Wiretapping & Data Interception in Civil and Family Law Cases

By Hon. Emily Miskel

Civil and family law attorneys are increasingly confronted with situations where a client's information has been improperly accessed or where a client has obtained information improperly. The laws relating to interception of communications and electronic data are a confusing web of state and federal statutes, which can include harsh penalties and damages for clients. These laws can also create personal criminal and financial liability for lawyers.

There are three general categories of laws relating to interception of communications. At the federal level they are referred to as:

- the Wiretap Act (Title I of the Electronic Communications Privacy Act),
- the Stored Communications Act (Title II of the ECPA) , and
- the Computer Fraud and Abuse Act.

Texas has also adopted state versions of each law, with criminal offenses in the Texas Penal Code and civil causes of action in the Texas Civil Practice and Remedies Code.

Wiretap Act

The wiretap laws apply to communications that are intercepted *contemporaneously* with transmission. This can include in-person conversations, phone conversations, and even electronic communications, as long as the communication is intercepted at the time it is being transmitted. The wiretap laws have the most severe penalties, strict exclusionary rules, and highest statutory damages.

Use and Disclosure Liability – Under the Wiretap Act, it is also a violation to "use" or "disclose" any contents of a communication if you know or have reason to know that it was obtained through interception. Cases have held that attorneys' use of information obtained from a client's wiretapped recordings to prepare deposition questions, make settlement offers, report criminal activity, or even to play the recordings at trial are violations. These are separate, independent wiretap violations by the attorney, and the attorney is personally liable for $10,000 or more in statutory damages and possible criminal penalties.

Exceptions – There are several exceptions to the Wiretap Act that permit recording. Under federal and Texas law, only one person in a communication need consent to a recording. In other words, a participant can record her communications. However, some states have all-party consent laws, and the law of the stricter state applies. It is safest to caution your clients not to record any conversation where a party may be outside Texas, without a disclosure that the communication may be recorded. A parent can give vicarious consent to the recording of a child's conversations if the parent has a good faith, objectively reasonable belief that the recording is necessary for the welfare of the child.

Stored Communications Act

The stored communications laws apply to communications that are intercepted while in electronic storage incident to transmission. Federal opinions conflict as to the interpretation of terms such as "temporary, intermediate storage" or "backup storage." For example, some courts have held that all webmail stored online is in electronic storage incident to transmission, while other courts have held that only unopened webmail is subject to an interception violation under the Stored Communications Act. In practice, proving a claim under stored communications laws can be complex because the success of the claim depends on technical fact issues as to how the electronic information was stored and sent.

Computer Fraud and Abuse Act

The Wiretap Act and Stored Communications Act would not generally apply to someone who obtained communications saved on the recipient's device. The Computer Fraud and Abuse Act (CFAA) and similar laws apply to circumstances where data is obtained locally from a person's computer or phone. These laws make it a violation to access a computer, network, or system without the effective consent of the owner, or to exceed authorization. Under the CFAA, "protected computer" includes any data processing device used in interstate commerce (i.e. any device that connects to the internet). Generally, proving a claim under the CFAA requires a minimum of $5,000 in damages, but that can include response costs, salaries of employees to repair the harms, lost profits, technical consultants, outside contractors, and more.

Violation of usage policies–Some federal courts have held that violating terms of service or a computer usage policy can be a violation of the CFAA. The 9th Circuit has taken a strong position against this broad application of the CFAA, but other circuits have enforced criminal penalties against, for example, employees who take an employer's electronic information.

Online Impersonation

Texas also has criminal and civil claims for online impersonation. It is a felony to impersonate someone by creating a web page or social media account, or sending messages through a website or social networking site. It is a misdemeanor to impersonate someone by sending email, instant messages, or text messages.

Originally published in the October 2015 issue of the Dallas Bar Association Headnotes.

About the Author

Emily Miskel is judge of the 470th district court in Collin Country. She can be reached at emily@emilymiskel.com.