PEEPING TOMS IN THE NEW MILLENNIUM:
DIGITAL DOS AND DON’TS

Presented and Written By:

HON. EMILY MISKEL
470th District Court
18484 Preston Rd., Suite 102-336
Dallas, Texas 75252
(972) 885-8510
emily@emilymiskel.com

MARK I. UNGER
Unger Law Firm
10010 San Pedro, Suite 660
San Antonio, Texas 78216
(210) 323-2341
miunger@gmail.com

KRISTAL C. THOMSON
Wilson, Pennypacker & Thomson
8620 N. New Braunfels, Suite 101
San Antonio, Texas 78217
(210) 826-4001
kthomson@wptfamilylaw.com

Presented By:

RICK ROBERTSON
KoonsFuller
5700 W. Plano Pkwy., Suite 2200
Plano, Texas 75093 (972) 769-2727
rick@koonsfuller.com

State Bar of Texas
NEW FRONTIERS IN MARITAL PROPERTY LAW
October 13-14, 2016
Louisville, KY

CHAPTER 4
# TABLE OF CONTENTS

I. Wiretapping and Other Federal Laws – Introduction and Scope ................................................................. 1
   A. Interception ........................................................................................................................................... 1
   B. Definitions .......................................................................................................................................... 1
   C. Use or Disclosure Violations .............................................................................................................. 1
   D. Consent ................................................................................................................................................ 1
   E. Vicarious consent ................................................................................................................................. 1
   F. Civil and Criminal Penalties .............................................................................................................. 1
   G. Exclusionary Rule ............................................................................................................................... 1
   H. Attorney Liability ............................................................................................................................... 1

II. Federal Claims in State Court .................................................................................................................. 1

   A. Interception ........................................................................................................................................ 1
   B. Definitions .......................................................................................................................................... 1
   C. Use or Disclosure Violations .............................................................................................................. 1
   D. Consent ................................................................................................................................................ 1
   E. Vicarious consent ................................................................................................................................. 1
   F. Civil and Criminal Penalties .............................................................................................................. 1
   G. Exclusionary Rule ............................................................................................................................... 1
   H. Attorney Liability ............................................................................................................................... 1

IV. Texas Wiretapping Law – Tex. Penal Code § 16.02, CPRC Ch. 123 ......................................................... 2
V. Overlap Between Wiretap Act and Stored Communications Act ............................................................... 2

   A. Electronic Storage ............................................................................................................................... 2
   B. Civil and Criminal Penalties .............................................................................................................. 2
   C. No Exception for Civil Subpoenas ...................................................................................................... 2

VII. Texas Stored Communications Law – Tex. Penal Code § 16.04 ............................................................. 2

   A. Definitions .......................................................................................................................................... 2
   B. Usage Violations ................................................................................................................................. 2
   C. Forfeiture .......................................................................................................................................... 3
   D. Civil Claim ........................................................................................................................................ 3

IX. Texas Breach of Computer Security Law – Tex. Penal Code § 33.02, CPRC Ch. 143 ............................ 3
X. Internet of Things – What is It? ................................................................................................................ 3
   A. What is Included in the Internet of Things ......................................................................................... 3
   B. Impact of the IoT on Family Law ..................................................................................................... 4

XI. New Causes of Action - Introduction ..................................................................................................... 4

XII. Invasion of Privacy .................................................................................................................................. 4
   A. Federal Law ....................................................................................................................................... 4
   B. Texas Privacy Claims ......................................................................................................................... 5
   C. Intrusion upon seclusion .................................................................................................................... 5

XIII. Unauthorized Access to Computer ......................................................................................................... 6
   A. Statutes ............................................................................................................................................. 6
   B. Violation Under Texas Penal Code § 33.02 & Penalties ................................................................... 6
   C. Recent Case law ............................................................................................................................... 7

XIV. Online Impersonation ............................................................................................................................ 8

XV. Revenge Porn ........................................................................................................................................ 9
   A. Civil Liability for Revenge Porn ....................................................................................................... 11
   B. Arguments Against Revenge Porn Statutes .................................................................................... 11
   C. Recent Case in News (unpublished; no opinion): ......................................................................... 12
XVI. Negligent Entrustment of a Chattel (computer) .......................................................... 12
XVII. Conclusion ................................................................................................................ 12
II. Federal Claims in State Court

Many of the laws discussed below are federal laws. These federal laws are still relevant to attorneys who practice exclusively in state court because these federal claims may be brought in state court. For example, it is possible to add a federal Wiretap Act civil claim to a divorce case. State courts are courts of general jurisdiction, and they have concurrent jurisdiction to hear cases arising under federal law.


The Wiretap Act generally sets forth four categories of offenses that are relevant to family law practitioners: interception of communications, use of “bugs” to intercept communications, use of intercepted communications, and disclosure of intercepted communications. The Wiretap Act also contains a civil cause of action and a strict exclusionary rule.

A. Interception.

The Wiretap Act is violated when any person intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication. The offense occurs when the communication is intercepted. A telephone conversation that is recorded, but not necessarily listened to, is still an “interception” under the Act.

B. Definitions.

A “wire” communication must be “aural,” or spoken by a human. Typically, “oral” communications include face-to-face communications where the participants have a reasonable expectation of noninterception. Unlike oral communications, wire communications are protected against interception regardless of the speaker’s expectation of privacy. “Electronic” communications are non-voice communications, such as e-mails or text messages. Video surveillance that does not capture audio is not an interception because no aural acquisition occurs.

C. Use or Disclosure Violations.

The Wiretap Act is also violated when any person “uses” or “discloses” the contents of an intercepted communication. The Wiretap Act prohibits the disclosure of “any information concerning the substance, purport, or meaning of that communication.” Therefore, even revealing the general nature of a communication may constitute an actionable disclosure. However, a person must know or have reason to know of the interception in order to commit a use or disclosure violation.

D. Consent.

The Wiretap Act contains an explicit exception for communications recorded with the consent of one of the parties to the communication. Under federal law and the laws of 38 states (including Texas), any person may record any conversation to which he or she is a party. Twelve states, however, require that all parties must consent to a recording. If a call is conducted across state lines, the law of the stricter state applies.

E. Vicarious consent.

A common fact pattern in family law involves one parent who records communications between the child and the other parent. 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.

F. Civil and Criminal Penalties.

Criminal penalties for a violation of the Wiretap Act include a fine, imprisonment up to five years, or both. The Wiretap Act also provides a civil cause of action. The Wiretap Act provides for civil remedies including equitable relief (injunctions), statutory damages of $10,000, punitive damages, and reasonable attorney’s fees.

G. Exclusionary Rule.

The Wiretap Act contains a strict exclusionary rule, prohibiting intercepted wire or oral communications from being used in any proceeding. Electronic communications are not covered by the exclusionary rule.

H. Attorney Liability.

An attorney can have personal criminal and civil liability for using or disclosing an improper recording made by a client. For example, the following can be
separate and independent wiretap violations: (1) attorney’s use of information in pleadings, (2) attorney’s use of information to form deposition questions, (3) attorney’s use of information in cross-examination, and (4) attorney turning over intercepted communications to a prosecutor. Further, the crime-fraud exception to the attorney-client privilege means that attorney-client communications about wiretapped communications are not privileged.

IV. Texas Wiretapping Law – Tex. Penal Code § 16.02, CPRC Ch. 123

Texas has its own state wiretapping law, contained in the Texas Penal Code. The offenses and definitions generally parallel the federal Wiretap Act, although Texas added an offense for effecting a covert entry for the purpose of intercepting communications. A violation of the Texas wiretap law is a felony. The Texas Civil Practice and Remedies Code contains a civil cause of action for interception of communications. Under the Texas cause of action, a person is entitled to minimum statutory damages of $10,000 for each interception plus punitive damages and attorney’s fees.

V. Overlap Between Wiretap Act and Stored Communications Act

The Wiretap Act applies only to data intercepted contemporaneously with transmission. Stored e-mail cannot be intercepted under the Wiretap Act. The Stored Communications Act applies to data in electronic storage and thus provides broader protection against data interception. However, the Stored Communications Act does not contain an exclusionary rule and does not provide for as much in statutory damages as the Wiretap Act.


The Stored Communications Act prohibits unauthorized access to electronic communications. The Act also creates privacy protections for online users and online content by limiting the ability of service providers to disclose information. While the Wiretap Act focuses on interceptions that happen contemporaneously with transmission, the Stored Communications Act focuses on accessing communications in electronic storage.

A. Electronic Storage

A threshold issue for the Stored Communications Act is whether a communication is in “electronic storage.” 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 recorder, but it is a violation to access voicemail messages stored on a telecommunications system. 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. There is some disagreement among courts about whether e-mail that is intercepted after it has been received and read is in “temporary, intermediate storage,” “backup storage,” or “post-transmission storage.” The first two categories would be protected under the Stored Communications Act, while the third would not.

B. Civil and Criminal Penalties

The Stored Communications Act has both criminal and civil penalties. The civil cause of action allows a party to recover minimum statutory damages of $1,000, punitive damages, and reasonable attorney’s fees and litigation costs.

C. No Exception for Civil Subpoenas

The Stored Communications Act prohibits a public service provider from divulging the contents of user communications even in response to a civil subpoena. Therefore, an attorney cannot obtain user content by subpoenaing Facebook or text messages by subpoenaing the phone carrier.

VII. Texas Stored Communications Law – Tex. Penal Code § 16.04

Texas has its own law regarding unlawful access to stored communications. 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 felony; otherwise, it is a misdemeanor.


The Computer Fraud and Abuse Act prohibits unauthorized access to computers. The law contains both criminal and civil causes of action.

A. Definitions

As used in the Computer Fraud and Abuse Act, a “computer” is broadly defined to include any data processing device, including computers, tablets, cellphones, and any other device that connects to the internet. A “protected computer” under the Act effectively includes all devices with internet access.

B. Usage Violations

Violations of the Computer Fraud and Abuse Act are often defined in terms of accessing computer “without authorization” or by “exceeding authorized access.” There is significant disagreement among federal courts as to what conduct constitutes access without authorization or access that exceeds authorization. Some federal courts have held that a person violates federal law when the person uses a computer or web services in violation of the provider’s usage policies. Other courts have held that such an interpretation is way too broad, and have limited the offense to situations where the person completely lacked authorization to a particular device or file.
Recently, concerned about prosecutorial abuse of the Computer Fraud and Abuse Act, lawmakers have introduced bills to exclude “terms of service” violations from the Act.

C. Forfeiture.

The Act includes a severe forfeiture provision. If a person is convicted of a violation of the Computer Fraud and Abuse Act, the court “shall” order the forfeiture of any personal property used to commit or facilitate the violation and any property, real or personal, derived from any proceeds obtained directly or indirectly as a result of the violation.

D. Civil Claim.

A person who suffers damage or loss by reason of a violation of the Computer Fraud and Abuse Act may maintain a civil action to obtain: (1) compensatory damages, (2) injunctive relief, and (3) other equitable relief. Unlike the other federal statutes discussed previously, this civil action does not provide for minimum statutory damages, punitive or exemplary damages, or attorney’s fees.

IX. Texas Breach of Computer Security Law – Tex. Penal Code § 33.02, CPRC Ch. 143

The Texas Penal Code contains a criminal offense for breach of computer security. A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

Texas has a civil cause of action for a person who is injured or whose property is injured by an intentional or knowing violation of Texas’s breach of computer security or online impersonation laws. The civil cause of action permits a person to recover actual damages and reasonable attorney’s fees and costs.

This law is discussed more thoroughly in other sections of this paper.

X. Internet of Things – What is It?

The “Internet of Things” (IoT) is a term that refers to the internetworking of physical devices, embedded with certain hardware and software, that enables these devices to collect and exchange data.\(^1\) It has also been called an “inextricable mixture of hardware, software, data and service.”\(^2\) In very basic terms, it’s a device/software that solicits and measures data (phone) and provides that data to another device/software (app) for consumer use.

The IoT revolves around “machine to machine” communication.\(^3\) It makes our “things,” and thus our way of life, “smarter.” The IoT exists because of cloud-based technology and sensors, meaning that in order for them to work, the data compiled by them lives in the cloud – outside of the control of the owner of the device.\(^4\) The devices are connected to each other and to the internet and interact with just a flip of a switch.\(^5\)

These items also use the same Internet Protocol (IP) that connects to the internet.\(^6\) As IP communications advance, they also become more uniform, and thus more “things” are easily able to communicate. This allows for even more items to flood the market place.

A. What is Included in the Internet of Things

According to technology research company, Gartner, the IoT will consist of 20.8 billion items by the year 2020.\(^7\) The types of items classified as IoT is vast and ever-expanding. The following is a non-exclusive list of IoT devices that may be relevant to family law clients:

1. smart phones;
2. tablet;
3. smart watches;
4. smart televisions;
5. cameras (including nanny cams);
6. vehicles;
7. refrigerators;
8. thermostats;
9. washers/dryers;
10. sound bars and speakers;
11. pacemakers;
12. insulin pumps;
13. hearing aids;
14. home security devices and smart locks;
15. electronic personal assistants (ex. Amazon’s Alexa, Apple’s Siri, or Microsoft’s Cortana);
16. drones;
17. keyboards and other Bluetooth enabled computer devices;
18. fitness devices;
19. scales;

---

5. Id.
20. one button product purchasers (Amazon);
21. dog activity monitors;
22. garage door openers;
23. shoes & fitness clothing;
24. coffee makers; and
25. smart lights.

It should also be noted that the items often contain location services in order to properly function. It does not take a professional level hacker to access these services, which means that spouses have multiple devices on which to research or investigate each other’s whereabouts.

B. Impact of the IoT on Family Law

The items listed above are the ones commonly used, and thus more apt to be involved or relevant in family law cases. There is a 100% chance that couples own at least one of the items listed above. Those items are typically part of the community estate, which means that two people likely have legal rights to management and control the items.

It is also important to note that much of the IoT is data collection and compilation. In addition to turning on the lights, your smart lights are also collecting data about how much and when you use your lights. Your Fitbit helps determine not only how many steps you took in one day, but when you took them, and where you took them.

The other potential problem with IoT in divorce is tracking, harassing, stalking and invading the privacy of the other party. Currently, family lawyers deal with their clients using their spouse’s password to gain access to phones, web sites, bank accounts and other things.

Hacking today is very different that it was 10, or even 5 years ago. A practice that was once only achievable by professional hackers is now simplified such that one purchase can get you into a thousand different devices. So now, you must be aware of the potential problems in your case – anything can be hacked. So, is your evidence good evidence? Is your client safe from intrusion? Do you know how to advise them regarding the IoT? Do you know how to explain to a judge what needs protection that goes beyond the standard family law restraining orders?

For example, at the 2016 DEF CON Hacker Conference (yes there is such a thing), researchers Anthony Rose and Ben Ramsey presented evidence where they were able to hack 12 out of 16 of the smart locks they tested. The ability to hack into these items ranged from “ridiculously easy” to moderately difficult. For family law attorneys, this means that

XI. New Causes of Action - Introduction

Credits: Credit and much thanks to Michelle M. Purvis and Ann M. Calabria for a good portion of their materials reproduced herein and from Advanced Family Law 2016 presentation by Tom Vick and Michael Heiskell, to Judge Emily Miskel for the massive amount of material provided, to John Browning, Shawn Tuma and Pierre Grosdidier for general contributions from published materials and to Craig Ball for creative offerings of recent developments.

XII. Invasion of Privacy

A. Federal Law.

The landmark United States Supreme Court case addressing individual privacy concerns is Katz v. United States, 389 U.S. 347 (1967). Although Katz was a case involving unreasonable search and seizure under the Fourth Amendment of the U.S. Constitution, it is important because it established the "reasonable expectation of privacy" test. The U.S. Supreme Court
ruled that the police’s placement of a listening device on the outside of a public telephone booth, without a warrant, constituted a violation of the wiretap statute because the defendant had a reasonable expectation of privacy when he closed the door to the telephone booth. See Id.

B. Texas Privacy Claims.

Privacy claims may be available in addition to claims under federal and state wiretapping and stored communications laws. Privacy claims may also be available for conduct that invades the privacy of others but which does not constitute a violation of a federal or state statute. There are three torts that are recognized under Texas law relating to invasion of privacy.

C. Intrusion upon seclusion

A person commits the tort of intrusion upon seclusion if a person intentionally intrudes upon another person’s solitude, seclusion, or private affairs. The intrusion must be an actual intrusion that is unreasonable, unjustified, or unwarranted, and it must be highly offensive to a reasonable person. The plaintiff must also show damage caused by the intrusion. Unlike defamation claims, truth is not a defense to a tort claim of intrusion upon seclusion. Additionally, the tort of intrusion upon seclusion does not depend upon the private affairs being made public. Rather, the focus is simply upon the intrusion.

1. Cases of Interest:

Hacking Into Private Computer:


Unauthorized Videos and Photographs Taken in Private Place:

- Clayton v. Richards, 47 S.W.3d 149 (Tex. App.—Texarkana 2001, pet. denied) (Wife hired PI to install cameras in couple’s bedroom—court ruled expectation of privacy from intrusion into seclusion exists in a person’s bedroom).
- Surveillance: Kramer v. Downey, 680 S.W.2d 524, 525 (Tex. App.—Dallas 1984, writ ref’d n.r.e. (continual stalking violated right to privacy).


To prevail in a claim for public disclosure of private facts, a plaintiff must show:

- the defendant publicized matters regarding plaintiff’s personal life;
- publicizing those matters would be highly offensive to a reasonable person of ordinary sensibilities; and
- the matter publicized is not of legitimate public concern.

Star-Telegram, Inc. v. Doe, 915 S.W.2d 471, 474 (Tex. 1994).

Scenarios Most Likely:

- Hidden Cameras (Nanny Cams) in bedrooms by husband or wife to obtain recordings later disclosed.
- Drones utilized to observe and record sexual acts or nude sunbathing, etc. and later disclosed or publicized (see also invasion of privacy).
- Disclosure of private facts such as sexual predilections, diseases, proclivities by one spouse against another.
- Security Systems with Cameras and Sensor Monitors (AT&T Digital Life)

“Texas recognizes a legal claim for publication of private facts. For the most part, the law in Texas is similar to that described in the general page on publication of private facts. See that page for a full discussion of the elements of and defenses to a private facts claim. Here, we will address only those aspects of Texas law that are different from the general description.

1. Elements of a Private Facts Claim.

In Texas, in order to recover for public disclosure of private facts, a plaintiff must show that

- publicity was given to matters concerning his or her private life;
- the publication of these facts would be highly offensive to a reasonable person of ordinary sensibilities; and
- the matter publicized was not of legitimate public concern.

Texas law does not impose liability for publication of information that is of legitimate public concern or newsworthy. A federal court applying Texas law has indicated that "reports of the investigation of crimes or matters pertaining to criminal activity have almost without exception been held to be newsworthy or matters of public interest as a matter of law." Lowe v. Hearst Communications, Inc., 487 F.3d 246, 250 (5th Cir. 2007)

Texas courts have found the following things, among others, to be of legitimate public concern or newsworthy:

- information that plaintiff was a gay, HIV-positive police officer;
- an incident involving the taping of high school students changing clothes by their band director; and
- details about a blackmailing scheme, through which a husband and wife team extorted thousands of dollars from the wife's lovers.

---

In addition, a photograph that was published in a newspaper that accidentally revealed a high school soccer player’s genitalia was protected because the photograph accurately depicted a public, newsworthy event. The court reasoned the First Amendment of the U.S. Constitution and the Texas Constitution provided the newspaper with immunity from liability for damages. McNamara v. Freedom Newspapers, Inc., 802 S.W.2d 901, 905 (Tex. App. 1991)

For additional information and discussion of Texas cases, see the Reporters Committee's Photographers' Guide to Privacy: Texas. For multiple states’ guides to public disclosure, see http://www.dmlp.org/legal-guide/state-law-publication-private-facts

2. Relying on Public Records.
In Texas, you generally cannot be held liable for publishing truthful information gathered from government records that are open to public inspection. So far, Texas courts have applied this protection to information revealed in open court proceedings and contained in police records, but it would likely apply to other government records as well, both because of a potential constitutional privilege and because the information is already exposed to the public eye.

3. Consent.
Texas recognizes consent as a defense to a publication of private facts claim. Texas courts may recognize verbal or implied consent, but it is advisable to get it in writing whenever possible. If getting written consent is not practical, you should try to record verbal consent using an audio or video recording device. The age of majority in Texas is eighteen; if you interview or photograph someone under the age of eighteen, you should seek consent from the subject's parent(s) or guardian. See the general description for a more detailed discussion of release forms.

4. Statute of Limitations.

E. Appropriation of Name or Likeness.
A plaintiff may recover under a cause of action for invasion of privacy by misappropriation if the following elements are established:

- the defendant appropriated the plaintiff’s name of likeness for the value associated with it;
- the plaintiff can be identified from the publication; and
- there was some advantage or benefit to the defendant.13

A plaintiff who prevails in a claim for invasion of privacy by misappropriation may recover actual, nominal, and exemplary damages. If clear and convincing evidence establishes that the defendant acted with malice, exemplary damages may be awarded. An injunction may be ordered to prevent future invasion of privacy by misappropriation. See K-Mart Corp. v. Trotti, 677 S.W.2d 632, 637 (Tex. App—Houston [1st Dist. 1984, writ ref’d n.r.e.), 686 S.W.2d 593 (Tex. 1985); Kramer v. Downey, 680 S.W.2d 524, 525 (Tex. App.—Dallas 1984, writ ref’d n.r.e.).

XIII. Unauthorized Access to Computer

A. Statutes:
- Texas Penal Code, Section 33.02 (See http://codes.findlaw.com/tex/penal-code/penal-sect-33-02.html)
- Texas Civil Practice and Remedies Code, Chapter 143, Sec. 143.001, 002; (See http://www.statutes.legis.state.tx.us/Docs/CP/htm/CP.143.htm)

Michelle M. Purvis and Ann M. Calabria cover Texas Penal Code, Section 33.02 from their Advanced Family Law paper follows–


B. Violation Under Texas Penal Code § 33.02 & Penalties.
Texas has created criminal and civil penalties for unauthorized access of a computer or computer network without the owner’s consent. Tex. Penal Code § 33.02. See Mitchell v. State, 12 S.W.3d 158 (Tex. App.—Dallas 2000, no pet.).

A person commits an offense under Section 33.02 of the Texas Penal Code “if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.”14

A person’s statements or actions may be considered to determine whether he or she has granted “consent” to access a computer or computer network.15

A violation of section 33.02(b) of the Texas Penal Code does not require that the owner of a computer or computer system be injured as a result of the unauthorized access.16

An offense under section 33.02(a) is “a Class B misdemeanor, except that the offense is a state jail felony if:

---

14 Tex. Penal Code § 33.02(a).
- the defendant has been previously convicted two or more times of an offense under this chapter; or
- the computer, computer network, or computer system is owned by the government or a critical infrastructure facility.  

A separate offense exists under section 33.02(b-1) if a person accesses a computer or network with intent to defraud or harm another or intends to harm or damage property.

“A person commits an offense if, with the intent to defraud or harm another or alter, damage, or delete property, the person knowingly accesses:
(1) a computer, computer network, or computer system without the effective consent of the owner; or
(2) a computer, computer network, or computer system:
(A) that is owned by:
   (i) the government; or
   (ii) a business or other commercial entity engaged in a business activity;
(B) in violation of:
   (i) a clear and conspicuous prohibition by the owner of the computer, computer network, or computer system; or
   (ii) a contractual agreement to which the person has expressly agreed; and
   (C) with the intent to obtain or use a file, data, or proprietary information stored in the computer, network, or system to defraud or harm another or alter, damage, or delete property.”

The penalties range from a Class C misdemeanor to a first degree felony, depending upon the monetary value resulting from the violation. Tex. Penal Code § 33.02(b-2).

They further describe the Civil Penalties available under Chapter 143 of the Texas Civil Practice & Remedies Code, titled “Harmful Access by Computer.” Section 143.001 of the Texas Civil Practice and Remedies Code and state that it provides a cause of action to “a person who is injured or whose property has been injured as result of a violation under Chapter 33” of the Texas Penal Code, if the violator acted “knowingly or intentionally.” Although actual injury is not required in establishing a violation of Texas Penal Code Chapter 33, injury to a person or property must be established to recover in a cause of action under section 143.001 of the Texas Civil Practice and Remedies Code.

The statute of limitations for filing suit is either five years after the last act constituting a violation or two years after the claimant discovered or had reasonable opportunity to discover the violation, whichever is earlier. Tex. Civ. Prac. & Rem. Code § 143.001(b). See Southwest Airlines, 318 F. Supp.2d at 443.

In addition, a prevailing plaintiff is entitled to actual damages and reasonable attorney’s fees and costs. Tex. Civ. Prac. & Rem. Code § 143.002.

C. Recent Case Law:

As of March 3, 2016, we now know that Breach of Computer security has, under certain circumstances been applied to cell phones, the most common form of access by one spouse against another’s possibly private information.

Shawn Tuma and others have recently discussed this, as it is the most recent and commonly known application of the law to a cell phone and used in a case between Husband and Wife.  

Tuma writes –

“Breach of Computer Security, Chapter 33, Section 33.02 of the Texas Penal Code, a criminal law that has a civil cause of action if the conduct constituting the violation was committed knowingly or intentionally, Chapter 143 of the Texas Civil Practice and Remedies Code, titled Harmful Access by Computer Act (HACA). This law was amended effective September 1, 2015.

Tuma offers the following three legal takeaways and states in relevant part as follows --

3 Key Legal Principles for Texas’ Unauthorized Access Law (HACA)

1. A cell phone is a “computer” for purposes of HACA (“In reality, ‘a modern cell phone is a computer ….”).
2. Examining a phone log and text messages from a cell phone necessarily requires retrieving the data on the phone which constitutes an “access” of a computer under HACA.
3. The misguided belief that, because a cell phone used exclusively by one spouse may technically constitute “community property,” the other spouse has “effective consent” to access the data on the cell phone, is absolutely false. “Nothing in chapter 33 of the penal code incorporates community property law for the purpose of establishing ownership of the computer. Rather, the statute defines ‘owner’ as a person who: (1) 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; (2) has the right to restrict access to the property; or (3) is the licensee of data or computer software.” Note, the Court’s fact-intensive approach to analyzing this issue is very important: Because both spouses agreed that the phone belonged to one spouse, she used it on a daily basis, it was the only way to reach her, she had the right to place a password on the phone, and had at various times restricted access to it by the password, and the other spouse accessed the phone at night when she was asleep and not using it, the evidence showed she had a greater right to possession of the phone. Id.

Tuma further offers this caveat –

“Based upon several discussions I have had since publishing this post, I need to make this point clear: I have not thoroughly researched this issue as it pertains to family law cases, however, in my past research on other issues, when I have seen family law cases dealing with “unauthorized access” issues nationwide, the way the Dallas Court of Appeals handled it is the prevailing view — but only when the device is clearly used by only one spouse or the other — this is definitely not the case in instances of things such as family computers, jointly used devices, etc.

This is only the rule in cases where the device is treated by the parties as being only one spouse’s or the others, despite the technicality that it’s true property ownership may be “community property.” In cases where devices are shared, the prevailing view is that both have a right to access the device.” Id

I agree with Tuma to the extent that phones, specifically smart phones such as the iPhone or Android phones are as much of a computer as any in the past. They contain data stored in various apps, on various servers (i.e. emails on servers, chat logs on a server or iTunes backup or within such other apps such as WhatsApp or Snapchat, documents in Apps such as GoodReader or iAnnotate or Pages, MS Office 365 Word or other documents, and even links to other documents via Dropbox, Box, MS One Drive or Google Drive). Smartphones are used in fact as computers by many millennials and some others as their sole means of computing and communicating. The lines have been blurred over the years and while the law will never keep up with the technology, to differentiate between an iPhone or iPad and a computer or server appears now to be a distinction without a difference. Each case must be evaluated, however on a case by case basis to determine whether there is unlawful access based on the statute(s).

We hear about this type of thing all the time in divorce cases. The interesting thing about it is that it can lead to many other causes of action. There are really two components or stages to pursuing these – one being the act of access itself, and two being what is found, disclosed, used or offered as evidence. In all or either cases, because of the nature of the violations and ambiguity surrounding predictability in outcome, often it is the knowledge and not the use that becomes the greatest weapon or defense.

XIV. Online Impersonation

We live in a pretend world, with pretend people, and pretend things. Pretending online seems to be the rule and not the exception. Yet when it comes to pretending to be someone you’re not online or in another virtual way, it’s not good. Perhaps some of the people using their real email addresses and pretending to be whomever they choose and who got caught in the Ashley Madison Scandal, (previously advertised with the tagline “life is short, have an affair”) might now want the anonymity that seems to be allowed in posting online and warn those against pretending to be someone they’re not when defaming others online. For those afraid of having been found out on Ashley Madison, they can check at https://www.trustify.info/check. For those seeking to find out if they’ve been breached on almost any social media website, which may be indicative of another impersonating them online, you can check most of your social media sites at https://havebeenpwned.com

Judge Emily Miskel writes about this topic as follows –

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. 21 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. 22 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. 23 The law carves out a defense for employees of social networking sites, internet service providers, etc. 24

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." 25 There is no requirement the harm be physical harm. 26 Emotional distress can be sufficient to qualify as harm under the Penal Code. 27 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 manifested psychic abilities. 28

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.

Shawn Tuma, points to the following for Civil liability—

Civil Practice & Remedies Code, Sec. 143 provides for Civil liability for violations of Texas Penal Code, Chapter 33, as follows—

Sec. 143.001: Cause of Action

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

(b) A person must bring suit for damages under this section before the earlier of the fifth anniversary of the date of the last act in the course of the conduct constituting a violation under Chapter 33, Penal Code, or the second anniversary of the date the claimant first discovered or had reasonable opportunity to discover the violation.

XV. Revenge Porn

Revenge is defined as to exact punishment or expiation for a wrong on behalf of, especially in a resentful or vindictive spirit. Porn or Pornography is defined as “sexually explicit videos, photographs, writings, or the like, whose purpose is to elicit sexual arousal.” 34 States and the District of Columbia now have revenge porn laws on the books.

Texas Penal Code Section 21.16 became effective September 1, 2015, enacting its own “Revenge Porn” statutes. Texas Penal Code Section 21.16 and states as follows—

Sec. 21.16: Unlawful Disclosure Or Promotion of Intimate Visual Material

(a) In this section:

(1) "Intimate parts" means the naked genitals, pubic area, anus, buttocks, or female nipple of a person.

(2) "Promote" means to procure, manufacture, issue, sell, give, provide, lend, mail, deliver, transfer, transmit, publish, distribute, circulate, disseminate, present, exhibit, or advertise or to offer or agree to do any of the above.

(3) "Sexual conduct" means sexual contact, actual or simulated sexual intercourse, deviate sexual intercourse, sexual bestiality, masturbation, or sadomasochistic abuse.

(4) "Simulated" means the explicit depiction of sexual conduct that creates the appearance of actual sexual conduct and during which a person engaging in the conduct...
exhibits any uncovered portion of the breasts, genitals, or buttocks.

(5) "Visual material" means:
(A) any film, photograph, videotape, negative, or slide or any photographic reproduction that contains or incorporates in any manner any film, photograph, videotape, negative, or slide; or
(B) any disk, diskette, or other physical medium that allows an image to be displayed on a computer or other video screen and any image transmitted to a computer or other video screen by telephone line, cable, satellite transmission, or other method.

(b) A person commits an offense if:
(1) without the effective consent of the depicted person, the person intentionally discloses visual material depicting another person with the person's intimate parts exposed or engaged in sexual conduct;
(2) the visual material was obtained by the person or created under circumstances in which the depicted person had a reasonable expectation that the visual material would remain private;
(3) the disclosure of the visual material causes harm to the depicted person; and
(4) the disclosure of the visual material reveals the identity of the depicted person in any manner, including through:
(A) any accompanying or subsequent information or material related to the visual material; or
(B) information or material provided by a third party in response to the disclosure of the visual material.

(c) A person commits an offense if the person intentionally threatens to disclose, without the consent of the depicted person, visual material depicting another person with the person's intimate parts exposed or engaged in sexual conduct and the actor makes the threat to obtain a benefit:
(1) in return for not making the disclosure; or
(2) in connection with the threatened disclosure.

(d) A person commits an offense if, knowing the character and content of the visual material, the person promotes visual material described by Subsection (b) on an Internet website or other forum for publication that is owned or operated by the person.

(e) It is not a defense to prosecution under this section that the depicted person:
(1) created or consented to the creation of the visual material; or
(2) voluntarily transmitted the visual material to the actor.

(f) It is an affirmative defense to prosecution under Subsection (b) or (d) that:
(1) the disclosure or promotion is made in the course of:
(A) lawful and common practices of law enforcement or medical treatment;
(B) reporting unlawful activity; or
(C) a legal proceeding, if the disclosure or promotion is permitted or required by law;
(2) the disclosure or promotion consists of visual material depicting in a public or commercial setting only a person's voluntary exposure of:
(A) the person's intimate parts; or
(B) the person engaging in sexual conduct; or
(3) the actor is an interactive computer service, as defined by 47 U.S.C. Section 230, and the disclosure or promotion consists of visual material provided by another person.

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

(h) If conduct that constitutes an offense under this section also constitutes an offense under another law, the actor may be prosecuted under this section, the other law, or both.

Legislation was filed on July 14, 2016 in California’s “Intimate Privacy Protection Act” by California Rep. Jackie Speier and which creates criminal penalties of up to five years in prison.

“Speier’s bill, just four pages long, would make it a crime to distribute a “visual depiction of a person who is identifiable from the image itself or information displayed in connection with the image and who is engaging in sexually explicit conduct, or of the naked genitals or post-pubescent female nipple of a person, with reckless disregard for the person’s lack of consent to the distribution.”

As 34 states now have statutes, it’s important to note that states such as California have a lower threshold (reckless disregard standard) as opposed to
other states that require an intentional act (i.e. Texas) and thus, the jurisdiction argument may come into play, given the fact that most publishing is likely to be done on the internet these days.

A. Civil Liability for Revenge Porn

Concurrent with the Texas Penal Code update criminalizing revenge porn, and explained by Pierre Grosdidier in his recent article, there is a civil component (effective September 15, 2015) which provides for civil damages as well. Grosdidier writes succinctly as follows regarding civil liability—

“The RPA creates a civil cause of action for the disclosure or promotion of intimate visual material...[and] adds Chapter 98B to the Texas Civil Practice & Remedies Code, which grants revenge porn victims a civil cause of action for “unlawful disclosure or promotion of intimate visual material.” The civil claim elements in §§ 98B.002(a) and (b) essentially track the corresponding criminal elements in Texas Penal Code §§ 21.16(b) and (d). A defendant may be held liable for posting offending pictures or for promoting the pictures on a website that the defendant owns or operates. A prevailing plaintiff may recover actual damages, including damages for mental anguish, court costs, reasonable attorney’s fees, and exemplary damages. Moreover, a court may grant injunctive relief to prevent the disclosure of intimate material, and impose fines of $1,000 for each willful or intentional violation of the court’s injunctive order.”29

Specifically, the law for civil liability for revenge porn comes from the following –

Civil Practice & Remedies Code, Sec. 98B.001 creates the following definitions --

In this chapter:

1) "Intimate parts," "promote," "sexual conduct," and "visual material" have the meanings assigned by Section 21.16, Penal Code.

2) "Intimate visual material" means visual material that depicts a person:

   (A) with the person's intimate parts exposed; or
   (B) engaged in sexual conduct.

While, Section 98B provides for the Civil Liability for Revenge Porn (violation of TPC sec. 21.16), as follows —

Sec. 98B.002: Liability for Unlawful Disclosure Or Promotion of Certain Intimate Visual Material

(a) A defendant is liable, as provided by this chapter, to a person depicted in intimate visual material for damages arising from the disclosure of the material if:

1) the defendant discloses the intimate visual material without the effective consent of the depicted person;

2) the intimate visual material was obtained by the defendant or created under circumstances in which the depicted person had a reasonable expectation that the material would remain private;

3) the disclosure of the intimate visual material causes harm to the depicted person; and

4) the disclosure of the intimate visual material reveals the identity of the depicted person in any manner, including through:

   (A) any accompanying or subsequent information or material related to the intimate visual material; or
   (B) information or material provided by a third party in response to the disclosure of the intimate visual material.

(b) A defendant is liable, as provided by this chapter, to a person depicted in intimate visual material for damages arising from the promotion of the material if, knowing the character and content of the material, the defendant promotes intimate visual material described by Subsection (a) on an Internet website or other forum for publication that is owned or operated by the defendant.

Damages for Revenge Porn are provided by the following—

Sec. 98B.003: Damages

(a) A claimant who prevails in a suit under this chapter shall be awarded:

1) actual damages, including damages for mental anguish;

2) court costs; and

3) reasonable attorney's fees.

(b) In addition to an award under Subsection (a), a claimant who prevails in a suit under this chapter may recover exemplary damages.

B. Arguments Against Revenge Porn Statutes:

In Response to Speier’s bill, Electronic Frontier Foundation staff attorney Lee Tien, for example, offers
a full-throated denunciation, saying its definition of revenge porn and the carve-out for tech companies are imprecise and that the bill’s lack of a requirement that a perpetrator have the intent to harass or humiliate, as do some state laws, creates potential problems. “It defines revenge porn in a way that doesn’t match very well with what revenge porn actually is,” he says. “It’s reaching stuff that’s not actually the problem.” Tien says the bill could chill constitutionally protected speech and frighten companies into removing content that is not actually revenge porn. “It’s never a good idea to create a rule that could go pear shaped if you do can do a better job,” he says.


I personally do not buy into these arguments. However, until freedom of speech is not used to defend anonymous (and often defamatory) postings with no repercussions to the hosting site, I believe that there should be some liability extended to the hosting entity. There have been a litany of sites that not only sensationalize anonymous posting of defamatory material, but encourage it under the guise of anonymity and without potential liability and some way to hold responsible if not prevent the anonymous poster from seeking to destroy other people in a cloaked environment.

C. Recent Case in News (unpublished; no opinion):

United Airlines pilot pleads guilty to stalking S.A. ex-girlfriend and to posting naked photos of her, See San Antonio Express News, September 28, 2016

A former United Airlines Pilot admitted and plead guilty to a federal stalking charge, admitting he posted nude photos and videos of an ex-girlfriend from San Antonio on the internet.

He posted the photos and videos to swinger sites, blogs and pornographic sites without her permission and then continued — in apparent acts of "revenge porn" — even after she got court orders barring him from doing so, claiming a sex addiction and an addiction to posting.

Records show the woman sued the defendant three times in Bexar County from 2009 to 2011 because he would not stop his conduct. The litigation resulted in restraining orders against him and he agreed to pay the woman more than $110,000 to settle the cases, records show.

Thereafter she turned to the FBI when he wouldn’t stop and was subsequently sentenced Wednesday to 41 months in federal prison for posting online nude photos and videos of an ex-girlfriend from San Antonio.

XVI. Negligent Entrustment of a Chattel (computer)

When someone such as a minor or an employee or possibly even husband with wife’s computer or iPad (or vice versa) does something bad there might be an argument that there was negligence on the part of the owner in entrusting that equipment to the bad actor. There are no known published cases on this front, but I’d look to the possibility of more being filed. The argument follows those similar to negligent entrustment of a vehicle.

Causes of Action for the elements for negligent entrustment of chattel shows that two of the essential elements are

- the person to whom the chattel was entrusted was negligent, and
- that person's negligence caused the plaintiff's injury.


Arguments For: It seems that negligence is one way for a plaintiff to arguably get at insurance or homeowners proceeds. It also appears to lower the burden and further take advantage of a ‘negligence per se’ analogy, if there is a criminal violation such as interception or breach of computer security or online posting (or even bullying in this day and age). Thus, if duty and breach are satisfied in a negligence per se argument, this leaves only causation and damages.

Arguments Against: The revenge porn law (for example), however, requires an intentional act, "the person intentionally discloses visual material," Tex. Penal Code Sec. 21.16 (b)(1), "the person intentionally threatens to disclose," id. 21.16(c), or knowing act, "knowing the character and content of the visual material, the person promotes ...", id. 21.16(d) -- and I do not think the law generally treats holding others responsible for a person's knowing or intentional acts the way it does for negligence. In one case, the plaintiff was required to show a defendant had actual knowledge that his son would use a rifle to intentionally shoot another, and failed to provide such proof. Kennedy v. Baird, 682 S.W.2d 377, 378-79 (Tex. App.--El Paso, 1984, no writ).

This cause of action, while not yet rampant may play out in a similar way that intentional v. negligent infliction of emotional distress did a couple decades ago. We shall see.

XVII. Conclusion

These federal and state statutes form a technical and complex web of laws that affect family law attorneys in potentially far-reaching ways. Pay attention if you become aware of information or evidence that may have been obtained illegally. The statutes are unquestionably very technical and you will have to research the statutes and case law each time
you come across an issue, because the interpretation of these laws is constantly evolving.