Electronic Communications Privacy Act of 1986

By Saranna Hack

Our society has seen many technological advances that shape our lives on a daily basis. With the invention of the computer and its technology, there has been a need for legal protections. Along with the computer has come the invention of email, a way of communicating with other individuals via "electronic communication". What once took days to communicate via mail carrier, now takes a matter of minutes via a modem. With this new technology of sending messages via a modem through the phone lines, the possible intrusion from individuals or even the government has created a great controversy over the legality of such communication. This creates an invasion of privacy as some would say. The Fourth Amendment constitutes that people have the right to expected privacy against unreasonable searches and seizures without a lawful search warrant. So how does one protect their self when it comes to the privacy of sending messages over a computer. The exposure of the electronic communication also raises the issue of interception of computer transmissions. I will attempt to discuss Title I of the Electronic Communication Privacy Act of 1986 and how it pertains to the privacy of individuals against such interception.

On 21 October 86 President Reagan signed into law the Electronic Communications Act (ECPA). This act amended Title III of the Omnibus Crime Control and Safe Street Act of 1968 (42 USC § 3789d), which authorized court-ordered Government wiretapping. This is referred to commonly as: The Federal Wiretap Law.

For nearly twenty years Title III remained the only protection against the invasion of privacy for oral and wire communications. With the invention of email, pagers, cellular phones, computer transmissions, and the technological changes during the 1970's and 1980's, Congress felt the outdated law needed updating to expand the legal privacy protection to include electronic communications. The act consists of two parts, Title I, which is codified in Chapter 119 and contains sections 2510 - 2522, and Title II which is codified in Chapter 121 and contains sections 2701 - 2709. Both Title I and Title II are encompassed under Title 18 of the United States Code ("18 USC § 2510 – 2522" and "18 USC § 2701 – 2709")

The purpose of the ECPA is to protect the "electronic communications" from unauthorized interception and access since it was not clear if the necessary security measures in assuring privacy were being met. The ECPA expanded these privacy protections of the Wiretap Act in five significant ways. First, it broadens the scope of privileged communications to include all forms of electronic transmissions, including video, text, audio, and data. Second, it eliminates the requirement for communications be transmitted via common carrier to receive legal protection. Third, it maintains restrictions on the interception of messages in transmission and adds a prohibition on access to stored electronic communications. Fourth, it responds to the Supreme Court's

ruling in Smith v. Maryland that telephone toll records are not private and restricts law enforcement access to transactional information pertaining to users of electronic communication services. And finally, it broadens the reach of the Wiretap Act by restricting both government and private access to communications.

Title I covers Fourth Amendment principles to include a provision supporting the "plain view doctrine". It regulates the interception of electronic data making any unauthorized interception illegal except in a criminal investigation where such interception would be legal. Under the ECPA, protected communications that are revealed to the public lose their privacy expectations. Where the law once said you can't bug private telephone communications it now says you can't bug private computer communications.

Title I consists of eleven sections (2510 – 2522). Section 2510 of the act defines electronic communications as: "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".

Section 2511 makes it a crime to attempt or intentionally intercept electronic communications, to intentionally disclose or use the contents of an intercepted communication. This also restricts electronic communication providers from intentionally divulging the contents of a communication during transmission. Section 2512 makes it illegal for any person to send through the mail or through interstate commerce a device whose primary purpose is intercepting electronic communications. This also restricts the manufacture, sale,

possession, advertisement and assembly of such devices. One exception is that electronic communications service providers, officials, agents, employees of the United States, or political subdivisions in the normal course of business, may mail, send, carry, possess, sell, or manufacture such devices without violating the Act.

Section 2513 allows for the seizure and forfeiture of interception devices to the United States if they violate the act.

Section 2515 allows for the exclusion of illegally intercepted communications and its contents from court.

Section 2516 allows for application to a court to obtain authorization to intercept electronic communications. The Act allows the United States Attorney General and "any attorney for the Government", as defined by the Federal Rules of Criminal Procedure to seek such an order for an investigation when the interception may provide evidence of a federal offense.

Section 2517 authorizes law enforcement officers who obtained information legally to disclose and use the contents of those communications to the extent that is appropriate, even if the information relates to an offense that was not included in the authorization request. As a result of such interception privileged communications will not lose their privileged status.

Section 2518 states the formal requirements for application by a law enforcement agency. It also contains the formal requirements for the court order authorizing interception, the standard for issuing such order, the jurisdictional requirements for issuing the order, and the territorial limitations of such order.

Section 2519 states that each court and law enforcement agency which grants or requests an order allowing interception is required to make a report to the Administrative Office of the United States Courts. The Administration Office compiles the information reported into its office's report to Congress.
Section 2520 allows for the person whose communication was intercepted to bring a civil action. If a person who in good faith relies on a court order, request from a law enforcement officer, or reading of the Act is exempt from liability. It also sets a two-year statute of limitations on any action brought under the Act. The statute of limitations begins running after the first reasonable discovery of the violation.
Section 2521 allows for an injunction to end violations or cut off suspected violations of the Act before they occur. The action must be initiated by the United States Attorney General, and must be intended to keep the United States, or the party on whose behalf the action is brought, from incurring continuing and substantial injury.
Section 2522 provides for a civil penalty against communication providers who fail to assist authorized interceptions of communications. The civil penalty may be up to $10,000 per day, depending on several factors listed in the section.

While it is illegal for any person, including a system operator (sysop), to intercept or disclose electronic communications to anyone other than the intended individual. There are exceptions for the sysop in which they can disclose such interception. First, the system operator can divulge the contents of the communication if authorized under section 2511(2)(a) or 2517. Second, he/she can divulge the contents of the interception with the lawful consent of either the sender or the intended recipient of the communication. Third,

he/she can divulge the contents to whomever necessary in order to forward it to its destination. Finally, he/she can divulge the contents if it appears that there is a crime in commission, but this only can be divulged to a law enforcement agency.

Although there are many exceptions to the ECPA, when it comes to computer crime, there are only seven exceptions, which apply. Interception pursuant to a §2518 court order. 'Consent' exception §2511(2)(c)-(d). 'Provider' exception §2511(2)(a)(i). 'Computer Trespasser' exception §2511(2)(i). 'Extension Telephone' exception §2510(5)(a). 'Inadvertently obtained Criminal Evidence' exception §2511(3)(b)(iv). 'Accessible to the Public' exception §2511(2)(g)(i). In order to determine if different surveillance strategies will apply, prosecutors and agents need to understand the scope of these seven exceptions.

Sources:

http://www.consumerprivacyguide.com/law/ecpa.shtml

http://legal.web.aol.com/resources/legislation/ecpa.html

http://www.betterboard.net/attserv/practice/cyberlaw/privacy/expa.asp

http://www.law.wfu.edu/students/IPLA/winds.pdf

http://www.privacilla.org/government/ecpa.html