THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) IN A NUTSHELL

BY
DANIEL J. SOLOVE
&
PAUL M. SCHWARTZ

for use in conjunction with

INFORMATION PRIVACY LAW
(4th edition, Aspen 2012)

	THE WIRETAP ACT	**THE STORED COMMUNICATIONS ACT**	**THE PEN REGISTER ACT**
Codified At	18 U.S.C. §§ 2510-2522	18 U.S.C. §§ 2701-2711	18 U.S.C. §§ 3121-3127
Applies To	Interception of communications in flight	(1) Accessing communications in "electronic storage"; (2) Records of ISPs	Pen registers and trap and trace devices
Key Provisions	Interception: provides strict controls on the "interception" of communications. "Interception" is the acquiring of the contents of a communication through an electronic, mechanical, or other device while the communication is being transmitted.	Stored Communications: requires the government to obtain via court order, subpoena, or warrant. § 2703 ISP Records: requires the government to obtain a warrant or court order to access specified customer data held by ISPs, including name, address, length of service, means of payment, etc. § 2703(c)	Requires court order before installation of pen registers and trap and trace devices.

	THE WIRETAP ACT	THE STORED COMMUNICATIONS ACT	THE PEN REGISTER ACT
Court Order	Application for court order to intercept must contain details justifying the interception and information about how the interception will occur and its duration. §2518 The judge must find: (1) probable cause (2) alternatives to interception had failed, are unlikely to succeed, or will be too dangerous. Orders must require that interception be conducted to "minimize the interception of the communications not otherwise subject to interception." §2518(6). Only high level government prosecutors can apply for orders. Orders are limited to certain crimes (most felonies); orders cannot be obtained to investigate misdemeanors.	Communications Stored 180 Days or Less: Government must obtain warrant supported by probable cause. §2703(a) Communications Stored Over 180 Days: Government must provide prior notice to subscriber and obtain a subpoena or court order. §2703(b) Court order requires "specific and articulable facts showing that there are reasonable grounds" to believe communications are relevant to the criminal investigation. §2703(d) If government does not provide prior notice to subscriber, it must obtain a warrant. §2703(b). ISP Records: Government must obtain court order; same standard as that for communications stored over 180 days.	The government must obtain a court order to install pen register and trap and trace devices. The court "shall" grant the order if the government has demonstrated that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." §3123(a).
Exceptions	Consent: Wiretap Act does not apply if one party to the communication consents. §2511(2)(c). Service Provider: Wiretap Act does not apply to the interception of communications by a communications service provider. §2511(2)(a)(i).	Consent: SCA does not apply if the subscriber consents. §2702(b). Service Provider: SCA does not apply to the accessing of stored communications by communications service providers. §2701(c)(1).	
Exclusionary Rule	Yes, for wire and oral communications. No, for electronic communications	No	No

	THE WIRETAP ACT	THE STORED COMMUNICATIONS ACT	THE PEN REGISTER ACT
Penalties	Damages (minimum $10,000 per violation) §2520 Up to 5 years imprisonment. §2511	Damages (minimum $1,000 per violation) Up to 1 year imprisonment (if done for commercial gain) §2701(b)	Fines. Up to 1 year imprisonment §3123(d).
USA-PATRIOT Act Changes	USA-PATRIOT Act shifts temporarily stored wire communications from the Wiretap Act to the SCA. Previously, voicemail that was not yet accessed by the recipient was considered in "temporary" storage, and accessing it was an "interception" because the message had not yet reached its recipient.	Stored Communications: Expands scope of warrants to obtain stored communications less than 180 days old to nationwide scope. ISP Records: USA-PATRIOT Act expands the list of ISP records that the government can obtain from the ISP, adding records of session times and durations, temporary IP addresses, and credit card or bank account numbers used for payment.	USA-PATRIOT Act expands the definition of pen registers and trap and trace devices. Old Definition: Prior definition defined these devices as "devices" that record "the numbers dialed or otherwise transmitted on the telephone device." New Definition: New definition includes "devices" or "processes" that record, in addition to numbers dialed, "dialing, routing, addressing or signaling information" §3127(3) This change expands the definition to include IP addresses and email header information. Expands scope of orders to nationwide.

THE FOURTH AMENDMENT vs.
FEDERAL ELECTRONIC SURVEILLANCE LAW

	FOURTH AMENDMENT	FEDERAL ELECTRONIC SURVEILLANCE LAW
Applicability	The Fourth Amendment applies to electronic surveillance when there is a reasonable expectation of privacy. The Fourth Amendment applies only to government officials (subject to limited exceptions).	Federal electronic surveillance law applies to all interceptions of communications and to accessing stored communications (even if there is no reasonable expectation of privacy). Federal electronic surveillance law applies to pen registers and trap and trace devices (Pen Register Act). The Fourth Amendment does not apply to these devices. *See Smith v. Maryland.* Federal electronic surveillance law applies to government officials and to private parties.
Judicial Authority to Obtain Access	Subject to a number of exceptions, the Fourth Amendment requires a warrant supported by probable cause.	Federal electronic surveillance law contains a wide variety of forms of judicial authority, including subpoenas, court orders with varying levels of notice to the subject of the investigation, warrants, and the super warrant required by the Wiretap Act.
Duration of Authority to Obtain Access	Fourth Amendment warrants authorize a single entry and prompt search. Warrants must be narrowly circumscribed.	Federal wiretap orders have a rather broad duration. A judge can authorize 24-hour surveillance for a 30-day period.
Enforcement	The Fourth Amendment is enforced by the exclusionary rule. The Fourth Amendment can serve as the basis for a §1983 or *Bivens* action.	Federal electronic surveillance law is enforced through the exclusionary rule only sometimes – for interceptions of wire or oral communications under the Wiretap Act. Federal electronic surveillance law also has civil and criminal penalties.