

Technology and 4th Amendment

CIS 381

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.

Background

- The Fourth Amendment specifically mentions "houses" as a place where person have a right "to be secure against unreasonable searches and seizures."
- Most interesting, perhaps, are cases in which courts have considered arguments that an activity that may be criminally punished outside the home is nonetheless protected when it occurs inside a home.

• <http://www.law.umkc.edu/faculty/projects/frisks/contlaw/homescastle.htm>

- Possession of obscene material inside a home
- ***Stanley v Georgia*** (1969) the Supreme Court found that the private possession of obscene material inside a home was constitutionally protected, even though states were free to punish the sale and distribution of those materials.

- Two persons of the same sex to engage in certain intimate sexual conduct.
- ***Lawrence and Gardner v Texas*** (2003) "Whatever may be the justifications for other statutes regulating obscenity, we do not think they reach into the privacy of one's own home. If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds."

<http://www.law.mskc.edu/faculty/projects/trials/condaw/lawrencevtexas.html>

- Use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a "search"
- ***KYLLO v UNITED STATES*** (2001) "At the very core" of the Fourth Amendment "stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no.

<http://www.law.mskc.edu/faculty/projects/trials/condaw/lawrencevtexas.html>

- Use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a "search"
- **KYLLO v UNITED STATES (2001)** "At the very core" of the Fourth Amendment "stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no.

<http://www.law.umkc.edu/faculty/projects/ftribals/condaw/lawrencevtxas.html>

Wiretaps

- Wiretapping, electronic eavesdropping, hidden videotaping, and even more complex means of gathering evidence are often used in criminal investigations. As technology has improved, so have the tools of police work. The Framers of the Constitution could hardly have anticipated these technological advances two centuries ago when they wrote the Bill of Rights. Determining how the principles they laid down should be applied to new problems generated by technology is a duty that has fallen to the courts.

http://www.phschool.com/school/supreme_court_cases/olmstead.html

Olmstead Case

- State and federal law enforcement agents conducted an investigation of a Seattle-based bootlegging operation which smuggled alcoholic beverages into the United States over the Canadian border a hundred miles away. Olmstead was engaged in the illegal sale of these goods, prohibited by the Volstead Act. Much of the case against Olmstead was based on information gathered by a wiretap on his home telephone, placed without prior issue of a warrant on the telephone lines outside. Olmstead was arrested and convicted of violations of the Volstead Act.

Olmstead v United States (1928)

- **Olmstead’s Fourth Amendment challenge was doomed by the absence of “an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house or curtilage for the purposes of making a seizure.”**

<http://www.epic.org/privacy/wiretap/98-326.pdf>

1934 Communications Act

- **Federal Communications Act outlawed wiretapping, but it said nothing about the use of machines to surreptitiously record and transmit face to face conversations. In the absence of a statutory ban the number of surreptitious recording cases decided on Fourth Amendment grounds surged.**

- **The use of a dictaphone to secretly overhear a private conversation in an adjacent office offended no Fourth Amendment precipes because no physical trespass into the office in which the conversation took place had occurred, Goldman v. United States (1942).**
- **The absence of a physical trespass precluded Fourth Amendment coverage of the situation where a federal agent secretly recorded his conversation with a defendant held in a commercial laundry in an area open to the public, On Lee v. United States (1952).**

- Fourth Amendment did reach the government's physical intrusion upon private property during an investigation, as for example when they drove a "spike mike" into the common wall of a row house until it made contact with a heating duct for the home in which the conversation occurred, *Silverman v. United States* (1961).
- Furthermore, the Fourth Amendment may protect against the overhearing of verbal statements as well as against the more traditional seizure of papers and effects.

Open Fields

- The open fields doctrine was first articulated by the U.S. Supreme Court in *Hester v. United States* (1924), which stated that "the special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers, and effects,' is not extended to the open fields."
- This opinion appears to be decided on the basis that "open fields are not a "constitutionally protected area" because they cannot be construed as "persons, houses, papers, [or] effects."
- While open fields are not protected by the Fourth Amendment, the curtilage, or outdoor area immediately surrounding the home, is. Courts have treated this area as an extension of the house and as such subject to all the privacy protections afforded a person's home (unlike a person's open fields) under the Fourth Amendment.

http://en.wikipedia.org/wiki/Reasonable_expectation_of_privacy

Plain View Doctrine

- Able to seize items in plain view as long as three requirements are met (sometimes four)
- All three requirements must be present
- If one or more requirements is missing then not plain view

http://www.amt.edu/cjus/Course_Pages/CJUS_4200/Chapter%209.ppt

Plain View Doctrine Requirements

- # 1 – Item must be seen by the officer
- # 2 – Officer must be legally present in the place from which the item is seen
- The officer must not have done anything illegal to get to the spot from which the items are seen

Plain View Doctrine Requirements

- # 3 – Must be “immediately apparent” that the item is subject to seizure
- Recognition must be immediate and not the result of further prying or examination
- Example – cant suspect item is stolen and get serial number to verify (justify by other means, consent or p/c and exigent circumstances)

Katz v United States (1967)

1. The Government's eavesdropping activities violated the privacy upon which petitioner justifiably relied while using the telephone booth and thus constituted a "search and seizure" within the meaning of the Fourth Amendment.
 - (a) The Fourth Amendment governs not only the seizure of tangible items but extends as well to the recording of oral statements.
 - (b) Because the Fourth Amendment protects people rather than places, its reach cannot turn on the presence or absence of a physical intrusion into any given enclosure.
2. Although the surveillance in this case may have been so narrowly circumscribed that it could constitutionally have been authorized in advance, it was not in fact conducted pursuant to the warrant procedure which is a constitutional precondition of such electronic surveillance.

<http://www.flylib.com/scripts/getcase.pl?lib=ty-CASE&case=1-USA-vb-398&page=347>

Katz

- **Established a two-part test for what constitutes a search within the meaning of the Fourth Amendment.**
- **The relevant criteria are**
 - "first 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."
- **Under this "new" analysis of the Fourth Amendment, privacy expectations deemed unreasonable by society cannot be validated by any steps taken by the defendant to shield the area from view.**

http://en.wikipedia.org/wiki/Open_fields_doctrine

Title III of the Omnibus Crime Control and Safe Streets Act of 1968

- **A comprehensive wiretapping and electronic eavesdropping statute that not only outlawed both in general terms but that permitted federal and state law enforcement officers to use them under strict limitations designed to meet the objections in *Berger v New York* (1967).**

<http://www.epic.org/privacy/wiretap/98-326.pdf>

United States v. United States District Court (1972)

- **Court held that the President's inherent powers were insufficient to excuse warrantless electronic eavesdropping on purely domestic threats to national security.**

<http://www.epic.org/privacy/wiretap/98-326.pdf>

FISA 1978

- The Act provides a procedure for judicial review and authorization or denial of wiretapping and other forms of electronic eavesdropping for purposes of foreign intelligence gathering.

<http://www.epic.org/privacy/wiretap/98-326.pdf>

Electronic Communications Privacy Act (1986)

- The Act sought to strike a balance between the interests of privacy and law enforcement, but it also reflected a Congressional desire to avoid unnecessarily crippling infant industries in the fields of advanced communications technology.
- The Act also included new protection and law enforcement access provisions for stored wire and electronic communications and transactional records access (email and phone records), and for pen registers as well as trap and trace devices (devices for recording the calls placed to or from a particular telephone).

<http://www.epic.org/privacy/wiretap/98-326.pdf>

Carnivore

- **Carnivore** is a name given to a system implemented by the **FBI** that is analogous to **wiretapping** except in this case, **e-mail** and other **communications** are being tapped instead of **telephone** conversations. Carnivore was essentially a customizable **packet sniffer** that could monitor all of a target user's **Internet** traffic.
- USG personnel are required to get a **warrant** or court order naming specific people or email addresses that may be monitored. When an email passes through that matches the filtering criteria mandated by the warrant, the message is logged along with information on the date, time, origin and destination. This logging is most likely relayed in real time to the FBI but the details are not currently known. All other traffic would presumably be dropped without logging or capture.
- As of the middle of January 2005, that the FBI has essentially abandoned the use of Carnivore in 2001, in favor of commercially available software. [http://en.wikipedia.org/wiki/Carnivore_\(FBI\)](http://en.wikipedia.org/wiki/Carnivore_(FBI))

Echelon

- **ECHELON** is a name used to describe a highly secretive world-wide **signals intelligence** and analysis network run by the **UKUSA Community** that has been reported by a number of sources including, in 2001, a committee of the **European Parliament**. According to some sources ECHELON can capture **radio** and **satellite** communications, **telephone** calls, **faxes**, **e-mails** and other data streams nearly anywhere in the world and includes computer automated analysis and sorting of intercepts.
- Reportedly created to monitor the military and diplomatic communications of the **Soviet Union** and its **East Bloc** allies during the **Cold War** in the early sixties, today ECHELON is believed to search also for hints of **terrorist** plots, drug-dealers' plans, and political and diplomatic intelligence. But some critics, including the **European Union**, claim the system is being used also for large-scale commercial theft and invasion of **privacy**.

<http://en.wikipedia.org/wiki/ECHELON>

Controversy

- US intelligence agencies are generally prohibited from spying on people inside the US, and other Western countries' intelligence services generally faced similar restrictions within their own countries. There are allegations, however, that ECHELON and the **UKUSA** alliance were used to circumvent these restrictions by, for example, having the UK facilities spy on people inside the US and the US facilities spy on people in the UK, with the agencies exchanging data. The **NSA** states on its **SIGINT** FAQ web page "We have been prohibited by executive order since 1978 from having any person or government agency, whether foreign or U.S., conduct any activity on our behalf that we are prohibited from conducting ourselves. Therefore, NSA/CSS does not ask its allies to conduct such activities on its behalf nor does NSA/CSS do so on behalf of its allies."

<http://en.wikipedia.org/wiki/ECHELON>
