Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22.

Background. The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986. The ECPA updated the Federal Wiretap Act of 1968, which addressed interception of conversations using "hard" telephone lines, but did not apply to interception of computer and other digital and electronic communications. Several subsequent pieces of legislation, including The USA PATRIOT Act, clarify and update the ECPA to keep pace with the evolution of new communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases.

General Provisions. The ECPA, as amended, protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically.

Civil Rights and Civil Liberties. "The structure of the SCA reflects a series of classifications that indicate the drafters' judgments about what kinds of information implicate greater or lesser privacy interests. For example, the drafters saw greater privacy interests in the content of stored emails than in subscriber account information. Similarly, the drafters believed that computing services available 'to the public' required more strict [sic] regulation than services not available to the public…To protect the array of privacy interests identified by its drafters, the [Act] offers varying degrees of legal protection depending on the perceived importance of the privacy interest involved. **Some information can be obtained from providers with a subpoena; other information requires a special court order; and still other information requires a search warrant.** In addition, some types of legal process require notice to the subscriber, while other types do not."

The Act reflects a general approach of providing greater privacy protection for materials in which there are greater privacy interests. For a more in-depth analysis,U.S. Dept. of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence In Criminal Investigations (2009), pp. 115-116, (287pp | 1.01mb | PDF).

Specific Provisions. The ECPA has three titles:

Title I of the ECPA, which is often referred to as the Wiretap Act, prohibits the intentional actual or attempted interception, use, disclosure, or "procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." Title I also prohibits the use of illegally obtained communications as evidence. 18 U.S.C. § 2515.

> Exceptions. Title I provides exceptions for operators and service providers for uses "in the normal course of his employment while engaged in any activity which is a necessary incident

to the rendition of his service" and for "persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act (FISA) of 1978." 18 U.S.C. § 2511. It provides procedures for Federal, State, and other government officers to obtain judicial authorization for intercepting such communications, and regulates the use and disclosure of information obtained through authorized wiretapping. 18 U.S.C. § 2516-18. A judge may issue a warrant authorizing interception of communications for up to 30 days upon a showing of probable cause that the interception will reveal evidence that an individual is committing, has committed, or is about to commit a "particular offense" listed in § 2516. 18 U.S.C. § 2518.

Title II of the ECPA, which is called the Stored Communications Act (SCA), protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses. 18 U.S.C. §§ 2701-12.

Title III of the ECPA, which addresses pen register and trap and trace devices, requires government entities to obtain a court order authorizing the installation and use of a pen register (a device that captures the dialed numbers and related information to which outgoing calls or communications are made by the subject) and/or a trap and trace (a device that captures the numbers and related information from which incoming calls and communications coming to the subject have originated). No actual communications are intercepted by a pen register or trap and trace. The authorization order can be issued on the basis of certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the applicant's agency.

Amendments. The ECPA was significantly amended by the Communications Assistance to Law Enforcement Act (CALEA) in 1994, the USA PATRIOT Act in 2001, the USA PATRIOT reauthorization acts in 2006, and the FISA Amendments Act of 2008 (116pp | 303kb | PDF). Other acts have made specific amendments of lesser significance.

Source: Page created by the DHS/Office for Civil Rights and Civil Liberties and the DHS/Privacy Office in cooperation with the DOJ, Office of Justice Programs, Bureau of Justice Assistance.