Privacy and Information Security Law

Randy Canis

CLASS 6

Privacy and Law Enforcement pt. 1
Privacy and Law Enforcement pt. 1
Privacy v. Security

• “One way that government promotes security is by investigating and punishing crimes. To do this, law enforcement officials must gather information about suspected individuals. Monitoring and information gathering pose substantial threats to privacy.”
Constitutional Regulatory Regime

• The Fourth and Fifth Amendments significantly limit the government's power to gather information.
  – 4th – "regulates the government's activities in searching for information or items as well as the government's seizure of things or people."
  – 5th – "guarantees that 'no person . . . shall be compelled in any criminal case to be a witness against himself. . . .' The Fifth Amendment establishes a 'privilege against self-incrimination,' and it prohibits the government from compelling individuals to disclose inculpatory information about themselves."
A. THE FOURTH AMENDMENT AND EMERGING TECHNOLOGY
4th Amendment

• The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
4th Amendment Issues

1) Is the government’s information collecting regulated by the 4th Amendment?

2) Is the search or seizure reasonable?

3) What is the result of the 4th Amendment violation?
Applicability of Searches and Seizures

- 4th Amendment applies every time government officials conduct a “search” or “seizure” of an object, document or person
Reasonable Searches and Seizures

- The 4th amendment does not bar searches and seizures, but requires that they be “reasonable”.
  - “Generally, a search or seizure is reasonable if the police have obtained a valid search warrant. To obtain a warrant, the police must go before a judge or magistrate and demonstrate that they have ‘probable cause’ to conduct a search or seizure.”
Scope of Search Warrants

• No unfettered search
  – “If the scope of the search exceeds that permitted by the terms of a validly issued warrant or the character of the relevant exception from the warrant requirement, the subsequent seizure is unconstitutional without more.”
Exceptions to Warrant and Probable Cause Requirements

• Searches and seizures can be reasonable even without a warrant and probable cause
  – Impracticality, consent to search, "special needs" exception
  – Terry stops
  – Checkpoint and information seeking stops
Exclusionary Rule and Civil Remedies

• Redress for government official’s violation of the 4th Amendment:
  – Suppression of evidence at a criminal trial ("exclusionary rule")
  – Civil remedy (1983 Action)
Subpoenas and Court Orders

- **Court orders** – information gathering mechanism specified by statute or regulations
- **Subpoena** – an order to obtain testimony or documents
Quashing

- “If the party served with the subpoena has an objection, she may bring a motion to quash or modify the subpoena.”
Wiretapping, Bugging, and Beyond

- "A 'wiretap' is a device used to intercept telephone (or telegraph) communications."
- "A 'bug' is a device, often quite miniature in size, that can be hidden on a person or in a place that can transmit conversations in a room to a remote receiving device, where the conversation can be listened to."
- "A 'parabolic microphone' can pick up a conversation from a distance. Typically, a small dish behind the microphone enables the amplification of sound far away from the microphone itself."
Electronic Surveillance

- "The Court has in the past sustained instances of 'electronic eavesdropping' against constitutional challenge, when devices have been used to enable government agents to overhear conversations which would have been beyond the reach of the human ear. ... It has been insisted only that the electronic device not be planted by an unlawful physical invasion of a constitutionally protected area."
- **Lopez v. United States**
Katz v. United States

- Accused
  - Transmitting wagering information by telephone

- Manner Intercepted
  - Electronic listening and recording device attached to the outside of a public phone booth
Katz v. United States

• "[The Fourth] Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion. But the protection of a person's general right to privacy — his right to be let alone by other people — is, like the protection of his property and of his very life, left largely to the law of the individual States."
Katz v. United States

- “[T]he Fourth Amendment protects people — and not simply ‘areas’ — against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.”
Katz v. United States

• “‘Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes,’ and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment — subject only to a few specifically established and well-delineated exceptions…”
Katz v. United States

• “[F]irst that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’ Thus a man’s home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the ‘plain view’ of outsiders are not ‘protected’ because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.”
“Reasonable Expectation” or Privacy Test

1) A person must exhibit an actual (subjective) expectation of privacy and
2) The expectation must be one that society is prepared to recognize as “reasonable”.

22
Berger v. New York

• “The Fourth Amendment’s requirement that a warrant ‘particularly describ(e) the place to be searched, and the persons or things to be seized,’ repudiated these general warrants and ‘makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.’”
Berger v. New York

• “The purpose of the probable cause requirement of the Fourth Amendment [is] to keep the state out of constitutionally protected areas until it has reason to believe that a specific crime has been or is being committed…”
Misplaced Trust Doctrine

- “[P]eople place their trust in others at their own peril and must assume the risk of betrayal.”
Smith v. Maryland

• Accused
  – Victim robbed
  – Threatening phone calls made to victim and home drive byes
  – Traced license plate of car
  – Installed a pen register without a warrant
  – Searched accused home and uncovered additional evidence tying accused to robbery
Smith v. Maryland

• "[T]his Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action. This inquiry... normally embraces two discrete questions. The first is whether the individual, by his conduct, has 'exhibited an actual (subjective) expectation of privacy,' — whether... the individual has shown that 'he seeks to preserve [something] as private.' The second question is whether the individual's subjective expectation of privacy is one that society is prepared to recognize as 'reasonable,' — whether... the individual's expectation, viewed objectively, is 'justifiable' under the circumstances."
Smith v. Maryland

• "Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."

28
Smith v. Maryland

• “[E]ven if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not ‘one that society is prepared to recognize as ‘reasonable.’””
Pen Register and Trap and Trace Devices

- **Pen register** – records outgoing telephone calls
- **Trap and trace device** – records incoming telephone calls
Bank Records

• Bank must report every deposit, withdrawal, or other transfer of currency exceeding $10,000
• Transactions exceeding $5,000 into or out of the United States must also be reported
• 31 U.S.C. §1081
Privacy and the Mail

• 4th Amendment protects the contents of a sealed letter but not the outside
• The government can search letters sent from abroad
Items Exposed to the Public

• “The warrantless search and seizure of the garbage bags left at the curb outside the Greenwood house would violate the Fourth Amendment only if respondents manifested a subjective expectation of privacy in their garbage that society accepts as objectively reasonable. ... [W]e conclude that respondents exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection.”

• California v. Greenwood (1988)
Plain View Doctrine

• “[I]t has long been settled that objects falling in the plain view of an officer who has a right to be in the position to have that view are subject to seizure and may be introduced in evidence.”

Open Fields Doctrine

• “An individual does not have a reasonable expectation of privacy in the open fields that she owns.”

• “Under the curtilage doctrine, parts of one’s property immediately outside one’s home do not fall within the open fields rule. This exception does not mean that the curtilage is automatically afforded Fourth Amendment protection; a reasonable expectation of privacy analysis still must be performed.”
Fenced In Areas

- We recognized that the yard was within the curtilage of the house, that a fence shielded the yard from observation from the street, and that the occupant had a subjective expectation of privacy. We held, however, that such an expectation was not reasonable and not one ‘that society is prepared to honor.’ Our reasoning was that the home and its curtilage are not necessarily protected from inspection that involves no physical invasion. “‘What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.’”

Aerial Photographs

- But the photographs here are not so revealing of intimate details as to raise constitutional concerns. Although they undoubtedly give EPA more detailed information than naked-eye views, they remain limited to an outline of the facility’s buildings and equipment. ... We hold that the taking of aerial photographs of an industrial plant complex from navigable airspace is not a search prohibited by the Fourth Amendment. ..."
Warrantless Searches of Homes

• “With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no.”
Thermal Imager

• "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," [c] constitutes a search — at least where (as here) the technology in question is not in general public use. ...On the basis of this criterion, the information obtained by the thermal imager in this case was the product of a search."

• *Kyllo v. United States*, 533 U.S. 27 (2001)
United States v. Jones

- Issue
  - Use of GPS tracking device on a vehicle to monitor movements on public streets is a search or seizure within 4\(^{th}\) Amendment
United States v. Jones

• “We hold that the Government’s installation of a GPS device on a target’s vehicle, and its use of that device to monitor the vehicle’s movements, constitutes a ‘search.’”
Drug Sniffing Dogs

- “[T]he use of a **drug-sniffing dog** on a homeowner’s porch to investigate the contents of the home was a ‘**search**’ within the meaning of the Fourth Amendment.”
B. INFORMATION GATHERING ABOUT FIRST AMENDMENT ACTIVITIES
Seizure of Books

• “[T]he constitutional requirement that warrants must particularly describe the ‘things to be seized’ is to be accorded the most scrupulous exactitude when the ‘things’ are books, and the basis for their seizure is the ideas which they contain. No less a standard could be faithful to First Amendment freedoms.”

• Stanford v. Texas, 379 U.S. 476 (1965)
Privacy Protection Act

- The PPA prohibits government officials from searching or seizing work product materials or documents possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication. in or affecting interstate or foreign commerce.' However, if there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate,' then such materials may be searched or seized.
Gonzales v. Google

• Issue
  – Subpoena of Google for URL samples and all search engine queries for a two month time period
  – Narrowed twice to sample of 50K URLs
Gonzales v. Google

• “Given the broad definition of relevance in Rule 26, and the current narrow scope of the subpoena, despite the vagueness with which the Government has disclosed its study, the Court gives the Government the benefit of the doubt. The Court finds that 50,000 URLs randomly selected from Google’s data base for use in a scientific study of the effectiveness of filters is relevant to the issues in the case of ACLU v. Gonzales.”
Gonzales v. Google

- "What the Government has not demonstrated, however, is a substantial need for both the information contained in the sample of URLs and sample of search query text. Furthermore, even if the information requested is not a trade secret, a district court may in its discretion limit discovery on a finding that 'the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive.' Rule 26(b)(2)(i)."
Gonzales v. Google

• The court allows for the URL samples but not the search queries themselves...
C. FEDERAL ELECTRONIC SURVEILLANCE LAW
47 U.S. Code §605 - Unauthorized publication or use of communications

(a) Practices prohibited
Except as authorized by chapter 119, title 10, no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception,

(1) to any person other than the addressee, his agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination, (3) to proper accounting or distributing officers of the various communicating carriers over which the communication may be passed, (4) to the master of a ship under whom he is serving, (5) in response to a subpoena issued by a court of competent jurisdiction, or (6) on demand of other lawful authority.

No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. No person having received any intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of such communication (or any part thereof) knowing that such communication was intercepted, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of such communication (or any part thereof) or use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is transmitted by any station for the use of the general public, which relates to ships, aircraft, vehicles, or persons in distress, or which is transmitted by an amateur radio station operator or by a citizens band radio operator.
Applicability

- States could still use evidence in violation of §605 (while the Federal government could not)
- §605 only applied to wire communications and wiretapping and not eavesdropping on non-wire communications
Title III

• Applied to wiretaps by Federal and State officials
• Required Federal agents to apply for a warrant before wiretapping
• Criminalized private wiretapping
• No violation if one party consents
Electronic Communications Privacy Act (ECPA)

1) Wiretap Act
   - Communications in transmission

2) Stored Communication Act (SCA)
   - Communications in storage

3) Pen Register Act

Passed in 1986; amended Title III
4th Amendment?

• “Electronic surveillance law operates independently of the Fourth Amendment. Even if a search is reasonable under the Fourth Amendment, electronic surveillance law may bar the evidence. Even if a search is authorized by a judge under federal electronic surveillance law, the Fourth Amendment could still prohibit the wiretap.”
Communication
Classifications Under ECPA

• Wire Communications
• Oral Communications
• Electronic Communications
Wire Communications

- "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce
- 18 U.S. Code §2510(1)
Oral Communications

- "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication
- 18 U.S. Code §2510(2)
Electronic Communications

“electronic communication” means 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, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) any wire or oral communication;
(B) any communication made through a tone only paging device;
(C) any communication from a tracking device []; or
(D) electronic funds transfer information [];

18 U.S. Code §2510(12)
Not Protected by the Exclusionary Rule

• Electronic communications are not protected by the exclusionary rule in the Wiretap Act or the Stored Communications Act

• Wire or oral communications that fall within the Stored Communications Act
Wiretap Act

• Except as otherwise specifically provided in this chapter any person who—

• (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication,

• (b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—
  – (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication, or
  – (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or
  – (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; ...
Wiretap Act (cont’d)

- (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
- (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection...
- 18 U.S.C. §2511(1)
Exclusion/Penalty

- Can move to exclude wire or oral communications
- Violations of Wiretap Act - 10K per violation plus up to 5 years imprisonment
Exceptions

1) When one party to the communication consents

2) Communication service providers: to intercept, disclose, or use that communication in the normal course of [] employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service"
Stored Communications Act

(a) Offense.—Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

18 U.S.C. §2701
Exclusion/Penalty

- Cannot move to exclude wire or oral communications
- Violations of Stored Communications Act - 1K per violation plus up to 6 months of imprisonment
Pen Register Act

• “Subject to certain exceptions, ‘no person may install or use a pen register or a trap and trace device without first obtaining a court order.’”

• 18 U.S.C. §3121(a)
Pen Register

- the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business
- 18 U.S.C. §2137(3)
Exclusion/Penalty

• Cannot move to material from violations of Pen Register Act
• Violations of Pen Register Act – fined plus up to one year of imprisonment
CALEA/
Digital Telephony Act

- The Communications Assistance for Law Enforcement Act (CALEA) of 1994 a/k/a “Digital Telephony Act
- Requires telecomm providers to help facilitate the government in executing legally authorized surveillance
- Does not apply to email and Internet access; FCC declared applies to VOIP
USA Patriot Act

• Congress passed in response to 9/11
• Sweeping law expanding government’s surveillance powers
Delayed Notice of Search Warrants

• 4th Amendment – gov’t must obtain a search warrant and provide notice before conducting a search or seizure

• §3103(a) addition – “enabling the government to delay notice if the court concludes that there is ‘reasonable cause’ that immediate notice will create an ‘adverse result’ such as physical danger, the destruction of evidence, delayed trial, flight from prosecution, and other circumstances.”
Pen Registers

• “These changes altered the definition of a pen register from applying not only to telephone numbers but also to Internet addresses, e-mail addressing information (the ‘to’ and ‘from’ lines on e-mail), and the routing information of a wide spectrum of communications. The inclusion of ‘or process’ after ‘device’ enlarges the means by which such routing information can be intercepted beyond the use of a physical device. ... The person whose communications are subject to this order need not even be a criminal suspect; all that the government needs to certify is relevance to an investigation.”
State Electronic Surveillance Law

- 1 party consent or all party consent?
- First amendment issues?
Program
Completed