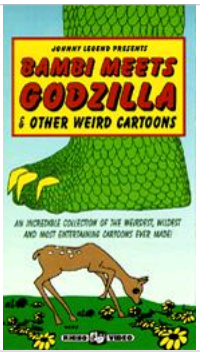
Privacy from Government

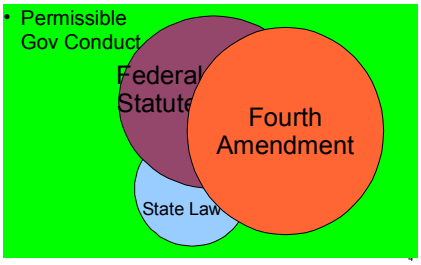
Reasonable Expectations of Privacy Meet Technologies of Surveillance



Sources of protection against surveillance

- Law
- Architecture/Technology
- Markets
- Norms

Sources of legal protection



Fourth 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.

flickr photo by Sarah to the G

Olmstead v. United States (1928)

- 1928: Olmstead was convicted of bootlegging, based on evidence from wiretaps.
- "The amendment does not forbid what was done here. There was no searching. There was no seizure."

Katz v. United States (1967)

- 1967: Katz is convicted for illegal bookmaking, based on wiretap evidence
- Supreme Court?

flickr photo by Sarah to the G

Katz v. United States (1967)

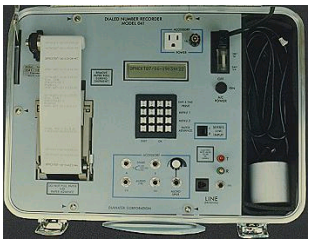
- [A] person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

Katz v. United States, Harlan concurrence

- [T]here is a twofold requirement, gfirst 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."

Smith v. Maryland (1979)

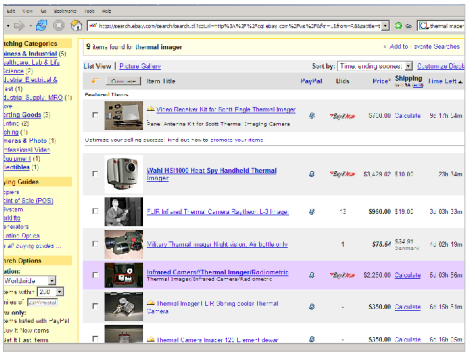
- "When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."



- Dianatek Pen Register: The Model 041 is connected to a telephone subscriber line and will capture, decode, display and print the dialed numbers on that circuit. It will also print the date and time of each call plus the call duration and necessary information regarding call progress to establish an acceptable determination of call completion. Every 12 hours a summary print is provided of incoming and outgoing calls by type and duration. The user can enter up to 10 dialable numbers for matching to trigger external accessory equipment for a timed duration. Matched numbers will also be flagged on the printout and summarized every 12 hours. All programming and parameter adjustments are done from the front panel. The instrument is complete with printer, LCD display and is housed in a polyethylene case. It has a carrying weight of about 15 pounds.

Kyllo v. United States (2001)

- "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,' constitutes a search–at least where (as here) the technology in question is not in general public use."



- Which of these is an email most like?

Which is an email most like?

- Unless encrypted, it travels through the 'Net like a postcard, visible to anyone stationed at any of the ISP "hops" along its route
- If most people don't realize this, is their "expectation of privacy" reasonable?
- Should we give *more* protection than the Fourth Amendment requires?

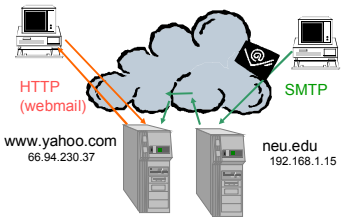
Sources of protection against surveillance

- Law
  - Fourth Amendment
  - Statute
    - Federal
    - State
- Code
- Markets
- Norms

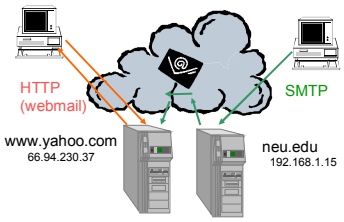
Statutory Protections, and their limits

- Wiretap Act (Omnibus Crime Control and Safe Streets Act of 1968)
- Electronic Communications Privacy Act (ECPA) of 1986
  - Wiretap Act, updated
  - Stored Communications Privacy Act
  - Pen Register / Trap and Trace
- USA PATRIOT Act, 2001

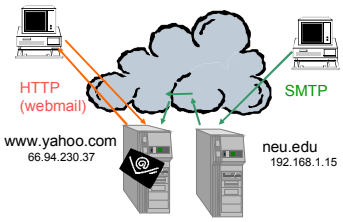
Email from alice@neu.edu to bob@yahoo.com



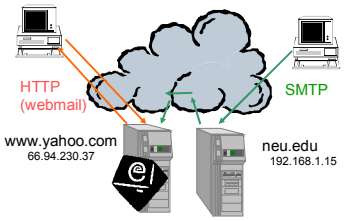
Email from alice@neu.edu to bob@yahoo.com



Email from alice@neu.edu to bob@yahoo.com



Email from alice@neuedu to bob@yahoo.com



claims:

- Privacy Protection Act
- Wiretap Act (ECPA Title I)
- Stored Communications Act (ECPA Title II)

Trial court ruled for plaintiffs

- Privacy Protection Act
- Stored Communications Act (ECPA Title II)

On appeal:

- Wiretap Act (ECPA Title I)
  - Interception?

requests	Real-time acquisition	Historical information
Contents of communications	Wiretap Act (super-warrant) or consent	Unopened: Warrant
		Opened: Subpoena with notice (poss. delayed)
Non-content-transactional or subscriber information	Pen register / trap-and-trace order (warrant-minus) or consent	Subscriber info: subpoena
		Transactional: 2703(d) "specific and articulable facts" order

Warrantless Wiretaps Telco Immunity?

- Foreign Intelligence Surveillance Act, additional authorizations for "foreign intelligence" surveillance, including emergency surveillance with 72-hour delayed warrant
- When government asks telcos to tap, can it get just foreign communications?
- Should the telcos be immunized from litigation (and discovery)?

U.S. v. Councilman

- Brad runs a bookstore, and on the side, offers email accounts to his customers. Sensing an opportunity for competitive advantage, Brad scans all the email for messages from "amazon.com" and copies them to his own account.
- Has Brad violated the Wiretap Act?

You're the Fed

- As a government lawyer, you're involved in a criminal investigation. Can you get the information? With what tool? What showing do you need?
  - The email addresses of a suspect's correspondents
  - The contents of a suspect's past emails to BigRed, a suspected co-conspirator
  - The time and date of the suspect's last ten Internet connections through ISP
  - The name of the Internet user BigRed@hotmail.com
  - Future emails the suspect might send to BigRed
  - Immediate alerts when the suspect logs on to ISP in the future

32

Procedural requirements on law enforcement

- Wiretap
  - "super warrant," probable cause +
  - "full and complete statement of the facts and circumstances relied on," and why less intrusive means failed or would fail
  - minimization
  - felony
  - authorization of high-level prosecutor
  - 30-day authorization, post-tap disclosure

33

Procedural requirements on law enforcement

- Stored communications (180 days or less)
  - Warrant, probable cause
- Stored communications (older than 180 days)
  - Notification to subscriber or warrant
- Re-stored communications?

34

Procedural requirements on law enforcement

- Pen Trap/Trace
  - Court order (probable cause -)
  - If government certifies that "information likely to be obtained by such installation and use is *relevant* to an ongoing investigation"
  - court "*shall* authorize installation and use of a pen register or a trap and trace device"

35

Wire and Electronic Communications

	In-flight interception	In "electronic storage" (temporary and intermediate, incidental to delivery)	In remote storage
Oral and wire communications, *contents*	"wiretap"; requires super-warrant; Exclusionary rule	Requires warrant (post-PATRIOT)	Requires subpoena with notice to subscriber
Electronic communications, *contents*	Requires super-warrant	Requires warrant	Requires subpoena with notice to subscriber
Dialing, routing, addressing, or signaling information, *Envelope* Subscriber records	Requires court order (court *shall* grant on certification of relevance) court order, including on relevance to authorized investigation to protect against international terrorism or clandestine intellegence activities		

36