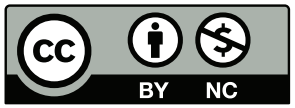
Wiretapping and Surveillance



The 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."

Important Clauses

persons. . . effects

Does this only apply to tangible items, or to information?

unreasonable

What is “reasonble”? In particular, when do people have a “reasonable expectation of privacy”?

probable cause

How much suspicion is needed?

particularly describing

How much specificity is needed?

Wiretaps: Katz v. United States (1967)

- Held that wiretaps are searches within the meaning of the Fourth Amendment
- Thus, a search warrant is required
- People talking on the phone in an enclosed space (home, office, phone booth — and they were generally enclosed in 1967) have a *reasonable expectation of privacy*
- (Amusingly, phone calls in an “open field” arguably were not protected, since cell phones weren’t conceivable in 1967. . .)

Structual Points in the *Katz* Opinion

- It contains a *syllabus*, the *opinion* of the court, three *concurring opinions*, one *dissenting opinion*
- The syllabus (headnote) — which is an interpretation, but *not* legally binding — explains the main points
- (That principle is itself specified in a Court opinion, in *United States v. Detroit Timber and Lumber Co.*, 200 U.S. 321 (1906)!)
- Only the court's opinion sets precedent
- The concurring and dissenting opinions explain viewpoints and give hints about future interpretations
- Note the use of page numbers within the opinion: e.g., "*Olmstead v. United States*, 277 U.S. 438, 457, 464, 466"

Court Practice

- Previous decision (*Olmstead*) completely overruled — unusual

☞ "We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling."

☞ (The Court took the same sort of controversial action recently in *Citizens United v. Federal Election Commission*.)

- The Court's ruling went further than even the appellant asked them to — also unusual
- Some subjects were explicitly described as out of scope: "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case." (Footnote 23)

☞ (Very unusually, the Court did not limit *Citizens United* that way.)

Effects of the Court's Ruling

- Until 1967, interception was regulated only by the *Communications Act*; no warrants were required
- Congress responded by passing the *Wiretap Act*, more formally known as *Title III* of the *Omnibus Safe Streets and Crime Control Act of 1968*
- This was amended in 1986 by the *Electronic Communications Privacy Act* (ECPA) to include data communications; see *18 USC 2510 et seq.* and *18 USC 2711 et seq.*
- Many subsequent amendments, especially the post-9/11 *PATRIOT Act*
- The law imposes more restrictions on law enforcement than are constitutionally required

Information, not Objects

- For our purposes, the Court's most important holding is that "the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements."
- The same constitutional principle would apply to data communications: a search warrant is necessary
- This requirement is independent of the ECPA

What is an “Unreasonable Search”?

- Some searches are “reasonable” and don’t require a warrant (i.e., patting down someone you’ve just arrested to see if he or she has a weapon)
- “A search occurs when the government infringes an expectation of privacy that society is prepared to consider reasonable.” *United States v. Jacobsen*, 466 U.S. 109 (1984).
- Cordless phones, 1992: “The significant difference between land line telephone conversations and conversations carried out over early versions of the cordless phone was the ease with which cordless phone conversations could be intercepted. It was so easy to overhear early cordless phone conversations that a user could never have a reasonable expectation of privacy.” (978 F.2d 171).
- What about WiFi?

WiFI

- Very commonly used — and almost all WiFi devices can trivially intercept other traffic
- *18 USC 2511(2)(g)(i)*: “It shall not be unlawful under this chapter or chapter 121 of this title for any person . . . to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public” (see definition at *18 USC 2510(14)*.)
- *18 USC 2511(2)(g)(v)*: “for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.”
- But what about WEP?

Wired Equivalent Privacy (WEP)

- All WiFi devices support WEP encryption — but WEP was a botched design from the very beginning and is trivially cracked
- Is its encryption strong enough to trigger the last clause of 2511(2)(g)(v)?
- In most common deployments, all users of a WEP-protected net share the same WEP key, so no cryptanalysis is necessary
- Is there a “reasonable expectation of privacy” under the Fourth Amendment? I suspect not.
- Do police need a search warrant to monitor WiFI? Not if there is no expectation of privacy. Does the answer change if WEP is used? No.
- But — they usually get an answer anyway, both to protect their case and to prevent adverse court rulings that would keep them from going after someone else doing it maliciously.

What About Voice over IP (VoIP)?

- Skype, voice iChat, and many conventional-seeming phones use VoIP. If one does VoIP over WiFi, what is its status?
- That's *very* complicated, since it involves the precise definitions in *18 USC 2510*. "Electronic communication" includes sounds but not "wire or oral communication".
- "Wire" sometimes includes voice; ditto "oral". However, other restrictions apply. . .
- An "electronic communication system" covers electronic and wire communications. . .
- Where does that leave VoIP?

☞ The technology has outpaced the law

Pen Registers: *Smith v. Maryland* (1979)

- Held that *pen registers* are not searches within the meaning of the Fourth Amendment, and hence don't require search warrants
- A pen register is a device for recording what numbers you dial. A *trap and trace* device records who dialed you
- Smith probably had no expectation of privacy and certainly no "legitimate expectation of privacy"

Why the Difference From *Katz*?

- Calling a number requires “giving” the number to the phone company
- ☞ People know this because of e.g., itemized bills
- Callers should not expect privacy
- ☞ If they do, it is not a “reasonable” expectation
- The information is being obtained from the phone company, not the individual
- ☞ Individuals have no expectation of privacy in information “voluntarily” given to a third party

What I Haven't Discussed

- The Foreign Intelligence Surveillance Act (FISA), *50 USC 1800*
- Stored Wire and Electronic Communications and Transactional Records Access, *18 USC 2701*

Pen Register Law

- *18 USC 3127* defines a pen register as “a device or process which records or decodes dialing, routing, addressing, or signaling information”
- They may be installed if “the information likely to be obtained is relevant to an ongoing criminal investigation”
- Very low threshold — no “probable cause” requirement

How Does All This Apply to Computers?

- The law was originally written for telephones
- Computer technology presents unique challenges
- There is also greater potential for abuse

Packets on the Internet

- Messages on the Internet are divided into *packets*
- Each packet has a *source* and *destination IP address*
- Packets are transmitted independently via *routers* to their destination
- Packet delivery may be unreliable; routers can delete, modify, duplicate, reorder, delay, etc., packets; it is up to end systems to assure that everything is received exactly once
- Packets often contain *port numbers*. Port numbers are (more or less) service identifiers; the web, for example, is usually on port 80

Addresses and Media

- IP addresses reflect the topology of the network — most sites get their blocks of IP addresses from their ISP.
- In turn, they hand out addresses locally to reflect the local physical networks: Ethernets, WiFi networks, etc.
- Most client machines aquire addresses dynamically, for a limited-period “lease”; the next day, they may have a different IP address
- Addresses are assigned based on userid, computer name, or computer hardware (“MAC”) address
- Most interesting media are shared amongst many computers; a tap is generally picking up lots of traffic
- How are wiretaps and pen register intercepts performed? What are the limits? What do some things mean?

What Does it Take to Wiretap my WiFi?

- CU has no WiFi logins, so there's no userid.
- MAC addresses and computer names can be hard to learn
- Worse yet, they're easy to change
- Suppose the (authorized) wiretapper does learn them. The wiretap device then has to listen to the IP address leasing protocol to learn my IP address, to start tapping it
- Then I relinquish my lease, change my MAC address, and start over. . .
- You, meanwhile, will tap someone else's traffic

What Can an Internet Pen Register *Legally* Learn?

- Clearly, it can learn the destination IP address; you “give” that to your ISP, and hence have no privacy interest in it
- What about emails? URLs? To whom do you “give” those?
- The answers aren’t simple

Email Handling

- At Columbia (or with most ISPs), the user's email client (the "MUA") transmits a list of recipients and the body of the email to a university mail server
- This mail server then contacts the recipients' email servers and sends the message
- The recipient's MUA contacts its mail server and retrieves the message
- What is the "dialing, routing, addressing, or signaling information"? Who has a reasonable privacy expectation in it?

Email Pen Registers

- You have to give the university the recipients' addresses, so you have no privacy expectation in them, per *Smith*
- The receiving mail server knows the sender's email address; it's an inherent part of the protocol
- The **`Subject:`** line is part of the body, and is not "given" to any other party, and hence is content, not addressing
- Header lines in the body can disagree with the "envelope" lines — but they're private, too

Email Dialog

```
220 machshav.com ESMTP Postfix
MAIL FROM:<smb@cs.columbia.edu>
250 2.1.0 Ok
RCPT TO:<smb2132@columbia.edu>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: Steve Bellovin <smb@cs.columbia.edu>
To: Steve Bellovin (UNI) <smb2132@columbia.edu>, bollinger@columbi
Subject: test

This is a test
.
250 2.0.0 Ok: queued as 9258B52D5DA
quit
221 2.0.0 Bye
```

It's More Complicated Than That

- I personally own a mail server
- So does a friend of mine
- When I email my friend, there are no third parties to whom address information is given
- But the only way to determine this is to intercept and analyze the data first
- The pen register can't decide if it can constitutionally look at traffic until after it has looked at it. . .

What About URLs?

- To whom is a URL given? Is some of it content?
- For most — but not all — users, URLs are end-to-end; nothing is given to the ISP except the IP address of the web server
- But — sometimes, multiple web servers share a single IP address. Is the **`Host:`** parameter content or addressing?
- Also, if a web proxy is used, there is a third party.
- What if there is a “transparent” proxy, unknown to the user?
- Are users as aware of these details as they are of the telephone company recording phone numbers?
- In a URL like `http://www.google.com/#q=bellovin` the `#q=bellovin` is *content* — but no higher court has ruled on that

When is Privacy Violated?

- In *Smith*, the Court wrote "Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate."
- But other courts have held that "The fact that a computer scans millions of e-mails for signs of pornography or a virus does not invade an individual's content-based privacy interest in the e-mails and has little bearing on his expectation of privacy in the content." (Warshak v. United States, 490 F.3d 455 (6th Cir. 2006), later overruled.)
- Does the presence of a human make a difference? If so, when?

More Issues

- Computerized text can be scanned much more easily than voice traffic
- Is a warrant for some offending packets, independent of IP address, legal? Probably not — remember the “particularly describing” clause.
- There is, however, significantly greater potential for abuse because it’s so easy to pick up too much with shared media

Conclusions

- The existing legal framework is poorly suited to the Internet
- Technology changes far more rapidly than legislators and judges can adapt
- What do we do?