INFORMATION PRIVACY LAW COURSE SERIES

Law Enforcement and National Security in the US

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA)

	THE WIRETAP ACT	THE STORED COMMUNICATIONS ACT	THE PEN REGISTER ACT
Codified	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.
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).	

	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 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).
Exclusionary Rule	Yes, for wire and oral communications. No, for electronic communications	No	No
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).