Lexis Practice Advisor® is a comprehensive practical guidance resource for attorneys. It includes "how to" practice notes, model forms, and on point cases, statutes, administrative materials, emerging issues articles, and treatise sections. The Labor & Employment offering contains access to a unique collection of expertly authored content, continuously updated to help you stay up to speed on leading practice trends. The following is a practice note from the Monitoring and Testing Employees subtopic under the Privacy, Technology, and Social Media topic.

Lexis Practice Advisor Labor & Employment

Understanding the Electronic Communications Privacy Act

by Michael E. Lackey, Mayer Brown LLP

Michael E. Lackey leads Mayer Brown's global litigation and dispute resolution practice, and is a partner in the firm's Electronic Discovery & Information Governance group. Assistance provided by former associate Joseph P. Minta.

Because electronic communication almost always occurs through a third party – such as an Internet Service Provider – Congress passed the Electronic Communications Privacy Act (ECPA) in 1986 to statutorily protect the privacy of these communications.

This practice note discusses key issues involving the ECPA. For a checklist concerning major ECPA issues, please see Checklist – Examining Electronic Communication Privacy Act (ECPA) Issues.

Structure of the ECPA

The ECPA has two main components: the Wiretap Act, 18 U.S.C. § 2510 et seq. and the Stored Communications Act (SCA), 18 U.S.C. § 2701 et seq.

Generally speaking, the Wiretap Act governs when communications (whether electronic, oral, or wire) are "intercept[ed]." It broadly defines the term "intercept" to mean "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." 18 U.S.C. § 2510(4).

The SCA, as the name suggests, governs access to electronic communications "in electronic storage." "Electronic storage" means "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). For additional guidance on the SCA, please see Navigating the Stored Communications Act; and Checklist – Examining Stored Communications Act (SCA) Issues.

Modern technology does not neatly divide into these categories, however, and you should exercise caution in determining which portions of the ECPA apply to particular factual circumstances. (If in doubt, consider bringing alternative claims under the Wiretap Act and the Stored Communications Act to avoid this issue.) Below, we discuss the principles courts apply in determining whether the Wiretap Act or the SCA applies. Note that, until 2001, the Wiretap Act also included an "electronic storage" component, further complicating the analysis. See, e.g., Noel v. Hall, 568 F.3d 743, 749 & n.10 (9th Cir. 2009).

Also note that the ECPA sets forth the rules governing pen registers and trap and trace devices, which record the telephone numbers called from or calling to (respectively) a particular telephone line. See 18 U.S.C. § 3121 et seq. The ECPA prohibits the use of these devices without a court order. See 18 U.S.C. §§ 3122-23. Although rarely litigated, this provision effectively prohibits private parties from using such devices.

E-mails

One of the most common ways potential ECPA liability arises involves unauthorized access to e-mails.

Although perhaps somewhat counter-intuitive, courts generally concur that unauthorized access of web-based e-mails violates the SCA and *not* the Wiretap Act. See Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004) (collecting cases). See Navigating the Stored Communications Act. Courts reason that Wiretap Act liability hinges on intercepting electronic communications at the time of their transmission. See United States v. Barrington, 648 F.3d 1178, 1202 (11th Cir. 2011). E-mails left with a provider for later retrieval and access are no longer in the process of "transmission."

Note that there is a fine line between transmission and storage. In *Councilman*, the petitioner was the vice-president of a listserv specializing in rare and out-of-print books. The listserv provides a webmail service to subscribers. Councilman instructed employees to intercept e-mails from subscribers to Amazon and copy those e-mails into a separate mailbox. The e-mail process necessarily involves assembling, disassembling, and reassembling messages at the appropriate mailboxes. During the assembly process, e-mails sit in temporary electronic storage. Councilman alleged that since he accessed the e-mails while they were sitting in temporary electronic storage, no Wiretap Act liability arises. The First Circuit sitting en banc rejected this argument, holding that because the electronic storage alleged by Councilman was transient and intrinsic to the communication process, the e-mail was still an electronic communication in transmission and therefore protected by the Wiretap Act. See United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (en banc). Courts have not further clarified what is transient electronic storage intrinsic to the communication process.

Similarly, if the e-mails are accessed and copied contemporaneously with being transmitted, courts have upheld Wiretap Act liability. See United States v. Szymuszkiewicz, 622 F.3d 701, 703-04 (7th Cir. 2010); Zaratzian v. Abadir, 2014 U.S. Dist. LEXIS 129616 (S.D.N.Y. Sept. 2, 2014).

Other Technologies

This section briefly discusses how courts have applied the ECPA to other types of technology.

- *Keylogger Software*. A court held recording a user's keystrokes using "keylogger" software did not violate the Wiretap Act because those keystrokes were not being transmitted beyond the computer at the time. See United States v. Scarfo, 180 F. Supp. 2d 572, 582 & n. 5 (D.N.J. 2001). The court noted that, in this case, the software was configured to work only when all communication ports were inactive.
- *Website Access*. When an individual accesses a secure website without authorization, this does not violate the Wiretap Act. Depending on the nature of the access, however, it may violate the Stored Communications Act. See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879-80 (9th Cir. 2002).
- *Replaying/Copying Technology*. Often when a communication is "intercepted," it is recorded for later use or analysis. Where a recorded communication is copied or replayed, it is not "intercepted" for a second time. Thus, the later act does not violate the Wiretap Act. See Noel v. Hall, 568 F.3d 743, 748-49 (9th Cir. 2009) (collecting cases).
- *Voicemails*. While technologically difficult to distinguish from general replaying technology, the Ninth Circuit has concluded that accessing voicemail messages violated the Wiretap Act. See United States v. Smith, 155 F.3d 1051 (9th Cir. 1998); see also *Noel*, 568 F.3d at 750 (discussing *Smith's* continued validity).

In light of the rapid pace of technological development and potential divergences among courts, you should research the specific technology at issue and case law in the relevant jurisdiction.

Scope of Liability Under the ECPA

The ECPA provides for criminal and private civil liability for violations of its provisions. See 18 U.S.C. § 2520(a) (Wiretap Act liability); 18 U.S.C. § 2707 (Stored Communications Act liability).

A civil plaintiff may recover either the actual damages they suffer, or statutory damages, along with punitive damages. See 18 U.S.C. § 2520 (Wiretap Act); 18 U.S.C. § 2707 (Stored Communications Act). However, courts disagree as to whether proof of some actual damage is a necessary prerequisite to statutory damages.

Compare Van Alstyne v. Electronic Scriptorium, Ltd., 560 F.3d 199, 206 (4th Cir. 2009) with Shefts v. Petrakis, 931 F. Supp. 2d 916 (C.D. Ill. 2013).

Courts generally agree that the ECPA does not impose civil liability under aiding-and-abetting theories. See, e.g., Kirch v. Embarq Management Co., 702 F.3d 1245, 1246-47 (10th Cir. 2012) (Wiretap Act); Council on American–Islamic Relations Action Network, Inc. v. Gaubatz, 891 F. Supp. 2d 13, 26–27 (D.D.C.2012) (Stored Communications Act).

Exceptions to ECPA Liability

Both the Wiretap Act and the Stored Communications Act contain numerous exceptions to their prohibitions. While many of these exceptions address law enforcement's ability to access electronic communications, many others potentially apply to private entities.

In evaluating potential ECPA liability, you should know about the following commonly used potential exceptions to Wiretap Act liability:

- *Normal Business*. The Wiretap Act does not apply to communications intercepted as part of the "ordinary course of business." See, e.g., Kirch v. Embarq Management Co., 702 F.3d 1245, 1249 (10th Cir. 2012). Without this exception, Internet Service Providers would face potential ECPA liability as they route electronic communications through the internet as part of their daily work;
- *Not Private*. The Wiretap Act also does not apply if the communications are "readily accessible to the general public." See 18 U.S.C. § 2511(2)(g)(i). This may provide a defense for the interception of, e.g., unencrypted radio communications, such as when a walkie-talkie accidentally picks up communications from other groups operating on the same frequency. See Joffe v. Google, Inc., 746 F.3d 920 (9th Cir. 2013) (declining to apply exception to interception of private wireless networks);
- *Silent Video*. Because of the use of the term "aural" in the definition of "interception," 18 U.S.C. § 2510(4), the Wiretap Act does not apply to silent video surveillance. See United States v. Larios, 593 F.3d 82, 90 (1st Cir. 2010) (collecting cases); and
- *Consent*. The Wiretap Act does not apply if one party to the communication consents. See 18 U.S.C. § 2511(2)(d). Although a number of states require all parties to consent, see, e.g., Cal. Penal Code § 632(a), Fla. Stat. § 934.03, federal law only requires one party to the communication to consent. Relatedly, the Wiretap Act does not apply where communications are sent to the intended recipient, who may then forward them on to others surreptitiously. See Crowley v. Cybersource Corp., 166 F. Supp. 2d 1263, 1268 (N.D. Cal. 2001).

There are also a variety of potential exceptions to Stored Communications Act liability. You should review Navigating the Stored Communications Act — Exceptions to SCA Prohibitions.

Examples of Potential ECPA Issues

The broad scope of the ECPA offers some hint at the many circumstances in which it might apply. Although by no means an exhaustive list, you should counsel clients to consult an attorney about potential ECPA liability if they are:

- *Monitoring Employee Electronic Communications*. Modern technology often allows employers to access employees' actions on company-provided computers, smart-phones, and other devices. If the employer conducts this monitoring without adequate consent, ECPA liability may result.
- *Tracking Consumers' Electronic Behavior*. Most companies today maintain a significant internet presence, seeking to further engage with current and potential customers. Efforts to track these individuals' actions, whether through smart-phone "apps," internet browser "cookies" (small pieces of data stored on an internet-user's computer), or other means, has led to a number of ECPA lawsuits.
- *Suffering from a "Hacking" Attack*. The ECPA, along with the Computer Fraud and Abuse Act can provide a remedy for companies whose computer systems are accessed without authorization.
- *Suspecting Disclosure of Confidential Information*. Numerous ECPA cases have arisen when disgruntled former employees have sought to take confidential electronic documents when they leave their employment or after termination. Depending on the methods these former employees use, the ECPA may offer a way to prevent these actions or recover for the injury caused by the disclosure.

- *Accessing Electronic Files of Another*. Whether by accident or not, companies may find themselves with access to electronic files of another company. Accessing these files without the other company's consent may result in ECPA liability. Similarly, spouses surreptitiously accessing or monitoring the others' electronic communications often leads to issues of ECPA liability.