Interception

by Emily Miskel

-A Practical Guide to Wiretapping and Data Interception Laws for Civil and Family Law Attorneys

Introduction

Family lawyers frequently have to deal with questionable evidence obtained by clients. This article will give an overview of federal and Texas laws relating to wiretapping, interception of data, breach of computer security, online impersonation, and other computer crime laws, including civil causes of action. The full book, available now on Amazon.com, includes much more detail, including summaries of key cases.

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.

Federal Wiretap Act – 18 U.S.C. §§ 2510-2522

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.

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.

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.

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.

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.

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.

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.

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.

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.

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 communication. 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.

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.

Federal Stored Communications Act – 18 U.S.C. §§ 2701-2712

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.

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.

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.

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.

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.

Federal Computer Fraud and Abuse Act – 18 U.S.C. § 1030

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

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 computers with internet access.

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 circuits 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.

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.

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.

Texas Breach of Computer Security Law – Tex. Penal Code § 33.02

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 Online Impersonation Law – Tex. Penal Code § 33.07

Texas was one of the first states to implement a law prohibiting online impersonation. The law creates two offenses: (1) using the name or persona of another person to create a website or send messages through a social networking site, or (2) sending an electronic communication as if it is from someone else, with the intent to harm. An offense can be a misdemeanor or felony. There is no requirement the harm be physical harm. Emotional distress can be sufficient to qualify as harm under the Penal Code.

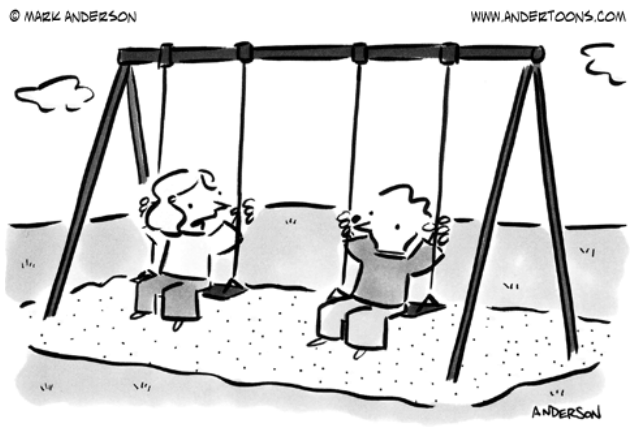
Another crucial element of this offense is the impersonation. If a person merely uses the internet to harm someone, without impersonating, the conduct would not be covered by this section. Rather, it would likely be considered harassment. It is interesting to note that online harassment is a misdemeanor,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

Texas Civil Causes of Action – Tex. Civ. Prac. & Rem. Code Ch. 143

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.

Conclusion

These federal and state statutes form a technical and complex web of laws that affect family law attorneys in potentially far-reaching ways. The book contains an overview of a field with significant depth, and interested practitioners should devote time to reading the statutes and the cases interpreting and applying them.



"I want to be a lawyer - they still get recess."