ILLEGAL EVIDENCE:
WIRETAPPING, HACKING, AND DATA INTERCEPTION LAWS

HON. EMILY MISKEL
470th District Court
2100 Bloomdale Rd.
McKinney, Texas 75071
(972) 885-8510
emily@emilymiskel.com

State Bar of Texas
SEX, DRUGS, & SURVEILLANCE
April 19, 2017
Austin

CHAPTER 4

EMILY A. MISKEL

Judge, 470th District Court, Collin County, Texas
emily@emilymiskel.com ▪ www.emilymiskel.com

BIOGRAPHICAL INFORMATION

EDUCATION

Stanford University, B.S. in Mechanical Engineering, with distinction
Harvard Law School, J.D.

PROFESSIONAL AFFILIATIONS

Director, Harvard Club of Dallas
Barrister, Henderson Inn of Court
Member, Collaborative Law Institute of Texas
Member, Texas Academy of Family Law Specialists (TAFLS)

PROFESSIONAL RECOGNITION

Board Certified, Family Law — Texas Board of Legal Specialization
Super Lawyers Rising Star, 2012-2015
D Magazine Best Lawyers in Dallas, 2015
Young Lawyer of the Year, 2010-2011, Collin County Young Lawyers Association
2010 DAYL Leadership Class
Life Fellow, DAYL Foundation
Fellow, Texas Bar Foundation

RECENT PUBLICATIONS AND SPEECHES

Digital Dirt—The Impact of Social Media on Your Case, Innovations: Breaking Boundaries in Custody Litigation Course, State Bar of Texas (2017).
Presiding Judge, 2017 Trial Institute, Texas Academy of Family Law Specialists (2017).
Advice from Judges on How to Present Your Case in Any Texas Court, Handling Your First (or Next) Divorce Case Course, State Bar of Texas (2017).
Online Impersonation, Revenge Porn, and Other New Causes of Action, Family Law & Technology Course, State Bar of Texas (2016).
Planning Committee, Sex, Drugs & Surveillance Course, State Bar of Texas (2016-2017).
Reunification Therapy and Court Orders: Best Practices to be on the Same Page, 12th Symposium on Child Custody Evaluations, Association of Family and Conciliation Courts (2016).
The Trial Lawyers Toolbox – Technology Tools for Litigation, Technology for Litigators Course, State Bar of Texas (2016).
Planning Committee, Advanced Family Law Course, State Bar of Texas (2016-2017).
Peeping Toms in the New Millennium: Digital Dos and Don'ts, New Frontiers in Marital Property Course, State Bar of Texas (2016).
Restraining Orders, Protective Orders, and Peace Bonds, Collin County Council on Family Violence (2016).
Course Director, Handling Your First (or Next) Divorce Case Course, State Bar of Texas (2016-2017).
Prepare and Present a Case for Final Trial, Family Law 101 Course, State Bar of Texas (2016).
Cloudy with a Chance of Data, Advanced Criminal Law Course, State Bar of Texas (2016).
From Private Practice to the Bench: Practice Management Tips, Law Practice Management Section, Collin County Bar Association (2016).
Planning Committee, 2017 Trial Institute, Texas Academy of Family Law Specialists (2016-2017).
Presentation of Electronic Evidence, Collin County Bench Bar Conference (2016).
Everything You Always Wanted to Ask a Judge but Were Afraid They Would Know It Was Me, Family Law Section, Collin County Bar Association (2016).
SAPCR Overview – Presumptions, Burdens, Statutes, and Case Law, Family Law Section, Collin County Bar Association (2016).
Wiretapping & Data Interception in Civil and Family Law Cases, Circuits newsletter, Computer & Technology Section, State Bar of Texas (2016).
A New Judge's Lessons from the Bench: What I Wish I Knew While Practicing, Civil Litigation/Appellate Section, Collin County Bar Association (2016).
Wiretapping and Data Interception in Civil and Family Law Cases, Dallas Bar Association Headnotes (2015).
Inside the Justice System, Harvard Club of Dallas (2015).
Wiretapping, Collin County Criminal Defense Lawyers Association (2015).
Admissibility of Electronic Evidence: Present and Future Considerations, 2015 Annual Judicial Education Conference, Texas Center for the Judiciary (2015).
Electronically Stored Information A-Z: Acquire, Evaluate, Admit, Advanced Family Law Course, State Bar of Texas (2015), co-author.
Illegal Evidence, Plano Bar Association (2015).

****Complete list available at www.emilymiskel.com****

TABLE OF CONTENTS

ILLEGAL EVIDENCE: WIRETAPPING, HACKING, AND DATA INTERCEPTION LAWS.

I. SCOPE OF ARTICLE.

This article will give an overview of state and federal laws relating to wiretapping and interception of data, including both criminal laws and civil causes of action. This paper focuses on the portions of the laws that are most likely to affect a civil or family practitioner. There are many other sections of the laws relating to law enforcement and criminal investigations that are beyond the scope of this paper.

The federal laws are very complex and technical, often requiring fine-grained statutory interpretation to understand. It would be possible to write an entire textbook on the intricacies of these laws. This article is designed to give a brief overview of the landscape of these interlocking laws so that the practicing attorney will have a basic understanding of the framework and will have a starting point for more in-depth learning.

II. FEDERAL CLAIMS IN STATE COURT

This paper contains an extensive discussion of federal laws relating to wiretapping and data interception. These federal laws are relevant to attorneys who practice exclusively in state court because these federal claims may be brought in state court. Although it is currently rare, it would be possible to add a federal Wiretap Act civil claim to a divorce case, for example.

This stems from the United States Constitutional system of federalism, which provides that federal courts are courts of limited jurisdiction, while state courts are courts of general jurisdiction. Nothing in the concept of the federal system prevents state courts from enforcing rights created by federal law.[1] Concurrent jurisdiction has been a common phenomenon in United States judicial history, and exclusive federal court jurisdiction over cases arising under federal law has been the exception rather than the rule.[2] Under the federal system, the states possess sovereignty concurrent with that of the federal government, subject only to limitations imposed by the Supremacy Clause.[3] Under this system of dual sovereignty, the U.S. Supreme Court has consistently held that state courts have inherent authority, and are thus presumptively competent, to adjudicate claims arising under the federal laws of the United States.[4]

A state court is only precluded from hearing federal claims if Congress has given exclusive jurisdiction to federal courts. To give federal courts exclusive jurisdiction over a federal cause of action, Congress must, in an exercise of its powers under the Supremacy Clause, affirmatively divest state courts of their presumptively concurrent jurisdiction.[5] Absent an exclusive grant of jurisdiction to the federal courts in the Congressional act, state courts of general jurisdiction have concurrent authority to adjudicate federally created causes of action.[6]

Specifically, state courts have jurisdiction over federal wiretap claims.[7] Nothing in the federal wiretapping act suggests that Congress confined jurisdiction solely to the federal courts.[8] Texas courts have addressed claims under the Federal Wiretap Act.[9]

For the reasons stated below, it will be increasingly likely to encounter these federal claims, even in a state-court practice.

III. FEDERAL WIRETAP ACT.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, more commonly known as the "Wiretap Act," is found at 18 U.S.C. §§ 2510-2522. As the name suggests, the Wiretap Act was passed in the 1960s. Although it was updated in 1986 and 1994, it can be an imperfect match for many of the modern technologies that have been created in the 20 years since its last update.

The Wiretap Act generally sets forth three categories of offenses: interception of communications, use of intercepted communications, and disclosure of intercepted communications. (There is a fourth category of offenses, dealing with mechanical devices or "bugs." This paper will not address those offenses, because they are not as relevant to the general practice of the audience for this paper.) The Wiretap Act also contains a civil cause of action and a strict exclusionary rule.

---

[1] *Charles Dowd Box Co. v. Courtney*, 368 U.S. 502, 507 (1962).
[2] *Id*.
[3] *Tafflin v. Levitt*, 493 U.S. 455, 458 (1990).
[4] *Id*. at 459.
[5] *Yellow Freight System, Inc. v. Donnelly*, 494 U.S. 820, 823 (1990).
[6] *Williams v. Horvath* (1976) 16 Cal.3d 834, 837, 129 Cal.Rptr. 453, 548 P.2d 1125.
[7] *Bunnell v. Department of Corrections*, (1998) 64 Cal.App.4th 1360, 1367, 76 Cal.Rptr.2d 58.
[8] *Id*.; s*ee also Young v. Young* (1995) 211 Mich.App. 446, 448, fn. 1, 536 N.W.2d 254, 255.
[9] *See, e.g., Boehringer v. Konkel*, No. 01-11-00702-CV (Tex.App.—Houston [1st Dist.] Apr. 4, 2013).

A. Interception.

1. Definition.

The Wiretap Act is violated when any person:

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication.[10]

The Wiretap Act is an extremely technical statute. Most of the words used are statutorily-defined terms which differ from the commonly-understood definitions of the words. Any time you are working with the federal statutes, it is extremely important to read and re-read the defined terms. The definitions of "wire communication," "oral communication," and "electronic communication" are discussed in more detail below.

2. Cordless, Wireless, or Cellular Communications.

In 1968, when the Wiretap Act was originally enacted, cordless, wireless, or cellular phones did not exist as a consumer product. Therefore, under the original act, cordless, wireless, or cellular transmissions were considered "radio transmissions" and were not protected at all against interception. Courts further held that no one could have any reasonable expectation of privacy in such conversations.[11] Now, however, most people strongly believe that there is an expectation of privacy in cordless or wireless conversations, and in fact the Act was updated in 1994 to explicitly protect such communications.[12] In 2001, the U.S. Supreme Court confirmed that the Wiretap Act "now applies to the interception of conversations over both cellular and cordless phones."[13]

B. Use and Disclosure.

The Wiretap Act is also violated when any person "uses" or "discloses" the contents of an intercepted communication:

(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;[14]

The Wiretap Act prohibits the disclosure of "any information concerning the substance, purport, or meaning of that communication."[15] Therefore, even revealing the general nature of a communication or intimating its contents may constitute an actionable disclosure.[16]

NOTE: An attorney can have personal criminal and civil liability for using or disclosing an improper recording made by a client.

C. Definitions.

Under the Wiretap Act, statutory definitions are critical.

1. Wire Communication.

"Wire communication" means "any 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…."[17] A "wire" communication

[10] 18 U.S.C. § 2511(1)(a).
[11] See e.g., *Tyler v. Berodt*, 877 F.2d 705 (8th Cir.1989); *Askin v. McNulty*, 47 F.3d 100 (4th Cir.1995); *United States v. Smith*, 978 F.2d 171 (5th Cir.1992).
[12] *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994). Available at: http://www.gpo.gov/fdsys/pkg/STATUTE-108/pdf/ STATUTE-108-Pg4279.pdf
[13] *Bartnicki v. Vopper*, 532 U.S. 514, 524 (2001).
[14] 18 U.S.C. § 2511(1)(c), (d).
[15] 18 U.S.C. § 2510(8).
[16] *Goodspeed v. Harman*, 39 F.Supp.2d 787, 790 (N.D. Tex. 1999).
[17] 18 U.S.C. § 2510 (1).

must be "aural," or spoken by a human.[18] It must also be transmitted at least in part by a wire. Wire communications are protected against interception regardless of the speaker's expectation of privacy.[19]

2. Oral Communication.

"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."[20] Typically, oral communications include face-to-face communications where the participants have a reasonable expectation of noninterception. The statute requires a court to determine whether a person had a subjective expectation that her conversations were free from interception, and whether that expectation was objectively reasonable.[21] It is not a violation to record oral communications where there is no reasonable expectation of privacy.

3. Electronic Communication.

"Electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system…but does not include any wire or oral communication…."

4. Overlap Between Wiretap Act and Stored Communications Act.

The Stored Communications Act is discussed below, but the two laws overlap in confusing ways.[22] Although the Wiretap Act is popularly thought to apply to voice communications, it can also apply to interception of data. However, the Wiretap Act applies only to data intercepted contemporaneously with transmission.[23] The Stored Communications Act applies to data in electronic storage and thus provides broader protection against data interception. Since the Stored Communications Act lacks an exclusionary rule, though, it may benefit a client to argue that a particular interception is a breach of the Wiretap Act.

D. Penalties.

1. Criminal.

Criminal penalties for a violation of the Wiretap Act include a fine, imprisonment up to five years, or both.[24]

2. Civil.

The Wiretap Act also provides a civil cause of action for "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used…."[25] The Wiretap Act provides for civil remedies including equitable relief (injunctions), damages, punitive damages, **and** reasonable attorney's fees and costs.[26] As damages, the court may assess the **greater** of:

a. Actual damages,
b. Statutory damages of $100 a day for each day of violation, or
c. $10,000.[27]

The $10,000 statutory damages is not per violation, but is a single sum that applies to a closely-related course of conduct over a relatively short period of time.[28] However, if multiple persons' communications were intercepted, the statutory damages are per plaintiff.[29] There is a split among federal circuits as to whether the $10,000 amount is a minimum that must be awarded or whether a court has the discretion to decline to award that amount.

---

[18] 18 U.S.C. § 2510(18).
[19] *Briggs v. American Air Filter Co., Inc*., 630 F.2d 414, 417 (5th Cir.1980).
[20] 18 U.S.C. § 2510(2).
[21] *Walker v. Darby*, 911 F.2d 1573, 1578 (11th Cir.1990).
[22] *United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir.1998) (the intersection of these two statutes "is a complex, often convoluted, area of the law").
[23] *Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868, 878 (9th Cir.2002).
[24] 18 U.S.C. § 2511(4)(a).
[25] 18 U.S.C. § 2520(a).
[26] 18 U.S.C. § 2520(b).
[27] 18 U.S.C. § 2520(c).
[28] *Dorris v. Absher*, 179 F.3d 420, 428 (6th Cir.1999).
[29] *Id*.

Courts holding that damages are discretionary:

- *Goodspeed v. Harman*, 39 F.Supp.2d 787 (N.D. Tex. 1999)
- *DirecTV, Inc. v. Brown*, 371 F.3d 814 (11th Cir. 2004)
- *Reynolds v. Spears*, 93 F.3d 428 (8th Cir. 1996)
- *Nally v. Nally*, 53 F.3d 649 (4th Cir. 1995)

Courts holding that damages are mandatory:

- *Rogers v. Wood*, 910 F.2d 444 (7th Cir. 1990)
- *Menda Biton v. Menda*, 812 F.Supp. 283 (D.P.R., 1993)

Wiretap Act claims are likely to become more frequent when attorneys realize that the law provides for large statutory damages in addition to attorney's fees.

3. Statute of Limitations.

Wiretap Act claims are subject to a two-year statute of limitations.[30] The statute of limitations begins to run when the claimant first has a reasonable opportunity to discover the violation.[31] It does not require the claimant to have actual knowledge of the violation; only that the claimant have had a reasonable opportunity to discover it.[32] However, even if the statute of limitations has run for the original interception, each "use" or "disclosure" is a separate offense and is subject to a separate two-year limitations period.[33]

4. *Schlueter* and Spousal Wiretap Claims

The *Schlueter* case stands for the proposition that a spouse cannot separately allege a fraud claim in a divorce and receive damages other than a disproportionate division of the community estate.[34] The case is broadly read to mean that economic torts between spouses must be addressed by a disproportionate division of the community property and that there may be no punitive damages for such tort claims. The case distinguishes personal injury torts because the recovery for those claims belongs to a spouse's separate estate.[35]

It is an interesting question whether Wiretap Act plaintiffs may seek punitive damages in a divorce case. A 1995 Texas case did allow punitive damages and actual damages for intercepting communications in a divorce case.[36] Further, that case held that it was not a double recovery to award a portion of the community estate in addition to the judgment for the tort claim.[37] However, the *Schlueter* case was decided after that case.

On one hand, recovery under the Wiretap Act would be distinguishable from *Schlueter*, because it is not "directly referable to a specific value of lost community property." On the other hand, a Wiretap Act recovery is not statutorily defined as the separate property of a spouse, so it does not dovetail with the reason personal injury awards are distinguishable. Until more Wiretap Act claims are brought, we will not have guidance on this issue.

E. Exclusionary Rule.

The Wiretap Act contains a strict exclusionary rule, prohibiting intercepted communications from being used in any proceeding:

> 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.[38]

---

[30] 18 U.S.C. § 2520(e).
[31] *Id*.
[32] *Davis v. Zirkelbach*, 149 F.3d 614, 618 (7th Cir.1998).
[33] *See, e.g., Fultz v. Gilliam*, 942 F.2d 396, 404 (6th Cir.1991).
[34] *Schlueter v. Schlueter*, 975 S.W.2d 584 (Tex.1998).
[35] *Id*. at 587.
[36] *Parker v. Parker*, 897 S.W.2d 918 (Tex. App.—Fort Worth 1995, writ denied) (civil claim brought under Tex. Civ. Prac. & Rem. Code Ch. 123).
[37] *Id*. at 936.
[38] 18 U.S.C. § 2515.

Criminal lawyers are familiar with exclusionary rules. However, normal Texas law only prohibits the introduction of illegally-obtained evidence in criminal trials.[39] Generally, illegally-obtained evidence is admissible in civil trials.[40] The Wiretap Act overrides this practice and specifically provides that evidence obtained in violation of the Act may not be used in any proceeding—civil, criminal, administrative, or otherwise. By excluding "evidence derived therefrom," the Wiretap Act also excludes "fruits of the poisonous tree"—any evidence obtained as a result of the intercepted communication.[41]

> **NOTE**: the exclusionary rule applies to "wire" or "oral" communications—not "electronic" communications. For example, this means that intercepted text messages would not be covered by the exclusionary rule. This example underscores the importance of a close reading of the statute and all defined terms.

Currently, as long as the communication is a voice communication, it will be subject to the stronger protections accorded to "wire" communications. That means that the exclusionary rule would apply to landline calls, cellular calls, and VoIP or internet calls (Skype, etc.).[42]

F. Consent.

1. One-Party Consent.

The Wiretap Act contains an explicit exception for communications "intercepted" by one of the parties to the communication. The Act provides:

> (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 where one of the parties to the communication has given prior consent to such interception....[43]

In other words, any private person may record any conversation to which he or she is a party. This is known as "one-party consent." Federal law and the laws of 38 states (including Texas) provide that only one person's consent to a recording is needed. Additionally, any further use or disclosure of such a recording is permissible and is not a violation of the Wiretap Act.

2. All-Party Consent.

Twelve states, however, require that all parties must consent to a recording. Those states include California, Connecticut, Florida, Hawaii (under some circumstances), Illinois, Maryland, Massachusetts, Montana, Nevada, New Hampshire, Pennsylvania, and Washington. In an all-party consent state, there may be criminal and civil penalties for recording or intercepting a communication without the consent of every party. Further, any subsequent use or disclosure of communications recorded without the consent of all parties may be additional violations under the law of those states (but not under federal law). If a call is conducted across state lines, the law of the stricter state applies. Therefore, it is best to advise clients not to record conversations if any party is outside Texas.

3. Vicarious Consent.

A common fact pattern involves one parent who intercepts communications between the child and the other parent. Because parents generally have the ability to provide legal consent on behalf of minor children, there is lots of case law interpreting the circumstances under which one parent can consent to recording communications between the child and others.

Some federal courts have found that where the parent has a good faith, objectively reasonable belief that the recording is necessary for the welfare of the child, a vicarious consent exception to the Wiretap Act will make such recordings permissible.[44] Texas state courts have followed this interpretation.[45]

---

[39] Code Crim. Proc. art. 38.23.
[40] *See, e.g., Baxter v. Tex. Dept. of Human Resources*, 678 S.W.2d 265, 267 (Tex.App.—Austin 1984, no writ).
[41] *United States v. Smith*, 155 F.3d 1051, 1059 (9th Cir.1998).
[42] See, e.g., "What About Phone Calls Using the Internet?" Surveillance Self-Defense Project, Electronic Freedom Foundation, available at: https://ssd.eff.org/wire/protect/voip
[43] 18 U.S.C. § 2511(2)(d).
[44] *See, e.g., Pollock v. Pollock*, 154 F.3d 601, 610 (6th Cir.1998).
[45] *Alameda v. State*, 235 S.W.3d 218 (Tex. Crim. App. 2007).

IV. TEXAS STATE WIRETAPPING LAW.

Texas has its own state-level wiretapping law, contained in the Penal Code.[46] The Texas law is designed to closely parallel the federal law, although it differs in some respects.

A. Offense.

Under the Texas wiretapping law, it is an offense if a 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....[47]

The offenses and definitions generally parallel the federal Act, although Texas added an offense for effecting a covert entry for the purpose of intercepting communications. The defined terms, including "wire," "oral," and "electronic" communications, also parallel the federal Act. The Texas law also specifically enumerates a variety of affirmative defenses, including the one-party consent requirement.[48]

One key difference is the knowledge requirement for a "use" offense. Under the federal Wiretap Act, a person commits an offense if the person uses the contents of an intercepted communication "knowing or having reason to know" that the information was obtained through interception. Under the Texas law, a person commits an offense if the person uses the contents of an intercepted communication if the person "knows or is **reckless** about" whether the information was obtained through interception. This is a broader definition and includes more conduct than the federal Act.

B. Penalties.

1. Criminal.

A violation of the Texas wiretap law is a 2nd degree felony.[49]

2. Civil.

The Texas Civil Practice and Remedies Code contains a civil cause of action for interception of communication:

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....[50]

For the purpose of the civil claim, a communication is defined as "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." This definition likely parallels "oral" communications and "wire" communications under the state and federal wiretap laws, so case law interpreting those terms would provide some guidance. Like the federal Wiretap Act, a person must be a party to the communication to have standing to sue under this law.

[46] Tex. Penal Code § 16.02.
[47] Tex. Penal Code § 16.02(b) (emph. added).
[48] Tex. Penal Code § 16.02(c).
[49] Tex. Penal Code § 16.02(f).
[50] Tex. Civ. Prac. & Rem. Code § 123.002(a).

3. Damages.

Under the federal Wiretap Act, most courts have interpreted the statutory damages provision to be discretionary, because the statute uses the term "may." The Texas cause of action differs, and provides that a person 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.[51]

While courts have held that the federal Wiretap Act provides **total** statutory damages of $10,000, the Texas civil claim allows statutory damages for "each occurrence." It is yet to be determined whether Texas courts will define "occurrence" to mean each interception or follow the federal meaning of a "closely-related course of conduct over a relatively short period of time."[52] Additionally, one court has held that the punitive damages are not subject to any statutory cap.[53] However, the relevant statute has been amended since that decision.

V. FEDERAL STORED COMMUNICATIONS ACT.

The Stored Communications Act was initially created as part of the Electronic Communications Privacy Act in 1986 and has been amended several times, with the last substantive changes occurring in 2002. While it overlaps the Wiretap Act, it differs from it in key respects.

A. Offense

The Stored Communications Act makes it an offense to:

(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....[54]

While the Wiretap Act focuses on interceptions that happen contemporaneously with transmission, the Stored Communications Act focuses on accessing communications in electronic storage, as that term is statutorily defined.

B. Definitions

1. Wire and Electronic Communications.

The Stored Communications Act adopts by reference the statutory definitions of the Wiretap Act. The Stored Communications Act refers solely to "wire" and "electronic" communications, omitting the "oral" communication coverage of the Wiretap Act.

2. Electronic Storage.

A threshold issue for the Stored Communications Act is whether a communication is in "electronic storage." The term is statutorily defined to mean:

(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;

Courts have struggled to define "temporary, intermediate storage" in the context of how data is stored and transmitted over the internet. For example, it is not a violation to obtain answering machine messages located on a physical

[51] Tex. Civ. Prac. & Rem. Code § 123.004.
[52] *Dorris v. Absher*, 179 F.3d 420, 428 (6th Cir.1999).
[53] *Parker v. Parker*, 897 S.W.2d 918, 930 (Tex. App.—Fort Worth 1995, writ denied).
[54] 18 U.S.C. § 2701(a).

recorder, but it is a violation to access voicemail messages stored on a telecommunications system.[55] Similarly, the Stored Communications Act is not violated when someone access emails that are stored locally on a computer, but it can be a violation to access webmail that is stored on the internet.[56]

C. Penalties.

1. Criminal.

Criminal penalties vary with the purpose of the offense and whether or not it is a first offense:[57]

Purpose	First Offense	Subsequent Offense
commercial advan-tage, malicious des-truction or damage, or private commercial gain, or in furtherance of any criminal or tortious act	Fine or imprison-ment for not more than 5 years, or both	fine or imprison-ment for not more than 10 years, or both
Any other purpose	fine or imprison-ment for not more than 1 year or both	fine or imprison-ment for not more than 5 years, or both

2. Civil.

The Stored Communications Act permits a broader group of people to bring civil claims, compared to the Wiretap Act. While the Wiretap Act only permits a person whose communication was intercepted to sue, the Stored Communications Act permits:

> …[any] person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind 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.[58]

Relief available in a civil claim under the Stored Communications Act includes:[59]

- preliminary, equitable, or declaratory relief, including injunctions;
- actual damages including any profits made by the violator as a result of the violation;
- minimum statutory damages of $1,000;
- punitive damages if the violation is willful or intentional; and
- reasonable attorney's fees and litigation costs.

3. Statute of Limitations.

Like the Wiretap Act, the Stored Communications Act is subject to a two-year statute of limitations.[60] The statute of limitations begins to run when a claimant has "inquiry notice" that her rights might have been invaded.[61]

VI. TEXAS STATE STORED COMMUNICATIONS LAW.

Texas has its own law regarding unlawful access to stored communications. Under the Texas law, it is an offense if a person:

> ...obtains, alters, or prevents authorized access to a wire or electronic communication while the communication is in electronic storage by:

[55] *See, e.g., U.S. v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998).
[56] *See, e.g., Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868, 874-880 (9th Cir. 2002).
[57] 18 U.S.C. § 2701(b).
[58] 18 U.S.C. § 2707(a).
[59] 18 U.S.C. 2710(b), (c).
[60] 18 U.S.C. § 2707(f).
[61] *Davis v. Zirkelbach*, 149 F.3d 614, 618 (7th Cir.1998).

(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.[62]

The Texas law is virtually identical to the federal law. If the offense is committed to obtain a benefit or to harm another, it is a state jail felony; otherwise, it is a class A misdemeanor.[63]

VII. OTHER TEXAS COMPUTER CRIMES.

A. Online Impersonation.

Texas was one of the first states to implement a law prohibiting online impersonation when it passed Tex. Penal Code § 33.07 in 2009. The law creates two offenses:

(a) A person commits an offense if the person, without obtaining the other person's consent and with the intent to harm, defraud, intimidate, or threaten any person, uses the name or persona of another person to:

(1) create a web page on a commercial social networking site or other Internet website; or
(2) post or send one or more messages on or through a commercial social networking site or other Internet website, other than on or through an electronic mail program or message board program.

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

(1) without obtaining the other person's consent;
(2) with the intent to cause a recipient of the communication to reasonably believe that the other person authorized or transmitted the communication; and
(3) with the intent to harm or defraud any person.

An offense under subsection (a) is a third-degree felony.[64] An offense under subsection (b) is a Class A misdemeanor, unless the actor commits the offense with the intent to solicit a response by emergency personnel, in which case it is a third-degree felony.[65] If the same conduct constitutes a violation of multiple sections of the Penal Code, the person may be prosecuted under any or all of the laws.[66] The law carves out a defense for employees of social networking sites, internet service providers, etc.[67]

Under this law, the defendant must have the intent to harm the victim. The penal code defines "harm" as "anything reasonably regarded as loss, disadvantage, or injury."[68] There is no requirement the harm be physical harm.[69] Emotional distress can be sufficient to qualify as harm under the Penal Code.[70] In the one Texas case interpreting § 33.07, the defendant disputed that when he sent the impersonating message, he had the intent to harm the victim, claiming he sent the message only to test the victim's professed psychic abilities.[71]

Another crucial element of this offense is the impersonation. If a person merely uses the internet to harm someone, without impersonating, the conduct would not be covered by this section. Rather, it would likely be considered harassment under Tex. Penal Code § 42.07. It is interesting to note that harassment is a misdemeanor, while impersonation is a felony.

---

[62] Tex. Penal Code § 16.04(b).
[63] Tex. Penal Code § 16.04(c), (d).
[64] Tex. Penal Code § 33.07(c).
[65] *Id*.
[66] Tex. Penal Code § 33.07(d).
[67] Tex. Penal Code § 33.07(e).
[68] Tex. Penal Code § 1.07(a)(25).
[69] *Hudspeth v. State*, 31 S.W.3d 409, 411 (Tex. App.-Amarillo 2000, pet. ref'd); *see also Halay v. State*, No. 03-07-00327-CR, 2008 WL 5424095, at *7 (Tex. App.-Austin Dec. 31, 2008, no pet.) (mem. op., not designated for publication) ("[E]ven emotional harm and aggravation . . . can reasonably be considered loss, disadvantage, or injury.").
[70] *White v. State*, No. 14-05-00454-CR, 2006 WL 2771855, at *2 (Tex. App.-Houston [14th Dist.] Sept. 28, 2006, pet. ref'd) (mem. op.).
[71] *See Taylor v. State*, No. 02-11-00092-CR (Tex.App.—Fort Worth Mar. 22, 2012) (memo op.).

B. Breach of Computer Security.

The Penal Code contains a criminal offense for breach of computer security. The first level of offense does not require that the defendant have any intent to harm:

> (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.[72]

An offense under subsection (a) is a Class B misdemeanor, except that the offense is a state jail felony if the defendant has been previously convicted two or more times or if the system is owned by the government or a critical infrastructure facility.[73]

The second level of offense has more severe penalties, but requires that the defendant have intent to harm:

> (b-1) A person commits an offense if with the intent to defraud or harm another or alter, damage, or delete property, the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

The penalty for an offense under this subsection varies with the "amount involved:"[74]

Penalty	**Aggregate Amount Involved**
State jail felony	< $20,000
3rd degree felony	≥ $20,000 < $100,000
2nd degree felony	≥ $100,000 < $200,000
1st degree felony	> $200,000

It is a second degree felony to obtain the identifying information of another by accessing only one computer, computer network, or computer system; or a third degree felony if more than one.[75]

For a family law practitioner, the "aggregate amount involved" measure is not incredibly helpful. For example, how does one measure the aggregate amount involved if the breach was done for the purpose of obtaining evidence in a custody case? Further, the offense is elevated to a felony if the offense was committed with the intent to harm another. Again, it can be argued that breaching computer security to obtain evidence in a custody case is harm, but it can also be argued that obtaining truthful evidence that is relevant to custody is not harm, but rather is protecting the best interests of children. This law was designed to protect financial institutions against hacking, but it does not helpfully translate onto the issues faced by a family law practitioner.

C. Civil Cause of Action.

Chapter 143 of the Civil Practice and Remedies Code creates a cause of action for a person who is injured or whose property is injured by an intentional or knowing violation of Chapter 33 of the Penal Code.[76] This includes both the online impersonation and breach of computer security offenses described above. The civil cause of action permits a person to recover actual damages and reasonable attorney's fees and costs.[77]

VIII. CONCLUSION

These statutes form a technical and complex web of laws that affect criminal and family practices in potentially far-reaching ways. This paper is an overview of a field with significant depth, and interested practitioners should devote time to reading the cases interpreting and applying these statutes.

---

[72] Tex. Penal Code § 33.02(a).
[73] Tex. Penal Code § 33.02(b).
[74] Tex. Penal Code § 33.02(b-2).
[75] *Id*.
[76] Tex. Civ. Prac. & Rem. Code § 143.001; *see also Institutional Securities Corp. v. Hood*, 390 S.W.3d 680, 684 (Tex.App.—Dallas 2012).
[77] Tex. Civ. Prac. & Rem. Code § 143.002.