Electronic Eavesdropping: Fourth Amendment, FISA, and NSA Surveillance

Alan Rubel
Assistant Professor
SLIS, Legal Studies
UW-Madison

Overview of Federal Privacy Law

- Fourth Amendment
  - Cases: *Olmstead*, *Katz*, *Miller*
- Privacy Act
- Electronic Communications Protection Act (FISA)
- Foreign Intelligence Surveillance Act (FISA)
- NSA Warrantless Surveillance

Fourth Amendment, U.S. Constitution

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.

Olmstead v. US (1928)

- Prohibition case
- Tap placed on phone lines outside Olmstead's office
- Supreme Court: not a search, and hence not a violation of Fourth Amendment

Katz v. U.S. (1967)

- Katz used a pay phone to transmit illegal bets across state lines.
- Recording device placed on the outside of the phone booth
- No trespass, no physical intrusion, no private property involved
- Supreme Court: Fourth Amendment protects people, not places.
- Sets forth "reasonable expectation of privacy" test for whether information gathering is a search.

Katz and *Olmstead*

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.

Katz and *Olmstead*

Fourth Amendment provides:

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.

U.S. v. Miller (1976)

- Distilling and selling unstamped whiskey
- Bureau of Alcohol, Tobacco, and Firearms subpoenaed Miller's bank records. Bank complied. Records were evidence of crime.
- Miller argued that this violated the Fourth Amendment.
- Supreme Court: Third party records not protected by Fourth Amendment. No reasonable expectation of privacy.

Smith v. Maryland (1979)

- Smith robbed McDonough.
- Afterward, Smith called McDonough repeatedly. During one call, McDonough saw the same suspicious car and got license information.
- Police traced that information to Smith, and got the phone company to place a pen register at its offices to capture numbers dialed from Smith's phone.

Smith v. Maryland (1979)

- Supreme Court: No reasonable expectation in privacy in numbers dialed:
  - Third party has information.
  - Must know third party has information, because its needed for system to work.
  - Notice placed in phone book.
  - Information only transactional, not content.

U.S. v. U.S. District Court (1972)

Supreme Court allowed that there may be different Fourth Amendment standards for national security surveillance

Foreign Intelligence Surveillance Act (FISA) (1978)

- Establishes standards for electronic surveillance to collect “foreign intelligence.”
- Exclusive authority for foreign intelligence surveillance “except as authorized by statute.”
- Prior to 2001, FISA applied only where foreign intelligence was “primary purpose” of surveillance.
- Post-2001, applies where foreign intelligence is “a significant purpose” of surveillance.

FISA

Provides for electronic surveillance **without a court order**, if authorized by U.S. Attorney General, if:

1. Targets foreign powers or their agents,
2. No substantial likelihood that surveillance will acquire contents of communication to which U.S. person is a party,
3. AG certifies (1) and (2) obtain, and
4. AG reports on compliance to Congress

FISA

Allows electronic surveillance **with a court order** if approved by FISA court. Court may approve surveillance with:

1. Probable cause that target is foreign power or agent thereof,
2. Places surveilled is, or will be, used by that power or agent, and
3. Surveillance minimizes collection of information of U.S. persons.

NSA Electronic Surveillance Program

NSA Electronic Surveillance Program

- National Security Agency began surveillance program in late 2001, in response to 9/11 attacks.
- In 2005-06, news agencies reported (confirmed by various sources, including members of Congress) that the surveillance included wholesale copies of phone and communications records of U.S. citizens.

NSA Electronic Surveillance Program

- Such surveillance was performed with the help of telecom companies, specifically AT&T
- Documents leaked by AT&T employee show installation of fiberoptic splitter at San Francisco offices that allows copying all internet traffic.
- Copying of traffic is not limited to any particular group (hence, both foreign and domestic persons' communications).

Administration Position

- FISA contains a provision that electronic surveillance is impermissible "except as authorized by statute“
- The Authorization for Use of Military Force Against Terrorists passed immediately after 9/11 provides such an authorizing statute.

AUMF

Allows president to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons."

Constitutional Argument

FISA precludes NSA electronic surveillance program. However, FISA is an unconstitutional limitation on Congressional and Executive power.