DON’T HACK ME, BRO

SOCIAL MEDIA, WIRETAPPING, AND INTERCEPTED EVIDENCE
My new book

Available now on Amazon.com
SOCIAL MEDIA FACTS
In 2014, 74% of American adults use social networking sites.

Up from 52% in 2011.

Significantly more Americans have a social media profile than do not.
Consumers continue to spend more time on social networks than on any other category of sites – 16 minutes per hour in the U.S.

Social media has overtaken pornography as the No. 1 internet activity.
35% of couples married between 2005 and 2012 met online.
Facebook has 1.28 billion monthly active users.

(U.S. population is 313.9 million.)

25% of Facebook users don’t bother with privacy settings.
72% of online adults visit Facebook at least once a month.

Facebook users “Like” 4.5 billion items daily.

23% of Facebook users check their account five or more times every day.
On a typical day, more than 500 million Tweets are sent on Twitter, averaging 5,700 per second.

The fastest-growing group on Twitter is the 55-64 age bracket.
YouTube reaches more US adults aged 18-34 than any cable network.

After Google, YouTube is the second largest search engine.
WIRETAPPING AND INTERCEPTED EVIDENCE
Wiretapping

- Texas – Tex. Penal Code 16.02
  Tex. CPRC Ch. 123
Stored Communications

- Federal – 18 U.S.C. 2701-2712
Unauthorized Access

- Federal – 18 U.S.C. 1030
- Texas – Tex. Penal Code 33.02
  Tex. Penal Code 33.07
  Tex. CPRC Ch. 143
Comparing the Acts

Wiretap Act = intercepted contemporaneously with transmission; exclusionary rule

SCA = intercepted while in electronic storage incidental to transmission
Federal Wiretap Act


Ex-wife placed spyware on ex-husband’s computer that forwarded all of his emails to her own private account. Court held that this was a violation of the Federal Wiretap Act and that ex-husband was entitled to $10,000 in liquidated damages.
Federal Laws in State Court

- Federalism

- State courts have general jurisdiction

- State courts have inherent authority and are presumptively competent to adjudicate claims arising under federal laws
Federal Wiretap Act

Offense:
“intentionally intercepts...any wire, oral, or electronic communication”

“wire communication” = “aural transfer”
“oral communication” = “oral communication”
“electronic communication” = “signs, signals, writing, images, sounds, data”
Federal Wiretap Act

Cordless, Wireless, and Cellular:

- Originally considered “radio transmissions” and not protected under the Wiretap Act
- Courts held no one could have reasonable expectation of privacy in such conversations
- Act updated in 1994, Supreme Court confirmed in 2001 that the Act applies
Federal Wiretap Act

Offense:

- “intentionally discloses, or endeavors to disclose, … knowing or having reason to know that the information was obtained through interception”

- “intentionally uses, or endeavors to use, … knowing or having reason to know”
Federal Wiretap Act

Attorney Personal Liability:

Using/disclosing intercepted information to:
- Create deposition questions
- Make a settlement offer
- Make a complaint to internal affairs
- Turn over intercepted recordings to DA
Federal Wiretap Act

**Criminal Penalty:**
- Fined and/or imprisoned up to 5 years

**Civil Cause of Action:**
- Actual damages, or statutory damages of $100/day or $10,000 -- whichever is greater
- Punitive damages, equitable relief
- Attorney’s fees
Federal Wiretap Act

$10,000:
- Per party
- Per violation
- Closely-related course of conduct over relatively short time
- Discretionary or mandatory
Federal Wiretap Act

Statute of Limitations:
- Two years per offense
- Each “use” or “disclosure” has own two-year limitations period
Federal Wiretap Act

Rodgers v. Wood, 910 F.2d 444 (7th Cir. 1990):
Homeowner had recording devices installed. Police illegally made calls during search that were intercepted. Homeowner’s lawyer provided tapes to DA, internal affairs, court. Officers sued lawyer, who had to pay $20,000.
Federal Wiretap Act

Exceptions:
- One-party consent
- All-party consent
- No spousal exception
- Vicarious consent
- First Amendment
Federal Wiretap Act

Exclusionary Rule:

“Whenever any wire or oral communication has been intercepted, no part of the contents…and no evidence derived therefrom may be received in evidence”
Federal Wiretap Act

Exclusionary Rule:

Applies to private conduct and gov’t

Only “wire” and “oral,” not “electronic”

- Internet calls, Skype
- Text messages
Texas Wiretap Law
Tex. Penal Code 16.02

Offense:
“intentionally intercepts...a wire, oral, or electronic communication”

“wire communication” = “aural transfer”
“oral communication” = “oral communication”
“electronic communication” = “signs, signals, writing, images, sounds, data”
Texas Wiretap Law

Offense:

- Intentional disclosure, knowing or having reason to know the information was obtained through interception

- Intentional use, if the person knows or is reckless about whether the information was obtained through interception
Texas Wiretap Law

Criminal Penalty:

- 2nd degree felony
Texas Wiretap Law  
Tex. Penal Code 16.02


Ex-wife taped conversations between her ex-husband and his adult son in which they planned to take her car keys and prevent her from using her car. She then took the recordings to the police station. No action was taken against ex-husband and son, but she was sentenced to 6 years in jail for recording a telephone conversation without consent of any of the parties to the conservation.

On appeal, she unsuccessfully made defenses of necessity and self-defense.
Texas Wiretap Law
Tex. Penal Code 16.02

Vicarious Consent – exception for recording a child


Parent believed her minor child was being abused, so she recorded a telephone conversation between her minor child and the defendant/alleged abuser. Court found that the vicarious consent was proper, and it complied with case law that required that the vicariously-consenting parent have an objective, reasonable belief that consenting to the recording of the conversation on behalf of the child is in the best interest of the child.
TX Wiretap Civil Cause of Action
TX CPRC Chapter 123

Cause of Action:

- Intercepts or attempts to intercept a communication
- Uses or divulges information – knows or reasonably should know was obtained by interception
TX Wiretap Civil Cause of Action

“Communication”:

- Speech uttered by a person
- Information (including speech) that is transmitted with the aid of a wire or cable
TX Wiretap Civil Cause of Action

- Injunction,
- Statutory damages of $10,000 per occurrence,
- Actual damages in excess of $10,000,
- Punitive damages, **AND**
- Attorney’s fees
TX Wiretap Civil Cause of Action

- Federal statute uses “may” in damages provision, damages can be discretionary
- Texas cause of action states a person is entitled to $10,000 for each occurrence
Federal Stored Comm. Act

Offense:
- Intentionally accesses
- Without authorization, or exceeds authorization
- And obtains access to a wire or electronic communication
- While it is in electronic storage
“Electronic storage”:

Temporary, intermediate storage of a wire or electronic communication incidental to its electronic transmission
Federal Stored Comm. Act

Protected:
- “Temporary, intermediate storage”
- “Backup storage”

Not Protected:
- “Post-transmission storage”
Federal Stored Comm. Act

Criminal Penalty:
- 1st offense – fined, imprisoned up to 5 years
- Subsequent – fine, imprisoned up to 10 years

Civil Cause of Action:
- Actual damages not less than $1,000
- Punitive damages, equitable relief
- Attorney’s fees
Miller v. Meyers, 766 F.Supp.2d 919, 923 (W.D.Ar.2011)

Ex-husband placed key-logging software on ex-wife’s computer during divorce. The software allowed him to discover various passwords which he then used to access her email account. He used information he found in her email account against her, and admitted all this to the court. Summary judgment as to his liability for violating the Stored Communications Act was awarded by the court, with damages to be determined at trial.

H used key-logging software to acquire W’s email password, accessed her email, and discovered sexual communications with various individuals. H shared emails with his attorney (co-Defendant) who sent them to W’s attorney for W to admit or deny their authenticity. W then sued H and his attorney for violating the Wiretap Act and the Stored Communications Act.
Federal Stored Comm. Act


Holding:
- H’s MSJ granted as to Wiretap Act because the emails were not viewed by H contemporaneously with their transmission (he read them after she had already opened them).
- H’s MSJ denied as to Stored Communications Act claim; Court disagreed with his interpretation of whether accessed emails were in “electronic storage.”
Criminal Penalty:

- State jail felony
Federal Comp. Fraud & Abuse Act

- Intentionally access a computer without authorization or exceeds authorized access and obtains information from any protected computer
  - + with intent to defraud
  - + causes damage
  - + with intent to extort
Federal Comp. Fraud & Abuse Act

- Crime
  - Penalties range from 1 year to life
  - Forfeiture provision – the court “shall” order the forfeiture of any personal property used to commit the violation and any real or personal property derived as a result of the violation
Federal Comp. Fraud & Abuse Act

○ Civil Cause of Action
  • Actual damages only
  • Includes response costs of employees
  • No exemplary damages, minimum statutory damages, or attorney’s fees
Texas Computer Security Law
Tex. Penal Code 33.02

Offense:

knowingly accesses a computer, network, or system without the effective consent of the owner
Texas Computer Security Law

Criminal Penalty:

- Amt. involved < $20,000 – state jail felony
- < $100,000 – 3\textsuperscript{rd} degree felony
- < $200,000 – 2\textsuperscript{nd} degree felony
- > $200,000 – 1\textsuperscript{st} degree felony

- If not to “harm another” - misdemeanor
Texas Computer Security Law
Tex. Penal Code 33.02


On her last day of work at the Dallas Fire Department, Defendant (a disgruntled employee) corrupted department documents on her work computer as retaliation. As a result of her actions, the department was forced to have the documents recreated at a cost of $1,400. The court found that because she was not authorized to access these documents for the purpose of corrupting them, her conduct was in violation of Tex. Penal Code 33.02.
TX Online Impersonation Law
Tex. Penal Code 33.07

Offense:

- Use the name or persona of a person to create a website, post, or send messages
- With the intent to harm or defraud
TX Online Impersonation Law

Criminal Penalty:
- Class A misdemeanor
- Third-degree felony
TX Online Impersonation Law

Tex. Penal Code 33.07


Man sends creepy packages and communications to woman. When caught and charged, he said he had no intent to harm, only to test victim’s professed psychic abilities.
TX Civil Cause of Action

- Violation of Ch. 33 of the Penal Code
- Breach of computer security, online impersonation
- Actual damages
- Attorney’s fees