Electronic Communication Privacy Act

Jason Lazarus & Saranna Hack
Electronic Communication Privacy Act

- Signed into law: October 21, 1986
- Codified: 18 USC 2510 - 2522
  18 USC 2701 - 2709
- Purpose: To protect “electronic communication” from unauthorized interception, disclosure or access
- Two Parts: Title I - Chapter 119
  Title II - Chapter 121
Wiretap Act Privacy Protections

- Broadens scope of privileged communications
- Transmitted communications requirements
- Maintains restrictions on the interception and prohibition on access to stored electronic communications
- Responds to the Supreme Court’s ruling in Smith v. Maryland
- Broadens the reach of the Wiretap Act
Title I

Covers Fourth Amendment Principles and the “plain view doctrine”

Where the law says you can’t bug private telephone communications it now says you can’t bug private computer communications
Title I: Wire and Electronic Communications interception and interception of Oral Communication

- Sec 2510: Definitions
  “electronic Communications “
- Sec 2511: Interception and Disclosure of wire, oral, or electronic communications prohibited
- Sec 2512: Manufacture, Distribution, Possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited
- Sec 2513: Confiscation of wire, oral, or electronic communication intercepting devices
- Sec 2515: Prohibition of use as evidence of intercepted wire or oral communications
- Sec 2516: Authorization for interception of wire, oral, or electronic communications
- Sec 2517: Authorization for disclosure and use of intercepted wire, oral, or electronic communications
- Sec 2518: Procedure for interception of wire, oral, or electronic communications
- Sec 2519: Reports concerning intercepted wire, oral, or electronic communications
- Sec 2520: Recovery of civil damages authorized
- Sec 2521: Injunction against illegal interception
- Sec 2522: Enforcement of the Communications Assistance for Law Enforcement Act
Sysop Exceptions

- If Authorized
- If the sysop gets permission from the sender or the intended recipients
- If the sysop must look at the content to forward it
- If a message looks like a possible crime
Computer Crime Exceptions

- Interception pursuant to a §2518 court order
- ‘Consent’ exception
- ‘Provider’ exception
- ‘Computer Trespasser’ exception
- ‘Extension Telephone’ exception
- ‘Inadvertently obtained Criminal Evidence’ exception
- ‘Accessible to the Public’ exception
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