family Law  
National Association of Counsel for Children  
American Academy of Matrimonial Lawyers  
Adjunct Professor, South Texas College of Law, Environmental Law, 1975-1977  
Guest Lecturer at Baylor College of Medicine  
Guest Lecturer at University of Houston Law School  
Guest Lecturer at South Texas College of Law  
Member, Chairman's Council, Harris County Democratic Party, 1990  
Master, American Inns of Court  
Chairperson, Family Law Task Force 2000  
Treasurer, American Inns of Court, Burta Raborn Chapter. 2005-2008  
President-Elect, American Inns of Court, Burta Raborn Chapter, 2009-2010

**RECENT LAW RELATED PUBLICATION, ACADEMIC APPOINTMENTS AND HONORS:**

Author/Speaker -University of Houston. Fall 2005, Parent Planning Texas Style  
Author/Speaker, Texas Chapter, Association of Family and Conciliation Courts, September 30- October 1, 2005  
Houston, Texas- Panel Interdisciplinary Approaches to Identifying and Addressing Alienation Issues  
Author/Speaker, Texas Chapter Association of Family and Conciliation Courts, September 30- October 1, 2005  
Houston, Texas- Panel Interdisciplinary Approaches to Identifying and Addressing Alienation Issues

Panelist, PBS Houston, "The Connection" Response to "Breaking the Silence: Children Stories" October 28th and 30<sup>th</sup>, 2005

Speaker, Future of Family Law, Burta Raborn Inns of Court, Houston, Tx January, 19,2006.

Speaker, Author, "Tracing Keeping It Simple", Burta Raborn Inns of Court, Houston, Tx February 16, 2006.Speaker, Author, Investigating Your Client, Family Law Conference for General Practitioner and the Legal Assistant, March 9, 2006, Houston, Tx

Recipient, David Gibson Award, Gulf Coast Family Law Specialist, May 11, 2006 Houston, Tx

Speaker, Co-Author, Parenting Plans, South Texas College of Law, Houston, Tx May 19, 2006

Speaker, Co-Author, Amicus Attorney- Who Represents the Child - Not me." State Bar of Texas 2006 Advanced Family Law, San Antonio, Tx August 16, 2006

Speaker, Co-Author, Origins of Parenting Plans, University of Texas, October 13, 2006 Dallas, Texas and November 3, 2006, Houston, Texas

Speaker, Author, Texas Parenting Plans- How We Got Here, University of Houston, November 10 and 17th, Dallas/Houston, Tx

Recipient, Top Family Lawyer, 2006.,Houston Magazine, August 2006

Recipient, Mentor, Award, Houston Bar Association, Family Law Section, January 3, 2006

Speaker, Author, Parenting Plans, How Did We Get Here, Spring 2006, Dallas and Houston, Tx

Speaker, Author, Who Represents the Child, Not Me, I am the Amicus Attorney, August 2006, San Antonio, Tx

Speaker, Author, Electronic Discovery, Hal-PC, April 18, 2007, Houston, Tx

Presenter, Burta Raborn Inns of Court, April 19, 2007, Houston., Tx

Recipient, Texas Super Lawyer, 2007, Family Law, Texas Monthly Magazine

Author, Speaker, University of Texas, Austin, Texas, November 8,2007,The Definitive Short Course on Parent Child Relationships, "The World of Court Appointees: Amicus Attorneys. Attorney Ad Litem, Guardian Ad Litem and Social Studies"

Author, Speaker, State of Texas Judicial College, "Electronic Evidence Issues", Richardson , Tx, April 17, 2008

Author, Speaker, Co Panelist, 8th Annual ,Family Law on the Front Line, "Electronic Evidence –Fighting the War of the Roses in the Electronic Age", June 20, 2008, Galveston, Tx

Recipient, Texas Super Lawyer, 2007, Family Law, Texas Monthly Magazine

Recipient, Judge Judy Warne's Weekly Acknowledgment of Contribution to the Bench and Bar, June 9, 2008

Author, Speaker, Advanced Family Law Course, "When Technology and Family Law Collide", San Antonio, August 11, 2008

Recipient, Texas Super Lawyer, 2008, Family Law, Texas Monthly Magazine

Speaker, HAL-PC Legal Sig, Electronic Evidence, January 21, 2009 Houston, Tx

Author, Speaker, The Impact of Technology on the Parent-Child Relationship, Parent -Child Relationships: Critical Thinking For Critical Issues, University of Texas, Austin, Tx January 29, 2009

Author, Speaker, Using Electronic Evidence,23rd Annual Family Law Conference, South Texas College of Law, March 5, 2009

Author, Speaker, What every CPA should know about Electronic Evidence, Houston CPA Society, April 24, 2009

Recipient, Texas Super Lawyer, 2009, Family Law, Texas Monthly Magazine

Author, Co-Speaker, Using the Latest Technology in the Courtroom and Electronic Evidence Workshop, Advanced Family Law, Dallas, Tx, August 3-6th, 2009

Speaker, Judges and Social Media, Bar to Bench: So You Want to Be a Judge?,Web Cast, State Bar of Texas, Austin, Tx, November 4, 2009

Author, Speaker, Electronic Evidence-How to Avoid Getting Shocked, Ultimate Trial Notebook, San Antonio, Tx December 3-4th, 2009

Speaker, Windows 7 and Office 2010,HAL-PC, Houston, Tx, January 20, 2010

Co-Speaker, Author, Electronic Evidence and Discovery, South Texas School of Law, 24th Annual Family Law Conference, Houston, Tx, March 10, 2010

Author, Speaker, Spy vs Spy, Soaking Up Some CLE, State Bar of Texas, South Padre Island ,May 20, 2010

Author, Speaker, Forensic Computing for Family Lawyers, Advanced Family Law, August 7,2009,San Antonio, TX

## TABLE OF CONTENTS

I.	INTRODUCTION .....	1
II.	IN THE BEGINNING .....	1
III.	THE RIGHT OF PRIVACY .....	1
IV.	WIRETAPS, COMPUTER BREACH, TRACKING DEVICES .....	3
	A. Interception of Communications - Federal and State Law .....	3
	1. The Federal Stored Wire and Electronic Communications Act (“Stored Communications Act”) .....	4
	2. The Federal Wiretap Act .....	5
	a. Consent of a Party .....	5
	b. Spousal Consent .....	5
	c. Vicarious Consent.....	5
	d. Criticism of ECPA.....	6
	B. Interception of Communications - The Texas Counterparts .....	6
	1. Texas Wiretap Statutes .....	7
	2. Breach of Computer Security .....	7
	3. Tracking Devices .....	7
V.	SPYWARE .....	8
	A. GPS (Global Positioning System) .....	8
	1. GPS-enabled Cell Phones .....	8
	2. Wireless Networks .....	8
	a. T-Mobile/Cingular/AT&T .....	8
	b. Sprint/Nextel .....	8
	c. Location-Based Services (LBS) .....	8
	d. Accutracking .....	9
	e. Sprint’s Mobile Locator .....	9
	f. Mapquest Find Me .....	9
	g. Wherify Wireless .....	9
	h. Google Latitude .....	9
	i. Additional Points to Consider .....	9
	i. Permissions and Privacy .....	9
	ii Tracking Application “Persistence” .....	9
	iii. Passive Tracking .....	9
	iv. Assisted GPS (AGPS) .....	9
	v. Tower reports .....	9
	vi. GeoFencing .....	9
	vii. Speed Alerts .....	9
	viii. Tracking Map Quality .....	9
	ix. Usage Costs .....	10
	x. Mobile to Mobile Tracking .....	10
	j. Caveat Emptor .....	10
VI.	“THE GOOD, THE BAD AND THE UGLY” .....	10
	A. The PI Takes Everyone Down .....	10
	B. Spyware on the Mobile Phone .....	11
	C. Spyware on Your Computer .....	11
VII.	CONCLUSION .....	12
	Appendix I .....	13

## I. INTRODUCTION

The topic sure has me scratching my head - how about you? (Note how little hair your speaker has.) With the evolution of technology there has been a battering of the rights of privacy being pummeled. If a war was going on, the white flag of privacy would be raised in a stiff breeze. For lawyers and lay persons it is a *caveat emptor* environment which means being forewarned is being forearmed. Lawyers are confronted weekly with substantive issues concerning technology either used by their clients, or more often, being used against their clients. To say the environment is hostile is an understatement. The goal of this paper is to reduce fear, supplant it with knowledge and remind everyone that the struggle to protect your client and yourself requires constant vigilance.

## II. IN THE BEGINNING

It probably started in the Garden of Eden when Adam and Eve's conversations were overheard. Today it is referred to as eavesdropping.

The telegraph was created in the early 1800's. By 1837 Samuel F. B. Morse had developed and patented the electrical telegraph. Alexander Graham Bell received a patent for the electric telephone in March 1876 (US Patent 174,465).

The Internet can trace its' origins back to ARPNET in 1969. In 1973 a patent was granted to Motorola for what is now known as the cell phone. For the record Steve Jobs was 18 years old in 1973. The Apple I went on sale in 1976 (no keyboard, case or monitor- you built it). The first IBM PC was introduced in 1981. There are multiple technologies that can be traced to the past. Modern technology is relatively new in terms of history.

With the evolution and development of electronic devices, almost everyone has the ability to ascertain the identity, location and analysis of both the sending and the receipt of electronic information. One of the terms used to describe this feature is "electronic fingerprinting." Although the tools over the last 20 years have become extremely robust in detection, recovery and analysis of electronic data, the counter measures have also increased in sophistication. It truly has become a game of "cat and mouse." As an example of the "cat and mouse game," consider Microsoft's release of various patches to it's software,

which is now known in the industry as "Patch Tuesday," followed by "Exploit Wednesday." It has been suggested that the reason for choosing Tuesday is so you can do work on Monday and use the rest of the week to resolve any problems resulting from the patch. For the lawyer and the client it is critically important to be aware of electronic fingerprints, as well as how to find them and make a client aware of how vulnerable their communications can be.

## III. THE RIGHT OF PRIVACY

It is important to discuss technology beginning with an examination of the right of privacy.

The idea of a right to privacy was first addressed within a legal context in the United States by Louis Brandeis (later a Supreme Court justice) and another young lawyer, Samuel D. Warren, who published an article called "The Right to Privacy" in the *Harvard Law Review* in 1890, arguing that the Constitution and the common law allowed for the deduction of a general "right to privacy". Their project was never entirely successful, and the renowned tort expert, Dean Prosser, argued that "privacy was composed of four separate torts, the only unifying element of which was a (vague) "right to be left alone." These elements were:

1. appropriating the plaintiff's identity for the defendant's benefit;
2. placing the plaintiff in a false light in the public eye;
3. publicly disclosing private facts about the plaintiff;
4. unreasonably intruding upon the seclusion or solitude of the plaintiff.

See *Wikipedia*, Privacy Law.

The word "privacy" is actually never used in the text of the US Constitution, or any of its amendments. The Texas Supreme Court in *Texas State Employees Union, et al., Petitioners, v. Texas Department of Mental Health and Mental Retardation, et al., Respondents* (Tex.) 746 S.W.2d 203; held:

While the Texas Constitution contains no express guarantee of a right of privacy, it contains several provisions similar to those in the United States Constitution that have been recognized as implicitly creating protected "zones

of privacy." *Cf. Roe v. Wade*, 410 U.S. 113, 152, 93 S.Ct. 705, 726, 35 L. Ed.2d 147 (1972). Section 19 of the Texas Bill of Rights protects against arbitrary deprivation of life and liberty. TEX.CONST., art. 1, § 19. Section 8 provides the freedom to "speak, write or publish", and section 10 protects the right of an accused not to be compelled to give evidence against himself. TEX.CONST., art. 1, §8, 10. Sections 9 and 25 guarantee the sanctity of the individual's home and person against unreasonable intrusion. TEX.CONST., art. 1, § 9, 25. Finally, the Texas Constitution protects the rights of conscience in matters of religion. TEX.CONST., art. 1, §6. Each of these provisions gives rise to a concomitant zone of privacy. *Cf. Griswold v. Connecticut*, 381 U.S. 479, 484, 85 S.Ct. 1678, 1681, 14 L.Ed.2d 510 (1965). We do not doubt, therefore, that a right of individual privacy is implicit among those "general, great, and essential principles of liberty and free government" established by the Texas Bill of Rights. TEX.CONST., art. I, Introduction to the Bill of Rights. We hold that the Texas Constitution protects personal privacy from unreasonable intrusion. This right to privacy should yield only when the government can demonstrate that an intrusion is reasonably warranted for the achievement of a compelling governmental objective that can be

achieved by no less intrusive, more reasonable means."

Therefore, one may assert a cause of action for invasion of privacy exists under Texas law even if a federal or state criminal statute has not been violated.

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. 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. Section 625B of the *Restatement (Second) of Torts* (1977) provides a cause of action in the following circumstances:

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or in his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person. Under Section 625B, to recover on the tort of 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.

Professor William L. Prosser catalogued four distinct injuries under the tort of invasion of privacy:

- (1) intrusion upon a person's right to be left alone in his or her own affairs;
- (2) publicity given to private information about a person;

- (3) appropriation of some element of the person's personality for commercial use; and
- (4) false light.

See, William L. Prosser, *HANDBOOK OF THE LAW OF TORTS* 638 (2D ED. 1955). These four variations of the tort were adopted by the Second Restatement of Torts. See Restatement (Second) of Torts § 652A (1977).

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).

The concept of invasion of privacy covers intrusion on a party's seclusion, solitude, or private affairs. See *Boyles v. Kerr*, 855 S.W.2d 593 (Tex. 1993); *Texas State Employees Union v. Texas Dep't of mental Health and Mental Retardation*, 746 S.W.2d 203 (Tex. 1987).

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.); Restatement (Second) of Torts 752B, cmt. A. One case has approved a punitive damages award of \$1,000,000 (21% of defendant chiropractor husband's net worth) where the defendant had bugged telephones of 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.

See ELECTRONIC INVESTIGATION AND DIGITAL EVIDENCE, Kathryn J. Murphy and Rick Robertson, State Bar of Texas, 30<sup>th</sup> Annual Marriage Dissolution Institute, May 10-11, 2007, El Paso, Texas.

A typical scenario might be:

My client has accessed the community computer and observed the spouse engaged in (Blank)\_\_\_\_\_ activity. You fill in the blank. Is that legal and what kind of trouble am I in by just looking at the material?

Let's examine the right of privacy aspect.

The real litmus test for claims of invasion of privacy depends on the answer to the question: **“Was the material or data preserved in a manner to give rise to a reasonable expectation of privacy?”** If the answer is “yes” there may have a claim for invasion of privacy. Certain criteria such as the location of the computer, was it password protected and if so was the password kept secret and not disclosed, was the computer used by family members or 3<sup>rd</sup> parties, was the computer a personal or business computer, was the computer used by the other spouse regular or infrequent, what steps did the user take to secure his or data, etc., are a factor. There are many weight components to consider, but the test again **“was there a reasonable expectation of privacy?”** This is the key to understanding the right of privacy.

As Justice Brandeis famously stated privacy "the most comprehensive of rights, and the right most valued by a free people."

Borrowed from the author by permission, *Electronic Evidence Issues*, by Reginald A. Hirsch, State of Texas Judicial College, April 17, 2008.

Another claim involving removing or accessing data from a computer might be easier to assert via a trespass claim.

#### IV. WIRETAPS, COMPUTER BREACH, TRACKING DEVICES

##### A. Interception of Communications - Federal and State Law

The Electronic Communications Privacy Act of 1986 (ECPA Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U.S.C. § 2510[2]) was enacted by the United States Congress to extend government restrictions on wire taps from telephone calls to include transmissions of

electronic data by computer. Specifically, ECPA was an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Statute), which was primarily designed to prevent unauthorized government access to private electronic communications. The ECPA also added new provisions prohibiting access to stored electronic communications, i.e., the Stored Communications Act, 18 U.S.C. §§ 2701-2712. The ECPA also included so-called pen/trap provisions that permit the tracing of telephone communications. §§ 3121-3127. Later, the ECPA was amended, and weakened to some extent, by some provisions of the USA PATRIOT Act. In addition, Section 2709 of the Act, which allowed the FBI to issue National Security Letters (NSLs) to Internet service providers (ISPs) ordering them to disclose records about their customers, was ruled unconstitutional under the First (and possibly Fourth) Amendments in *ACLU v. Ashcroft* (2004). It is thought that this could be applied to other uses of National Security Letters. See Wikipedia, ECPA.

This portion of the paper and Appendix 1 is adapted from “Spy Torts” by John Nichols, Sr., Brandi Branch, and Richel Rivers, presented at the CLE Webcast “Spy Torts” on February 13, 2007 at Texas Law Center. The author would like to thank Mr. Nichols, Ms. Branch and Ms. Rivers for their permission to use their outstanding and comprehensive article.

The reader is encouraged to spend some time reviewing this section and the accompanying Appendix to familiarize yourself with the applicable Federal and State Statutes.

1. The Federal Stored Wire and Electronic Communications Act (“Stored Communications Act”)

The Stored Communication Act prohibits: (1) the intentional accessing of a facility through which an electronic communication service is provided without authorization; or (2) the intentional exceeding of an authorization to access a facility; and thus, obtaining, altering, or preventing authorized access to a wire or electronic communication (such as, e-mail or voice mail) while it is in

electronic storage. 18 U.S.C. §2701(a).

The Act defines “electronic communication service” as any service that provides users the ability to send or receive wire or electronic communications. 18 U.S.C. §2510(15).

The Act defines “electronic storage” as: (1) “any temporary, immediate storage of a wire or electronic communication incidental to the electronic transmission thereof;” and (2) “any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. §2510(17)(2000). Possible penalties include a fine, imprisonment, or both. 18 U.S.C. §2701(b). Several courts have interpreted the definition of “electronic storage.” In *Fraser v. Nationwide Mutual Insurance Co.* 135 F. Supp.2d 623 (E.D. Pa. 2001), the Eastern District Court of Pennsylvania held that access to e-mail on a hard drive was not subject to the Stored Communications Act. The court reasoned that the “post-transmission storage [on a hard drive]” is not commensurate with “electronic storage” as contemplated by the Act. A New Jersey court in *White v. White*, 781 A.2d 85 (N.J. Super Ct. Ch. Div. 2001) tested the holding of *Fraser*. The state court evaluated the applicability of the Act, as well as state statutes, to interspousal access to e-mail stored on a computer in the family home. After Wife discovered a letter from Husband to his girlfriend, allegedly in plain view, Wife hired a computer detective. The detective, at Wife’s discretion and without using Husband’s password, copied his emails that were stored on the hard drive. *Id.* at 87. The New

Jersey Court held that Wife did not violate the Act because: (1) the e-mail was not in “electronic storage” when it was accessed because the family computer’s hard drive was not “electronic storage” and (2) the access was not “without authorization” as contemplated by the Act. *Id.* at 87. Nevertheless, the

Western District Court of Wisconsin in *Fischer v. Mt. Olive Lutheran Church*, 207 F. Supp.2d 914 (W.D. Wis. 2002) held that the Act does apply to stored e-mail – at least in some situations. The court found that e-mails from a Hotmail account that were accessed without authorization were stored by an electronic communication service because the e-mails were saved on Hotmail’s servers. *Id.* at 925.

## 2. The Federal Wiretap Act

The Federal Wiretap Act specifically prohibits “any person” from intercepting a wire, oral, or electronic communication without a court order or the consent of one of the parties to the conversation. 18 U.S.C. §§2510-2520. The Act defines “intercept” as 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.” 18 U.S.C. §2510(4). The interception must be intentional. 18 U.S.C. §2511(1). The penalty for violations may be a fine, imprisonment for up to five years, or both.

There are exceptions such as:

a. Consent of a Party. It is not unlawful for a person to intercept an oral or wire communication if the person is a party to the communication or if a party to the communication has given prior consent to the interception. 18 U.S.C. §2511(2)(d).

b. Spousal Consent. Though most federal circuits have not recognized an interspousal exception to the wiretapping statute, the Second and Fifth circuit courts of appeals have held that there is such an exception to the statute. *Simpson v. Simpson*, 490 F.2d 803 (5th Cir.

1974); *Anonymous v. Anonymous*, 558 F.2d 677 (2d Cir. 1977).

In *Simpson v. Simpson*, the Fifth Circuit Court of Appeals held that the recording of telephone conversations in the marital home by Husband who suspected Wife of infidelity did not violate the Federal Wiretap Act. 490 F.2d 803 (5<sup>th</sup> Cir. 1974) The Court reasoned that because federal courts have typically left family matters to state courts, Congress did not intend to counteract this tradition through the Federal Wiretap Act. Similarly, the Second Circuit Court of Appeals in *Anonymous v. Anonymous* found that interspousal wiretaps involve marital disputes, which are an area generally left to the discretion of states. 558 F.2d 677 (2d Cir. 1977). These opinions have been widely criticized and rejected by other federal courts which have found no Congressional intent to exception willful, intercepted spousal communications. See *United States v. Jones*, 542 F.2d 661 (6<sup>th</sup> Cir. 1976). See also *Pritchard v. Pritchard*, 732 F.2d 372 (4<sup>th</sup> Cir. 1984); *Kempf v. Kempf*, 868 F.2d 970, 973 (8<sup>th</sup> Cir. 1989); *Heggy v. Heggy*, 944 F.2d 1537, 1539 (10<sup>th</sup> Cir. 1991); *Platt v. Platt*, 951 F.2d 159 (8<sup>th</sup> Cir. 1989).

c. Vicarious Consent. Some courts have recognized a limited “vicarious consent” exceptions in cases where parents have tape recorded the phone conversations of their minor children within the home. The Federal Wiretap Act may not be violated if a party to the intercepted conversation has “vicariously” consented to the recording. State and federal courts have found that parents and guardians of minors have the authority to consent for their minor child when it is perceived by the parent or guardian to be in the best interests of the child. See *Wagner v. Wagner*, 64 F. Supp. 895, 896 (D. Minn. 1999); *March v. Levine*, 136 F Supp.2d 831, 849 (M.D. Tenn. 2000), *aff’d*, 248 F.3d 462 (6<sup>th</sup> Cir. 2001); *Allen v. Mancini*, 170 S.W.3d 167 (Tex.App.–Eastland 2005, *pet. filed*). In *Pollock v. Pollock*, 154 F.3d 601 (6<sup>th</sup> Cir. 1998) the Sixth Circuit Court of Appeals articulated a “good faith” test. The court held that, if the parent has a “good faith, reasonable basis for believing such consent was necessary for the welfare of the child,” then a recording of a child’s conversation would be admissible. See *id.* at 610. The Court also found that the parent doing the recording on behalf of the minor child must demonstrate a reasonable belief “... that the minor child

is being abused, threatened, or intimidated by the other parent.” *Silas v. Silas*, 680 So.2d 368, 371 (Ala.Civ.App. 1996). The exception does not apply to every situation. The West Virginia Supreme Court of Appeals in *West Virginia Dep’t of Health and Human Resources v. David L.*, 453 S.E.2d 646, 654 (1994) found that a parent did not have a right to record conversations with the other parent while the children were in the other parent’s house.

#### d. Criticism of ECPA

Recently a group formed to revise the ECPA due to many problems associated with the ACT. See <http://www.digitaldueprocess.org>

Among the problems they reported were the following:

Since enactment of ECPA, there have been fundamental changes in communications technology and the way people use it, including -

**Email:** Most Americans have embraced email in their professional and personal lives and use it daily for confidential communications of a personal or business nature. Because of the importance of email and unlimited storage capabilities available today, most people save their email indefinitely, just as they previously saved letters and other correspondence. The difference, of course, is that it is easier to save, search and retrieve digital communications. Many of us now have many years worth of stored email. Moreover, for many people, much of that email is stored on the computers of service providers.

**Mobile location:** Cell phones and mobile Internet devices constantly generate location data that supports both the underlying service and a growing range of location-based services of great convenience and value. This location data can be intercepted in realtime, and is often stored in easily accessible logs files. Location data can reveal a person’s movements, from which inferences can be drawn about activities and associations. Location data is augmented by very precise GPS data being installed in a growing number of devices.

**Cloud computing:** Increasingly, businesses and individuals are storing data "in the cloud," with

potentially huge benefits in terms of cost, security, flexibility and the ability to share and collaborate.

**Social networking:** One of the most striking developments of the past few years has been the remarkable growth of social networking. Hundreds of millions of people now use these social media services to share information with friends and as an alternative platform for private communications.

In the face of these developments, ECPA does not provide protection suited to the way technology is used today:

**Conflicting standards and illogical distinctions:** ECPA sets rules for governmental access to email and stored documents that are not consistent. A single email is subject to multiple different legal standards in its lifecycle, from the moment it is being typed to the moment it is opened by the recipient to the time it is stored with the email service provider. To take another example, a document stored on a desktop computer is protected by the warrant requirement of the Fourth Amendment, but the ECPA says that the same document stored with a service provider may not be subject to the warrant requirement.

**Unclear standards:** ECPA does not clearly state the standard for governmental access to location information.

**Judicial criticism:** The courts have repeatedly criticized ECPA for being confusing and difficult to apply. The Ninth Circuit in 2002 said that Internet surveillance was "a confusing and uncertain area of the law." In the past 5 years, no fewer than 30 federal opinions have been published on government access to cell phone location information, reaching a variety of conclusions.

**Constitutional uncertainty:** The courts are equally conflicted about the application of the Fourth Amendment to new services and information. A district court in Oregon recently opined that email is not covered by the constitutional protections, while the Ninth Circuit has held precisely the opposite. Last year, a panel of the Sixth Circuit first ruled that email was protected by the Constitution and then a larger panel of the court vacated the opinion.

This murky legal landscape does not serve the government, customers or service providers well

Customers are, at best, confused about the security of their data in response to an access request from law enforcement. Companies are uncertain of their responsibilities and unable to assure their customers that subscriber data will be uniformly protected. The current state of the law does not well serve law enforcement interests either as resources are wasted on litigation over applicable standards, and prosecutions are in jeopardy should the courts ultimately rule on the Constitutional questions.

## B. Interception of Communications - The Texas Counterparts

### 1. Texas Wiretap Statutes

Texas Civil Practice and Remedies Code §123.002(1) provides that:

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 a communication;

(2) uses or divulges information that the person 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.

For purposes of the statute, "interception" means "the aural acquisition of the contents for a communication through the use of an electronic, mechanical, or other device that is made without the consent of a party to the communication." TEX.CIV. PRAC.&REM. CODE §123.001(2). A person who establishes a cause of action under the statute is entitled to: "(1) an injunction prohibiting further interception or divulgence or use of the 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 to be determined by the court or jury; and (5) reasonable attorney's fees and costs." TEX.CIV.PRAC.&REM CODE §123.004.

Section 16.02 of the Texas Penal Code creates a criminal offense for the unlawful interception of wire, oral, or electronic communications. Under §16.02(b)(1):

a person commits the offense of unlawful interception, use, or disclosure of wire, oral, or electronic communications "if the person intentionally intercepts, endeavors to intercept, or procures another person to intercept or endeavor to intercept a wire, oral, or electronic communication." An offense under this section is a second degree felony. 96 92 See id.; *Silas v. Silas*, 680 So.2d 368, 371 (Ala. Civ. App. 1996). 93 453 S.E.2d 646, 654 (1994 ).

TEX.PEN.CODE 16.02(f).

Exception: Express or Implied Consent. Texas law allows one party to a conversation to tape or intercept the conversation. *Kotria v. Kotria*, 718 S.W.2d 853, 855 (Tex.App.–Corpus Christi 1986, writ ref'd n.r.e.).

Non-exception: Spousal Consent. Texas does not recognize the interspousal exception to wiretapping. *Collins v. Collins*, 904 S.W.2d 792 (Tex.App.–Houston [1<sup>st</sup> Dist.] 1995, writ denied). Texas courts generally have declined to follow the *Simpson* case to attach a spousal immunity exception to applicable federal or state wiretap statutes. See *Kent v. State*, 809 S.W.2d 664 (Tex.App.–Amarillo 1992, writ ref'd).

### 2. Breach of Computer Security

Section 33.02 of the Texas Penal Code provides that:

"[a] person commits an offense if the person knowingly accesses a computer,

computer network, or computer system without the effective consent of the owner.” An offense under this section is a class B misdemeanor. If the person who commits the offense knowingly obtains a benefit, defrauds or harms another, or alters, damages, or deletes property, the offense is based on the value of the harm done. TEX.PEN.CODE §33.02(2).

### 3. Tracking Devices

Section 16.06 of the Texas Penal Code provides that a person commits the offense of unlawful installation of a tracking device “if the person knowingly installs an electronic or mechanical tracking device on a motor vehicle owned or leased by another person.” Such an offense is a Class A misdemeanor. TEX.PEN.CODE § 16.06(c).

See *Electronic Evidence - Spy Torts*, John Nichols, Sr., Brandi Branch and Richel Rivers, 34<sup>th</sup> Annual Advanced Family Law Course, Chapter 50.2, August 2008

## V. SPYWARE

Spyware equipment can range from simple (Maxwell Smart) to highly complex. A tape recorder, a mobile phone, an EZ tag, a webcam and a computer all can all be used to find information.

### A. GPS (Global Positioning System)

Until recently, tracking people with Global Positioning System technology required purchasing expensive hardware and software. Now, complete solutions are available through cellular service providers. Here is background information and a few options for keeping up with the whereabouts of your family, friends and employees.

Locating People in an Emergency. The increased demand for enhanced 911 (e911) emergency calling capabilities, stimulated by the events of September 11, 2001, has pushed forward GPS tracking technology in cell phones. At the end of 2005, all cell phone carriers were required to provide the ability to trace cell phone

calls to a location within 100 meters or less.

To comply with FCC requirements, cell phone carriers decided to integrate GPS technology into cell phone handsets, rather than overhaul the tower network. However, the GPS in most cell phones is not like those in a GPS receiver that might be used for hiking. Most cell phones do not allow the user direct access to the GPS data. Accurate location determination requires the assistance of the wireless network, and the GPS data is transmitted only if a 911 emergency call is made. So, in general, you can not track someone using their cell phone, unless the person you want to track has the right kind of cell phone, connected to the right network, with the right service.

### 1. GPS-enabled Cell Phones

Motorola and Blackberry were the first GPS-enabled phones to proliferate the United States. Initially, Motorola "iDEN" phones were commonly used for employee tracking on the business-oriented Nextel network. Then GPS enabled Blackberry phones, once used almost exclusively by corporate and government VIPs, began to penetrate the consumer market stimulated by the demand for phones with advanced messaging capability. Next came specialty devices produced under the names of "Disney Mobile" and "Wherify Wireless" targeting use by children and elderly. Of course with Google Maps and the proliferation of iPhones we have seen a tremendous increase in products capable of tracking. Now in 2010, a variety of GPS-enabled phones and tracking services are available.

### 2. Wireless Networks.

In the United States, the wireless networks used for GPS tracking are primarily those operated by cell phone carriers. It is not likely that an individual will negotiate network access with a carrier. It is more likely that an individual will select a solution including a cell phone provisioned to communicate in a certain way on a specific wireless network. Listed below are some carriers for use with GPS cell phones and services.

a. T-Mobile/Cingular/AT&T - The Global System for Mobile (GSM) communications as adopted by these carriers represents the network with the largest coverage footprint. Roaming agreements between these carriers provide end users with service throughout the country. GSM is also the prominent cellular network abroad.

b. Sprint/Nextel, not so much because of coverage, but because of their emphasis on data. Nextel has created their own data formats and communication protocols for high bandwidth mobile electronics applications. This company, who gave new meaning to the term "walkietalkie", provides the most flexibility for the communication of GPS data between cell phones and location-based service providers. Recent co-operation between Sprint and Nextel has increased this network's footprint.

c. Location-Based Services (LBS) - LBS providers have agreements with the wireless network carriers to receive data from a cell phone and make it accessible to you via an Internet web site or call center. Most all LBS providers will be able to tell you the approximate last known location, but beyond that, services offered will vary, depending on the type of cell phone and the capabilities of the service provider.

d. Accutracking - Accutracking is a full-featured low-cost LBS provider using Motorola, Boost Mobile and Blackberry phones operating on the Sprint/Nextel network. See [Accutracking.com](http://Accutracking.com)

e. Sprint's Mobile Locator - Nextel's Mobile Locator is a service used in conjunction with Nextel calling plans using Nextel GPS-enabled phones. Mobile locator allows you to view and monitor your people's location in real-time, either singly or within a group, on a zoomable, online map. The web interface allows you to view location history, based on your most recent queries. See: [Sprint Mobile\\_Locator](http://Sprint_Mobile_Locator) web site for more information.

f. Mapquest Find Me - Using certain models of Nextel phones, you can view a group of your peoples' locations on one map, or you can view a track of an individual's location history. Powered by uLocate, Mapquest provides a web interface for mobile devices like PDAs as well cell phones. Other features include in-depth location history detail. See [www.mapquestfindme.com](http://www.mapquestfindme.com).

g. Wherify Wireless - Developers of the "Wherifone" designed specifically for children, seniors, and business users. The Wherifone is supported solely by Wherify's Global Location Service Center. See: [Wherify.com](http://Wherify.com).

h. Google Latitude - Free when downloaded and installed Google Latitude will track your cell phone.

i. Additional Points to Consider:

i. Permissions and Privacy. Simply put, tracking someone without their knowledge can get you in trouble. Typically, the subscriber must give permission and the cell phone must be enabled for tracking. Consult with the service provider for more detail.

ii. Tracking Application "Persistence." Again, the tracking application on a cell phone typically must be enabled by the user. Depending on the equipment, the application may persist - remaining enabled when the phone is turned on after having been turned off. This feature is particularly handy if you do not want to instruct the person using the phone on how to turn tracking on and off.

iii. Passive Tracking. Some tracking devices will record location data internally so that it can be downloaded later. Also referred to "data logging," which can provide location data even when the device has traveled outside the wireless network. Passive tracking is not a common feature built-in to cell phones (at the time this article was published), but more sophisticated java-enabled cell phones, PDAs, and other mobile devices may have this feature. Consult with the LBS provider to see if their application can accommodate passive tracking data from the more sophisticated tracking devices.

v. Assisted GPS (AGPS). Some cell phones can receive ephemerid information on the GPS satellites, which speeds up the initial position fix. AGPS information may also help in finding satellites and getting positions in difficult conditions. To have AGPS features, services must be set up to provide AGPS information to the cell phone and the cell phone must be able to process AGPS information. Note, the Apple IPHONE uses AGPS.

v. Tower reports. In the absence of an accurate GPS location, service providers may record the location of the nearest cell tower. Check with the LBS to determine if Tower locations are used to determine cell phone locations. Zoombak now implements LBS.

vi. GeoFencing. GeoFencing is a term used to describe a feature that enables the cell phone to only start

tracking when it has entered or exited a predefined region, avoiding unnecessary tracking when your people are close to home, office, or school. Or GeoFencing may also mean that an alert is sent when their phone crosses a virtual fence. For example, AccuTracking will send email or SMS message when they move across the designated areas.

vii. Speed Alerts. Some LBS providers provide email or SMS message alerts when specified speed limits are exceeded.

viii. Tracking Map Quality. Most location services do not produce their own maps. Instead they purchase or license mapping products from other companies. Several popular services use Mapquest maps. Indeed, Mapquest can produce a map for just about anywhere in the world, but the service provider's license may be limited to United States. Microsoft MapPoint and Tiger map data are also popular for applications in the United States. If choosing between LBS providers, compare what the maps will look like. Aerial photos – street names are not available from an aerial photo but there is a better idea of the surrounding environment. The better location services will provide both maps and aerial photos.

ix. Usage Costs. The costs associated with using the GPS for people tracking, include equipment costs, setup/activation fees, and usually network access subscriptions. In addition, the location service may charge for each location report or allot a limited number of reports and charge a premium for overages. For example Disney Mobile includes 5 location reports each month, but unlimited reporting is available as an optional plan.

x. Mobile to Mobile Tracking. Some tracking solutions enable access to tracking maps on a mobile device. The ability to track someone using a cell phone, by using another cell phone, conjures up a chase scene from an old movie, where our hero is sitting in the back seat of a moving car with a radar-type device in a briefcase, shouting turn-by-turn directions to the driver in hot pursuit of evil villains.

j. **CAVEAT EMPTOR:** A husband buys a new cell phone for his wife and activates a real time GPS plan. The program is hidden on her phone or Blackberry and the wife has no idea that wherever she goes she can be tracked.

In one of my favorite stories, a wife noted her husband going out at night on a regular basis, allegedly to his office, and she became suspect about her husband's activities. The wife remembered that the husband had installed an EZTAG on their car. When the wife checked the online log, it showed that while the husband's office was located South on the Hardy Toll Way; the husband was always headed North on the toll way every evening he claimed he was going to the office.

Occasionally a client will inquire about hiring a Private Investigator to place a GPS device on the spouses' care. Please be advised that it is a violation of Texas law to install a tracking device on a vehicle unless the vehicle is registered in the client's name. See Occupations Code Chapter 1702, Section 17.02.332. Also see Section 16.06 of the Texas Penal Code which states as follows:

(b) A person commits an offense if the person knowingly installs an electronic or mechanical tracking device on a motor vehicle owned or leased by another person.

(c) An offense under this section is a Class A misdemeanor.

Note that the same rules may not apply to law enforcement as revealed in *United States of America, Plaintiff-Appellee, v. Bernardo Garcia, Defendant-Appellant*. United States of Appeals for the Seventh Circuit, No. 06-2741, January 10, 2007, Argued-February 2, 2007, Decided 474 F.3d 994, wherein the police attached a GPS device to a suspect and the 7<sup>th</sup> Circuit found no violation of the suspect's constitutional rights. Here is an example of a blackberry or Windows Mobile program that provides GPS tracking and hides the program so that the user is unaware of its presence.

## VI. "THE GOOD, THE BAD AND THE UGLY"

As one individual said "I wouldn't fight for custody of the kids. I would fight for custody of the computer."

### A. The PI Takes Everyone Down.

Instead of explaining the risk of using technology in family law cases, the following case indicates the dangers associated with the improper intersection of technology and family law. United States District Court for the Central District of California, February 2005,

Grand Jury, United States of America, CR No. 05-1046 (c)-RMT, Plaintiff v. Anthony Pellicano, Mark Arneson, Rayford Earl Turner, Kevin Kachikian, Robert Pfeifer, Abner Nicherie, Daniel Nicherie, and Terry Christensen, Defendants, (Third Superseding Indictment) 18 U.S.C. §1962(c): (Racketeer Influenced and Corrupt Organizations (RICO)); 18 U.S.C. §1962(d): (RIC Conspiracy); 18 U.S.C. §§ 1343, 1346 (Honest Services Wire Fraud); 18 U.S.C. § 1030(a)(2)(B), (c)(2)(B) (I):(Unauthorized Computer Access of United States Agency Information); 18 U.S.C. §1028(a)(7): (Identity Theft); 18 U.S.C. §1030(a)(4): (Computer Fraud); 18 U.S.C. §371 (Conspiracy); 18 U.S.C. §2511 (1)(a), (d) (Interception of Wire Communication); 18 U.S.C. §2512 (1)(b): (Possession of Wiretapping Device); 18 U.S.C. §1001 (a)(2): (False Statements); 18 U.S.C. §1512(b)(3): (Witness Tampering); 18 U.S.C. §1512 (c) (1): (Destruction of Evidence); 18 U.S.C. §2 (Aiding and Abetting and Causing an Act to be Done); 18 U.S.C. § 1963 (RICO Forfeiture).

Pellicano was the “PI for the Stars” and after 9 days of jury deliberation (he represented himself) was convicted on 76 of the 77 charges contained in the indictment against him. The last name in the indictment was a lawyer, Terry Christensen, who according to a February 20, 2008 article in the LA Times stated:

Christensen is accused of paying Pellicano \$100,000 to wiretap the former wife of Christensen’s longtime client, Kirk Kerkorian, to gain a tactical edge in a bitter child-support case between the billionaire investor and his wife, Lisa Bonder Kerkorian. Christensen has long helped Kerkorian, one of the nation’s richest people and a Hollywood fixture for more than 30 years, oversee a vast empire that includes the MGM Grand and Bellagio hotels and, until last year, the MGM studio.

According to the indictment, the wiretapping of Lisa Kerkorian began March 15, 2002, when an attorney called Pellicano and told him to contact Christensen about “going after” the wife’s attorney in the child custody dispute. During snippets of alleged conversations included in the indictment, Pellicano alluded to eavesdropping on conversations between Lisa Kerorian and her attorneys that could help

Christensen with a court hearing. Pellicano also told Christensen to “be careful” about the information he was receiving from the private eye because “there is only one way for me to know this,” the indictment said. To add to Christensen’s problems, Pellicano is reported to have recorded his conversations with Christensen. See Vanity Fair, June, 2006. If you ever needed to know what Federal Laws apply to wire tapping, just review the U.S.C. sections contained in this indictment.

As lawyers we have a duty to use due diligence in the hiring and oversight of private investigators. In the case of *Noble v. Sears, Roebuck and Co.*, 33 Cal.App.3rd 654, (July 25, 1973) the California Court concluded that Seas and it’s attorney’s may have vicarious liability for the acts of its agents, i.e., the private detective agency. The California Court found actionable “invasion of privacy” and “neglect entrustment of agents” claims by the Plaintiff.

The Court also noted: “the Florida Supreme Court recognized that an investigation done by trailing and shadowing a claimant could amount to an actionable invasion of privacy, if it is unreasonably intrusive. (*Tucker v. American Employers’ Insurance Company* (Fla.App.1965) 171 So2d 437 [13 A.L.R.3d 1020].) It is uncertain as to whether Texas would follow a vicarious liability theory, but caution should be taken when employing private investigators. Also remember, Intentional Torts are not covered by malpractice insurance. See Parker and Pine, *The Pellican’s mess, Ethical Considerations for Attorney’s Who Hire Private Investigator’s in the Wake of Pellicano*, June, 2006, <http://www.pmmlaw.com>.

## B. Spyware on the Mobile Phone

The advertisement reads:

*How to Tell if Your Wife or Girlfriend is Cheating on You*

To catch a cheating wife or girlfriend you need to be able to reveal all on her mobile. XXXX will give you this information and put your mind to rest. Listen to their phone conversation with XXXX mobile call tapping and gps tracker can be installed invisibly on

most cell phone, Blackberry, Windows Mobile, etc.; can provide :

Calls History  
SMS History  
Contacts  
Appointments History  
Internet Browsing History  
Bookmarks History  
Emails History  
Current Location  
Location History  
Calls Recording History  
Surround Recording  
History  
Pictures History  
Videos History  
GPS tracking  
Capture text message  
3 way calling - a party can listen in on another parties cell phone calls  
Can remotely activate the cell phone's microphone  
Chronicle every cell phone call made or received  
And coming in the future the program will activate the cell phone's camera/video recorder..

All this for \$39.00 to \$400.00.

### C. Spyware On Your Computer

Most key logger programs are available for less than \$100.00 and can readily be purchased in computers stores and via the internet. What the programs share in common is the ability to capture the following:

- i. Every email;
- ii. Most of the most popular IM programs text
- iii. Websites visited;
- iv. Peer-to Peer activity;
- v. Keystrokes including name and password;
- vi. Screenshots;
- vii. Program activity; and
- viii. Pictures.

The key logger programs also run in stealth mode and some now provide web access - no longer requiring access to the actual computer where the spyware was installed versus emailing you the content.

The Federal Court held in *United States v. Ropp*, 347 F. Supp.2d 831 (C.D.Cal.2004):

Because the key logger in *Ropp* recorded the keystroke information in transit between the keyboard and the CPU, the court found that the system transmitting the information did not affect interstate commerce as the statute requires. *Ropp*, 347 F.Supp.2d 837-38. the keystroke signals, therefore, were not "electronic communication" under the Wiretap Act.

On February 14<sup>th</sup>, the District Court for the Southern District of Ohio ruled that evidence obtained in a divorce case through the use of spyware could be admitted, Judge Thomas Rose refused to grant an injunction preventing the evidence from being admitted, noting that the Electronic Communications Privacy Act does not permit courts to disallow such evidence, saying that appears courts "have concluded that Congress intentionally omitted illegally intercepted electronic communications from the category of cases in which the remedy of suppression is available." Jeffrey Havlicek admitted installing monitoring software on the family computer. He also admitted to downloading e-mail from his wife Amy's Web-based email account, but claimed it was authorized because she had chosen to save her username and password through the browser's "remember me" feature. Though Rose declined to grant the injunction, he did say that "disclosure of the information in state court by Jeffery Havlicek or his attorney might be actionable civilly or criminally." He suggested that the "remember me" option probably didn't give Jeffery an implied right to view his wife's e-mail messages. The case may be found on Westlaw at 2007 WL 539534 (S.D.Ohio) *Potter v. Havlicek*.

Also the court in *Porter v. Havlicek, supra* questioned whether *Ropp's* construction of "affecting interstate commerce" is correct. It suggested that *Ropp* reads the statute as requiring that the communication must be traveling in interstate commerce as opposed to merely "affecting interstate commerce." The keystrokes, while not traveling in interstate commerce, do "affect interstate commerce."

### VII. CONCLUSION

Simply stated: FOREWARNED IS FOREARMED.

## Appendix 1

### Chapter 123. Interception of Communication

#### §123.001 Definitions

#### §123.002 Cause of Action

#### §123.003 Defense

#### §123.004 Damages

### CPRC §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.

History of CPRC §123.001: Acts 1985, 69th Leg., ch. 959, §1, eff. Sept. 1, 1985.

See also CCP art. 18.20; 18 U.S.C. §§2510-2522 (Federal Wiretap Statute).

*Collins v. Collins*, 904 S.W.2d 792, 798 (Tex.App.—Houston [1st Dist.] 1995), *writ denied*, 923 S.W.2d 569 (Tex.1996). “The state wiretap statute makes it illegal to tape a conversation ‘without the consent’ of the person being recorded. The wife, who had the right to talk with their child, did not consent to be taped by speaking with the child over the telephone. Her only option was not to talk with their child over the telephone. This Hobson’s choice was not a waiver of objections or a consent to recording. “We hold the wife did not waive her objections to the post-order taping of her conversations with their child.”

*Kotrla v. Kotrla*, 718 S.W.2d 853, 855 (Tex.App.—Corpus Christi 1986, *writ ref’d n.r.e.*). “Article 9019 [now CPRC §123.002] confers a cause of action upon a party to a communication who has been the victim of an ‘eavesdropping.’ “The statute provides that ‘interception’ occurs when a ‘communication’ is acquired ‘without the consent of a party to the communication.’ In this case, ‘a party,’ ... consented to the recording. The statute is therefore inapplicable under these facts.”

### CPRC §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.

History of CPRC §123.002: Acts 1985, 69th Leg., ch. 959, §1, eff. Sept. 1, 1985.

See also CCP art. 18.20; 18 U.S.C. §§2510-2522 (Federal Wiretap Statute).

**Collins v. Collins**, 904 S.W.2d 792, 797 (Tex.App.—Houston [1st Dist.] 1995), *writ denied*, 923 S.W.2d 569 (Tex. 1996). “Neither the state nor the federal wiretap statutes contain any exception for wiretaps between spouses.” [S]pouses, as any other persons, have rights of privacy under [federal and state] wiretap statutes. *At 799*: Section 123.002 of the state wiretap statute states that a party has a cause of action against any person who ‘divulges information’ that was obtained by an illegal wiretap.... Because the tapes were illegally obtained under the federal and state statutes, the trial court should not have admitted them into evidence on the issue of custody. *At 804*: An action under the state wiretap statute sounds in tort and is controlled by a 2-year statute of limitations.”

**Figure World Inc. v. Farley**, 680 S.W.2d 33, 35 (Tex.App.—Austin 1984, *writ ref’d n.r.e.*). “We hold that [plaintiff] failed to prove she had been the victim of any activity prohibited by art. 9019 [now CPRC §123.002]. The evidence introduced in the trial court proved only that the appellant had the capacity to intercept conversations in the sales offices. There was no testimony or other evidence that the eavesdropping devices were ever used while [plaintiff] was in one of the sales offices. While the practice a violation under even the most liberal interpretation of the statute.”

**Peavy v. WFAA-TV, Inc.**, 221 F.3d 158, 170 (5th Cir. 2000). “The Texas Act does not define ‘obtains’....” Webster defines it as ‘to gain or attain possession or disposal of usu[ally] by some planned action or method’ .... “In the absence of a statutory definition, statutory language is measured by common understanding and practices.” Held: Common understanding of “obtain” is to gain or attain by planned action or effort.

#### CPRC §123.003. DEFENSE

(a) A switchboard operator or an officer, employee, or agent of a communication common carrier whose facilities are used in the transmission of a wire communication may intercept, disclose, or use a communication in the normal course of employment if engaged in an activity that is necessary to service or for the protection of the carrier’s rights or property. A communication common carrier may not use service observation or random monitoring except for mechanical or service quality control checks.

(b) It is a defense to an action under Section 123.002 that an interception, disclosure, or use of a communication is permitted by this section.

(c) A defendant must establish by a preponderance of the evidence a defense raised under this section.

History of CPRC §123.003: Acts 1985, 69th Leg., ch. 959, §1, eff. Sept. 1, 1985.

See also CCP art. 18.20; 18 U.S.C. §§2510-2522 (Federal Wiretap Statute).

**Peavy v. WFAA-TV, Inc.**, 221 F.3d 158, 176 (5th Cir.2000). “Defendants contend disclosures to WFAA employees of the contents of the interceptions are not actionable because a corporation cannot disclose information to itself. “ Defendants cite no authority for holding intra-organization disclosures are not violative of the [Federal & Texas] Wiretap Acts. The Acts authorize certain specified disclosures. Such exceptions do not include the types made by defendants. “Accordingly, such use and disclosure, during defendants’ investigation and newsgathering, are proscribed by the Federal and Texas Acts.”

#### CPRC §123.004. DAMAGES

(a) 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.

History of CPRC §123.004: Acts 1985, 69th Leg., ch. 959, §1, eff. Sept. 1, 1985. Amended by Acts 2001, 77th Leg., ch. 1049, §1, eff. Sept. 1, 2001.

**Collins v. Collins**, 904 S.W.2d 792, 799 (Tex.App.—Houston [1st Dist.] 1995), *writ denied*, 923 S.W.2d 569 (Tex. 1996). “Although the Texas wiretap statute does not specifically provide for the exclusion of illegally obtained ‘communications,’ the provisions for a cause of action for divulging wiretap information and the injunctive remedies provided in §123.004 [CPRC] are sufficient to rebut the presumption of admissibility under [TRCP] 402. “The tape-recorded conversations were not admissible because the criminal statute dealing with the use of the intercepted communications criminalizes their dissemination, and the civil statute provides a method to prevent dissemination. To permit such evidence to be introduced at trial when it is illegal to disseminate it would make the court a partner to the illegal conduct the statute seeks to proscribe.” *But see Kotrla v. Kotrla*, 718 S.W.2d 853, 855 (Tex.App.—Corpus Christi 1986, writ ref’d n.r.e.) (statute does not address *admissibility* of tape recording; tape recording, even if obtained without consent of party to it, is admissible if proper predicate is laid).

## Chapter 16. Criminal Instruments, Interception of Wire or Oral Communication, & Installation of Tracking Device

### §16.01 Unlawful Use of Criminal Instrument

### §16.02 Unlawful Interception, Use, or Disclosure of Wire, Oral, or Electronic Communications

### §16.03 Unlawful Use of Pen Register or Trap & Trace Device

### §16.04 Unlawful Access to Stored Communications

### §16.05 Illegal Divulgence of Public Communications

### §16.06 Unlawful Installation of Tracking Device

## PENC §16.01. UNLAWFUL USE OF CRIMINAL INSTRUMENT

(a) A person commits an offense if:

- (1) he possesses a criminal instrument with intent to use it in the commission of an offense; or
- (2) with knowledge of its character and with intent to use or aid or permit another to use in the commission of an offense, he manufactures, adapts, sells, installs, or sets up a criminal instrument.

(b) For the purpose of this section, “criminal instrument” means anything, the possession, manufacture, or sale of which is not otherwise an offense, that is specially designed, made, or adapted for use in the commission of an offense.

(c) An offense under Subsection (a)(1) is one category lower than the offense intended. An offense under Subsection (a)(2) is a state jail felony.

History of PenC §16.01: Acts 1973, 63rd Leg., ch. 399, §1, eff. Jan. 1, 1974. Amended by Acts 1975, 64th Leg., ch. 342, §7, eff. Sept. 1, 1975; Acts 1993, 73rd Leg., ch. 900, §1.01, eff. Sept. 1, 1994; Acts 1999, 76th Leg., ch. 728, §2, eff. Sept. 1, 1999.

**Danzi v. State**, 101 S.W.3d 786 (Tex.App.—El Paso 2003, pet. ref’d). Held: A “slim jim” is not a criminal instrument proscribed by §16.01(b).

**Ex parte Andrews**, 814 S.W.2d 839, 841 (Tex. App.—Houston [1st Dist.] 1991), *pet. dismiss’d sub nom. Ex parte Chunn*, 831 S.W.2d 326 (Tex.Crim.App.1992). “[T]he gravamen of the offense intended by the language used by the legislature is the physical adaptation of the alleged instrument for a specific criminal intent. [A]ny illegality to be proved is in the inherent characteristics of the object itself as adapted, and not in the conduct of defendants in using the object within a particular criminal episode. An object does not become a criminal instrument by the context of its use, but by the limited nature and specialized criminal use of its own distinctive properties.” *See also Janjua v. State*, 991 S.W.2d 419, 426 (Tex.App.—Houston [14th Dist.] 1999, no pet.).

## PENC §16.02. UNLAWFUL INTERCEPTION, USE, OR DISCLOSURE OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS

*Section 16.02 below was effective Sept. 1, 2005.*

‘16.02

(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 or endeavor 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:

(1) an operator of a switchboard or an officer, employee, or agent of a communication common carrier whose facilities are used in the transmission of a wire or electronic communication intercepts a communication or discloses or uses an intercepted communication in the normal course of employment while engaged in an activity that is a necessary incident to the rendition of service or to the protection of the rights or property of the carrier of the communication, unless the interception results from the communication common carrier's use of service observing or random monitoring for purposes other than mechanical or service quality control checks;

(2) an officer, employee, or agent of a communication common carrier provides information, facilities, or technical assistance to an investigative or law enforcement officer who is authorized as provided by this section to intercept a wire, oral, or electronic communication;

(3) a person acting under color of law intercepts:

(A) a wire, oral, or electronic communication, if the person is a party to the communication or if one of the parties to the communication has given prior consent to the interception;

(B) a wire, oral, or electronic communication, if the person is acting under the authority of Article 18.20, Code of Criminal Procedure; or

(C) a wire or electronic communication made by a computer trespasser and transmitted to, through, or from a protected computer, if:

(i) the interception did not acquire a communication other than one transmitted to or from the computer trespasser;

(ii) the owner of the protected computer consented to the interception of the computer trespasser's communications on the protected computer; and

(iii) actor was lawfully engaged in an ongoing criminal investigation and the actor had reasonable suspicion to believe that the contents of the computer trespasser's communications likely to be obtained would be material to the investigation;

(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;

- (5) a person acting under color of law intercepts a wire, oral, or electronic communication if:
- (A) oral or written consent for the interception is given by a magistrate before the interception;
  - (B) an immediate life-threatening situation exists;
  - (C) the person is a member of a law enforcement unit specially trained to:
    - (i) respond to and deal with life-threatening situations; or
    - (ii) install electronic, mechanical, or other devices; and
  - (D) the interception ceases immediately on termination of the life-threatening situation;
- (6) an officer, employee, or agent of the Federal Communications Commission intercepts a communication transmitted by radio or discloses or uses an intercepted communication in the normal course of employment and in the discharge of the monitoring responsibilities exercised by the Federal Communications Commission in the enforcement of Chapter 5, Title 47, United States Code; [FN1]
- (7) a person intercepts or obtains access to an electronic communication that was made through an electronic communication system that is configured to permit the communication to be readily accessible to the general public;
- (8) a person intercepts radio communication, other than a cordless telephone communication that is transmitted between a cordless telephone handset and a base unit, that is transmitted:
- (A) by a station for the use of the general public;
  - (B) to ships, aircraft, vehicles, or persons in distress;
  - (C) by a governmental, law enforcement, civil defense, private land mobile, or public safety communications system that is readily accessible to the general public, unless the radio communication is transmitted by a law enforcement representative to or from a mobile data terminal;
  - (D) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or
  - (E) by a marine or aeronautical communications system;
- (9) a person intercepts a wire or electronic communication the transmission of which causes harmful interference to a lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of the interference;
- (10) a user of the same frequency intercepts a radio communication made through a system that uses frequencies monitored by individuals engaged in the provision or the use of the system, if the communication is not scrambled or encrypted; or
- (11) a provider of electronic communications service records the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service towards the completion of the communication, or a user of that service from fraudulent, unlawful, or abusive use of the service.
- (d) A person commits an offense if the person:
- (1) intentionally manufactures, assembles, possesses, or sells an electronic, mechanical, or other device knowing or having reason to know that the device is designed primarily for nonconsensual interception of wire, electronic, or oral communications and that the device or a component of the device has been or will be used for an unlawful purpose; or
  - (2) places in a newspaper, magazine, handbill, or other publication an advertisement of an electronic, mechanical, or other device:
    - (A) knowing or having reason to know that the device is designed primarily for nonconsensual interception of wire, electronic, or oral communications;
    - (B) promoting the use of the device for the purpose of nonconsensual interception of wire, electronic, or oral communications; or
    - (C) knowing or having reason to know that the advertisement will promote the use of the device for the purpose of nonconsensual interception of wire, electronic, or oral communications.
- (e) It is an affirmative defense to prosecution under Subsection (d) that the manufacture, assembly, possession, or sale of an electronic, mechanical, or other device that is designed primarily for the purpose of nonconsensual interception of wire, electronic, or oral communication is by:
- (1) a communication common carrier or a provider of wire or electronic communications service or an officer, agent, or employee of or a person under contract with a communication common carrier or provider acting in the normal course of the provider's or communication carrier's business;
  - (2) an officer, agent, or employee of a person under contract with, bidding on contracts with, or doing business with the

United States or this state acting in the normal course of the activities of the United States or this state;

(3) a member of the Department of Public Safety who is specifically trained to install wire, oral, or electronic communications intercept equipment; or

(4) a member of a local law enforcement agency that has an established unit specifically designated to respond to and deal with life-threatening situations.

(f) An offense under this section is a felony of the second degree, unless the offense is committed under Subsection (d) or (g), in which event the offense is a state jail felony.

(g) A person commits an offense if, knowing that a government attorney or an investigative or law enforcement officer has been authorized or has applied for authorization to intercept wire, electronic, or oral communications, the person obstructs, impedes, prevents, gives notice to another of, or attempts to give notice to another of the interception.

(h) Repealed by Acts 2005, 79th Leg., ch. 889, § 1.16.02

PENC §16.021. DELETED

Deleted by Acts 1993, 73rd Leg., ch. 900, §1.01, eff. Sept. 1, 1994.

Penc §16.03. Unlawful Use of Pen Register or Trap & Trace Device

(a) A person commits an offense if the person knowingly installs or uses a pen register or trap and trace device to record or decode electronic or other impulses for the purpose of identifying telephone numbers dialed or otherwise transmitted on a telephone line.

(b) In this section, “authorized peace officer,” “communications common carrier,” “pen register,” and “trap and trace device” have the meanings assigned by Article 18.21, Code of Criminal Procedure.

(c) It is an affirmative defense to prosecution under Subsection (a) that the actor is:

(1) an officer, employee, or agent of a communications common carrier and the actor installs or uses a device or equipment to record a number dialed from or to a telephone instrument in the normal course of business of the carrier for purposes of:

(A) protecting property or services provided by the carrier; or

(B) assisting another who the actor reasonably believes to be a peace officer authorized to install or use a pen register or trap and trace device under Article 18.21, Code of Criminal Procedure;

(2) an officer, employee, or agent of a lawful enterprise and the actor installs or uses a device or equipment while engaged in an activity that:

(A) is a necessary incident to the rendition of service or to the protection of property of or services provided by the enterprise; and

(B) is not made for the purpose of gathering information for a law enforcement agency or private investigative agency, other than information related to the theft of communication or information services provided by the enterprise; or

(3) a person authorized to install or use a pen register or trap and trace device under Article 18.21, Code of Criminal Procedure.

(d) An offense under this section is a state jail felony.

History of PenC §16.03: Acts 1985, 69th Leg., ch. 587, §6, eff. Aug. 26, 1985. Amended by Acts 1989, 71st Leg., ch. 958, §2, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, §1.01, eff. Sept. 1, 1994; Acts 1997, 75th Leg., ch. 1051, §10, eff. Sept. 1, 1997.

#### PENC §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.

History of PenC §16.04: Acts 1989, 71st Leg., ch. 958, §3, eff. Sept. 1, 1989. Amended by Acts 1993, 73rd Leg., ch. 900, §1.01, eff. Sept. 1, 1994; Acts 1997, 75th Leg., ch. 1051, §11, eff. Sept. 1, 1997.

#### PENC §16.05. ILLEGAL DIVULGENCE OF PUBLIC COMMUNICATIONS

- (a) In this section, “electronic communication,” “electronic communications service,” and “electronic communications system” have the meanings given those terms in Article 18.20, Code of Criminal Procedure.
- (b) A person who provides electronic communications service to the public commits an offense if the person knowingly divulges the contents of a communication to another who is not the intended recipient of the communication.
- (c) It is an affirmative defense to prosecution under Subsection (b) that the actor divulged the contents of the communication:
  - (1) as authorized by federal or state law;
  - (2) to a person employed, authorized, or whose facilities are used to forward the communication to the communication’s destination; or
  - (3) to a law enforcement agency if the contents reasonably appear to pertain to the commission of a crime.
- (d) Except as provided by Subsection (e), an offense under Subsection (b) that involves a scrambled or encrypted radio communication is a state jail felony.
- (e) If committed for a tortious or illegal purpose or to gain a benefit, an offense under Subsection (b) that involves a radio communication that is not scrambled or encrypted:
  - (1) is a Class A misdemeanor if the communication is not a public land mobile radio service communication or a paging service communication; or
  - (2) is a Class C misdemeanor if the communication is a public land mobile radio service communication or a paging service communication.
- (f) Repealed by Acts 1997, 75th Leg., ch. 1051, §13, eff. Sept. 1, 1997.

History of PenC §16.05: Acts 1989, 71st Leg., ch. 1166, §17, eff. Sept. 1, 1989. Renumbered from §16.04 by Acts 1990, 71st Leg., 6th C.S., ch. 12, §2(24), eff. Sept. 6, 1990.

Amended by Acts 1993, 73rd Leg., ch. 900, §1.01, eff. Sept. 1, 1994; Acts 1997, 75th Leg., ch. 1051, §§12 & 13, eff. Sept. 1, 1997.

#### PENC §16.06. UNLAWFUL INSTALLATION OF TRACKING DEVICE

- (a) In this section:
  - (1) “Electronic or mechanical tracking device” means a device capable of emitting an electronic frequency or other signal that may be used by a person to identify, monitor, or record the location of another person or object.
  - (2) “Motor vehicle” has the meaning assigned by Section 501.002, Transportation Code.
- (b) A person commits an offense if the person knowingly installs an electronic or mechanical tracking device on a motor vehicle owned or leased by another person.
- (c) An offense under this section is a Class A misdemeanor.
- (d) It is an affirmative defense to prosecution under this section that the person:
  - (1) obtained the effective consent of the owner or lessee of the motor vehicle before the electronic or mechanical tracking device was installed;
  - (2) was a peace officer who installed the device in the course of a criminal investigation or pursuant to an order of a court to gather information for a law enforcement agency;
  - (3) assisted another whom the person reasonably believed to be a peace officer authorized to install the device in the

course of a criminal investigation or pursuant to an order of a court to gather information for a law enforcement agency;  
or

(4) was a private investigator licensed under Chapter 1702, Occupations Code, who installed the device:

(A) with written consent:

(i) to install the device given by the owner or lessee of the motor vehicle; and

(ii) to enter private residential property, if that entry was necessary to install the device, given by the owner or lessee of the property; or

(B) pursuant to an order of or other authorization from a court to gather information.

History of PenC §16.06: Acts 1999, 76th Leg., ch. 728, §1, eff. Sept. 1, 1999. Amended by Acts 2001, 77th Leg., ch. 1420, §14.828, eff. Sept. 1, 2001.

## PENAL CODE

### 2. TITLE 7. OFFENSES AGAINST PROPERTY

#### CHAPTER 33. COMPUTER CRIMES

Sec. 33.01. DEFINITIONS. In this chapter:

(1) "Access" means to approach, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer network, computer program, or computer system.

(2) "Aggregate amount" means the amount of:

(A) any direct or indirect loss incurred by a victim, including the value of money, property, or service stolen or rendered unrecoverable by the offense; or

(B) any expenditure required by the victim to verify that a computer, computer network, computer program, or computer system was not altered, acquired, damaged, deleted, or disrupted by the offense.

(3) "Communications common carrier" means a person who owns or operates a telephone system in this state that includes equipment or facilities for the conveyance, transmission, or reception of communications and who receives compensation from persons who use that system.

(4) "Computer" means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.

(5) "Computer network" means the interconnection of two or more computers or computer systems by satellite, microwave, line, or other communication medium with the capability to transmit information among the computers.

(6) "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data or perform specific functions.

(7) "Computer services" means the product of the use of a computer, the information stored in the computer, or the personnel supporting the computer, including computer time, data processing, and storage functions.

(8) "Computer system" means any combination of a computer or computer network with the documentation, computer software, or physical facilities supporting the computer or computer network.

(9) "Computer software" means a set of computer programs, procedures, and associated documentation related to the operation of a computer, computer system, or computer network.

(10) "Computer virus" means an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself or to affect the other programs or files in the computer by attaching a copy of the unwanted program or other set of instructions to one or more computer programs or files.

(11) "Data" means a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or processed, or has been stored or processed in a computer. Data may be embodied in any form, including but not limited to computer printouts, magnetic storage media, laser storage media, and punchcards, or may be stored internally in the memory of the computer.

(12) "Effective consent" includes consent by a person legally authorized to act for the owner. Consent is not effective if:

(A) induced by deception, as defined by Section 31.01, or induced by coercion;

(B) given by a person the actor knows is not legally authorized to act for the owner;

(C) given by a person who by reason of youth, mental disease or defect, or intoxication is known by the actor to be unable to make reasonable property dispositions;

(D) given solely to detect the commission of an offense; or

(E) used for a purpose other than that for which the consent was given.

(13) "Electric utility" has the meaning assigned by Section 31.002, Utilities Code.

(14) "Harm" includes partial or total alteration, damage, or erasure of stored data, interruption of computer services, introduction of a computer virus, or any other loss, disadvantage, or injury that might reasonably be suffered as a result of the actor's conduct.

(15) "Owner" means a person who:

(A) has title to the property, possession of the property, whether lawful or not, or a greater right to possession of the property than the actor;

(B) has the right to restrict access to the property; or

(C) is the licensee of data or computer software.

(16) "Property" means:

(A) tangible or intangible personal property including a computer, computer system, computer network, computer software, or data; or

(B) the use of a computer, computer system, computer network, computer software, or data.

Added by Acts 1985, 69th Leg., ch. 600, Sec. 1, eff. Sept. 1, 1985. Amended by Acts 1989, 71st Leg., ch. 306, Sec. 1, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994; Acts 1997, 75th Leg., ch. 306, Sec. 1, eff. Sept. 1, 1997; Acts 1999, 76th Leg., ch. 62, Sec. 18.44, eff. Sept. 1, 1999.

Sec. 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 but 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.

(c) When benefits are obtained, a victim is defrauded or harmed, or property is altered, damaged, or deleted in violation of this section, whether or not in a single incident, the conduct may be considered as one offense and the value of the benefits obtained and of the losses incurred because of the fraud, harm, or alteration, damage, or deletion of property may be aggregated in determining the grade of the offense.

(d) A person who his subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

Added by Acts 1985, 69th Leg., ch. 600, Sec. 1, eff. Sept. 1, 1985. Amended by Acts 1989, 71st Leg., ch. 306, Sec. 2, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994; Acts 1997, 75th Leg., ch. 306, Sec. 2, eff. Sept. 1, 1997; Acts 2001, 77th Leg., ch. 1411, Sec. 1, eff. Sept. 1, 2001.