

A. THE WIRETAP ACT (as amended by the ECPA)

a. *The Claim/Crime*

In order to state a civil claim under Section 2511(1)(a), a plaintiff must demonstrate that the defendant:

- (1) intentionally intercepted, endeavored to intercept, or procured another person to intercept or endeavor to intercept;
- (2) any wire, oral, or electronic communication.

See 18 U.S.C. § 2511(1)(a). The criminal component of the Act requires the same elements for each of these three potential violations, albeit with the higher standard of proof.

“**Intercept**” means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. *Id.* § 2510(4).

“**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, photo-electronic or photo-optical system that affects interstate or foreign commerce, but does not include . . . any wire or oral communication.” *Id.* § 2510(12).

b. Defenses

(1) CONSENT

It shall **not be unlawful** [under the WTA] for a person acting under color of law to intercept a wire, oral, or electronic communication, **where such person is a party** to the communication **or one of the parties** to the communication **has given prior consent** to such interception.

It shall **not be unlawful** [under the WTA] 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 **unless** such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(2) PUBLICLY ACCESSIBLE

It shall **not be unlawful** under [the WTA or the SCA] to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily **accessible** to the general **public**.

(3) COURT ORDER

C. THE STORED COMMUNICATIONS ACT

a. The Claim/Crime

To state a claim under Section 2701(a), the plaintiff must demonstrate that the defendant:

- (1) intentionally accessed without authorization or by exceeding an authorization;
- (2) a facility through which an electronic communication service is provided; and
- (3) thereby obtained, altered or prevented authorized access to an electronic communication while it was in electronic storage.

See 18 U.S.C. § 2701(a). The criminal component of the statute requires the Government to prove the same, albeit pursuant to a higher standard of proof.

The statute defines an “**electronic communication service**” as any “service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15).

The key component of the SCA is “**electronic storage.**”

That term is defined in the statute as:

- (1) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; or
- (2) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

See 18 U.S.C. § 2510(17).

b. Exceptions/Defenses

(1) AUTHORIZATION

A section of the SCA entitled “**Exceptions**” provides that the SCA does not apply to conduct authorized:

- (1) by the person or entity providing a wire or electronic communications service; or
- (2) by a user of that service with respect to a communication of or intended for that user.

See 18 U.S.C. §§ 2701(c)(1), (2).

“**user**” means any person or entity who

- (A) uses an electronic communication service; and
- (B) is duly authorized by the provider of such service to engage in such use.

Id. §§ 2711(1), 2510(13).

(2) COURT ORDER