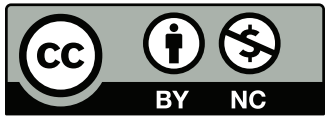
Legal Aspects of Privacy



Ownership of Data

- Who owns data?
- More precisely, who owns data about *individuals*?
- Who regulates it?
- Legally, this matters

American Attitudes

- Traditional American attitude: data belongs to the *compiler* of the data
- When you buy something and a store records it, the store owns the *record*
- Note: not the *fact* of the purchase, but the record of it
- But you own your image, though probably not the copyright on any pictures of you

More American Attitudes

- Free speech is a core value
- Recording and publishing of *truthful* information is acceptable
- No preemptive regulation of “speech”

Consequences

- Compiling and using data is accepted — the database is the property of the compiler
- As with other forms of property, it can be used, sold, etc., with few regulations
- Restrictions have been imposed after abuses

Example: Video Rental Records

"A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person." (18 USC 2710(b)(1))

But: "however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer" (18 USC 2710(b)(2)(D)(ii) — but there is an opt-out provision)

Passed after a reporter obtained Judge Robert Bork's rental records, looking for evidence that he was viewing porn

Privacy Laws in America

- Very few, and mostly sector-specific
- A very strong law: HIPAA, which protects medical information
- Credit records: primary issue is correctness (FCRA)
- FERPA: protects school records

HIPAA

- Intended to provide strong protections on disclosure
- But — given health payment system, doctors must disclose sensitive patient information to insurance companies
- Result: you're always asked to sign waivers
- Also — HIPAA applies to providers and insurance companies, not to third-party record providers like Apple and Microsoft

Electronic Health Records

- Promise: single database of all of your health information
- Available to all doctors, everywhere
- Who will have authorized access?
- ☞ The information is far more detailed than the MIB's data
- Who will have the ability to abuse authorized access?
- What are celebrity health records worth to the tabloids? What are your records worth to a snoopy neighbor?

But. . .

- Statistical information valuable to researchers
- Completeness and availability of records is a major health issue
- Very useful in case of emergencies
- Very useful when people switch doctors
- What about mentally incompetent patients?
- Single nationwide system currently stalled by cost and usability issues, as well as privacy concerns

Credit Records

- The credit bureaus own the information they collect about you
- You do not—and, at least in the past, were considered to have no interest in those records
- Why FCRA?
- You could be harmed by an error

☞ More like a tort issue

- In a world of identity theft, should the FCRA be amended to require confidentiality as well?

You Don't Own Your Records

- The data is *about* you—but is *owned* by the credit bureaus
- That's why consumers have no recourse against Equifax—*their* property wasn't stolen, Equifax's was
- But consumers are harmed by the disclosure

Privacy and the Government

- Americans do not trust the government
- More restrictions on what the government can do, both in general and with data
- Major restriction: *Privacy Act* — establishes Fair Information Principles for the government
- Note well: does *not* apply to the private sector

The Privacy Act of 1974

- Individuals have the right to access and correct their records
- Records (generally) cannot be disclosed without consent
- Agencies must have legal authority to collect such data
- Agencies must publish *SORNs* (System of Records Notices)
- Agencies must carry out *PIAs* (Privacy Impact Assessments)

PIAs

- Nominally, honest descriptions of the privacy impact of a system
- (Can be partly or completely classified, for classified programs)
- Might be controversial. Example: DHS asserts that IP addresses are not personally identifiable information. The EU disagrees. Who's right?

The Private Sector

- Those rules do not apply to the private sector
- As noted, companies can generally do what they want with their data
- This is sometimes explicitly enshrined in the law

Phone Company Records

"A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications . . . (6) to any person other than a governmental entity." (18 USC 2702(c))

That's right – phone companies and ISPs can sell your calling habits to anyone not in the government. (Effectively repealed in 1996, but not for privacy reasons.)

Can the government purchase such records from some third party? Yes. . .

More Casual Attitudes?

- Mark Zuckerberg of Facebook:

  "And then in the last 5 or 6 years, blogging has taken off in a huge way and all these different services that have people sharing all this information. People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.

  "We view it as our role in the system to constantly be innovating and be updating what our system is to reflect what the current social norms are."

- Or—all other social networks
- Abuse? Or reflection of societal change?

Government Abuses

- Government database systems are run by fallible, corruptible human beings
- Every few years, some IRS employees are caught looking at celebrity tax returns
- During the 2008 presidential campaign, some people looked at candidates' passport applications
- Regular scandals involving abuse of law enforcement databases
- During the Nixon administration, the White House sought access to tax records of political enemies
- Trump?

Outside the US

- Privacy laws outside the US are generally much stronger
- The EU and Canada have privacy laws that implement a variety of protections, including use limitations and restrictions on overcollecting
- In many countries, certain databases even need to be registered with a government privacy office

But. . .

- Many such databases are useful to law enforcement, especially for anti-terrorism investigations
- Especially useful: communications records
- EU law: data retention directive
- Requires phone companies and ISPs to retain records (including URL accesses) for 1-2 years

☞ Struck down by the European Court of Justice

- The FBI wants a similar law here. . .

International Issues

- With the Internet, offshore processing of data is very easy
- What if the receiving country has laxer data protection laws or practices?
- The TSA wants lots of information on EU airline passengers — but it's normally illegal to export that data from the EU to the US

Privacy Law in the EU

- Original version: the Data Protection Directive (1995)
- In essence, enacted the Fair Information Processing Principles
- Not uniform in EU member states
- Effectively pre-Internet and pre-smartphone
- Being replaced by the General Data Protection Regulation (effective May 2018)

The GDPR

- A *regulation*, not a *directive*—and therefore legally binding throughout the EU
- Modernizes the rules:
  - Stronger rules for obtaining consent
  - Decisions by automated systems can be contested
  - Data impact assessments often required
  - Pseudonymization encouraged—but pseudonymized data is still protected
  - Privacy by design
  - Restrictions on data export from the EU
- Companies are worried about the conversion to the new legal regimen

The Right to be Forgotten

- In a Spanish court case (Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014)), Google was required to delete links to old, derogatory information about someone
- The information held elsewhere wasn't deleted; just Google's links to it
- Balances the right to privacy with the right to free expression

☞ Would not apply to information about public figures

- Newer court cases have held that this order applies to all of Google's sites around the world, not just within the EU

What is Wiretapping?

Photo from Wikimedia Commons

- We all know what wiretapping is—some police officer with a *buttset* uses alligator clips to listen in on a phone line
- Higher-end wiretappers use tape recorders
- More or less this is actually done

Loop Extenders

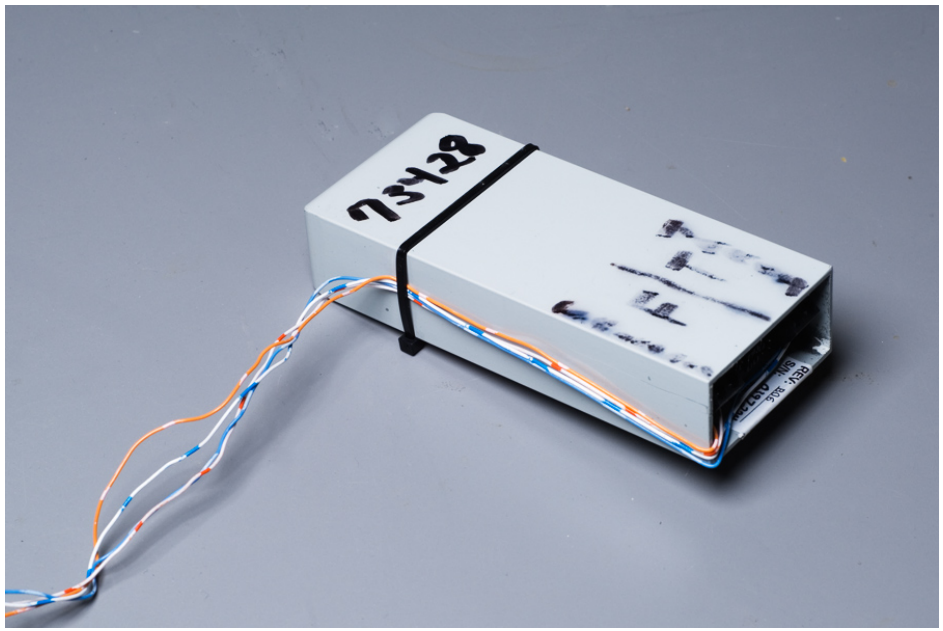


Photo © Matt Blaze; used by permission

- Attach one set of wires to the target's line.
- Attach the other set to an unused "friendly pair" to run the signal back to the central office.
- Listen in from the comfort of an office environment—no more cold vans. . .

What is Picked Up?

- Butt sets and tape recorders pick up sounds
- The numbers you dial are sounds
- If you have CallerID, the calling number is also a set of sounds

Pen Registers: What Numbers Did You Dial?

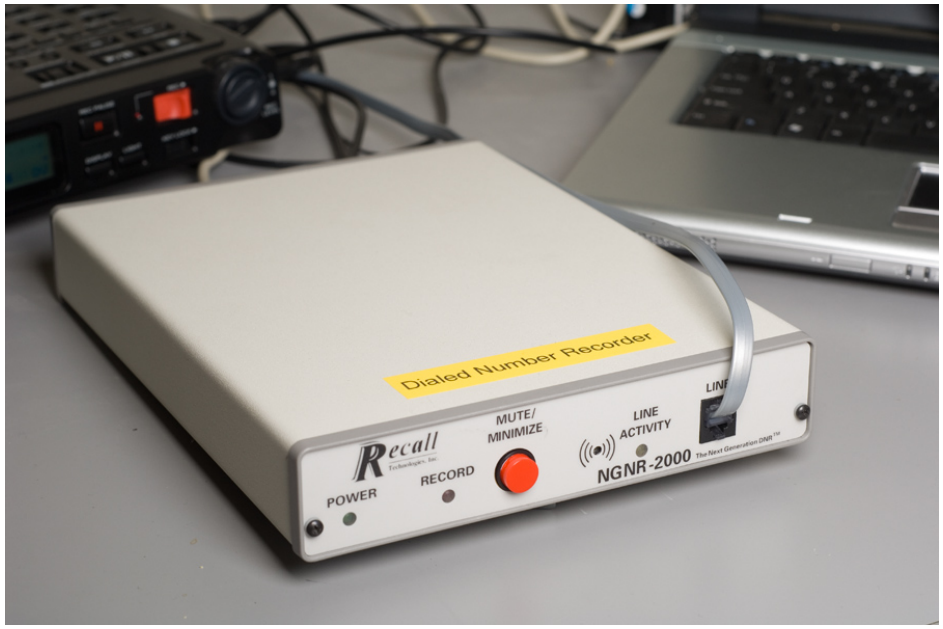


Photo © Matt Blaze; used by permission

- Note the phone jack on the front—it's designed to plug in to a standard phone line
- It just listens to dialing tones and records them
- The "minimize" button suggests that it's part of a general wiretap setup. "Minimize"?

Legal Distinctions

- Not all telephone “sounds” are treated the same way
- Who is the target of the wiretap?
- To whom are the sounds sent?

Why?

- Searches in the US are regulated by the Fourth Amendment to the US constitution
- (Is a wiretap legally a "search"? It is now—but before 1967, it wasn't considered one: see *Olmstead v. United States*, 277 U.S. 438 (1928))
- The Fourth Amendment bars "unreasonable searches"
- A warrant must "particularly describing the place to be searched, and the persons or things to be seized"
- Warrants require "probable cause"; mere suspicion isn't enough
- Instantiated by the Wiretap Act; separate procedures in the Foreign Intelligence Surveillance Act

FISA: The Foreign Intelligence Surveillance Act

- For purely criminal cases, a warrant or other court order is necessary for wiretapping, getting metadata, etc.
- For foreign intelligence operations, it's considered a military function, under direction of the Commander-in-Chief; no warrants are needed
- But what about a foreign intelligence operation *within the US*? In particular, what about NSA collecting information about a "US person"?
- That is governed by FISA. A special (and secretive) court can issue FISA warrants permitting such activities

Content/Non-content

- Legal principle: if you voluntarily give information to a third party, you no longer have a “reasonable expectation of privacy” in it
- To make a phone call, you tell the phone company what number you’re calling
- You have therefore voluntarily shared it, so no warrant is required
- Legally, this is *non-content*

Metadata

- Metadata is the set of non-content information associated with a call
- For telephony, at a minimum that is the calling number, the called number, and the call duration
- Often, much more is revealed

Internet Metadata

- IP addresses?
- TCP port numbers?
- Email addresses?
- URLs? Parts of URLs?
- It would take another full lecture to explain, but the answers are very complicated

The Importance of Metadata

- It is very hard to hide metadata
- You can encrypt the call—but the phone company *must* know the number you're calling
- Metadata is very revealing

The EFF's Examples

- They know you rang a phone sex service at 2:24 am and spoke for 18 minutes.
- They know you called the suicide prevention hotline from the Golden Gate Bridge.
- They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour.
- They know you received a call from the local NRA office while it was having a campaign against gun legislation, and then called your senators and congressional representatives immediately after.
- They know you called a gynecologist, spoke for a half hour, and then called the local Planned Parenthood's number later that day.

(From `https://www.eff.org/deeplinks/2013/06/why-metadata-matters`)

Traffic Analysis

- A person from a suspicious country has a pattern: a short Skype call at the same time every week
- One week, there's a long call
- The next week, there's nothing. . .
- An agent checking in, a planning call, then the plan is in motion?
- Or a student hearing from home, learning of an illness, and then hurriedly returning?

Contact Chaining

- Police are monitoring Alice, a known criminal
- Suppose Alice calls Bob.
- ☞ The metadata shows the association between them
- Now Bob calls Carol
- ☞ There is thus an indirect link between Alice and Carol
- Is she implicated?
- To do this, you need a good database of call records

Section 215

- Section 215 of the PATRIOT Act authorized access to "business records" for terrorism investigations
- The FISA court issued a (secret) order permitting bulk collection: metadata for all calls, from all carriers
- Note well: this did not include content. Also remember that under the law, metadata is only very lightly protected
- Members of the House and Senate Intelligence Committees knew that §215 was being used that way, but that was classified; most people did not know. Some Senators did warn that controversial things were happening.
- Struck down by the Second Circuit; repealed by Congress before the Supreme Court

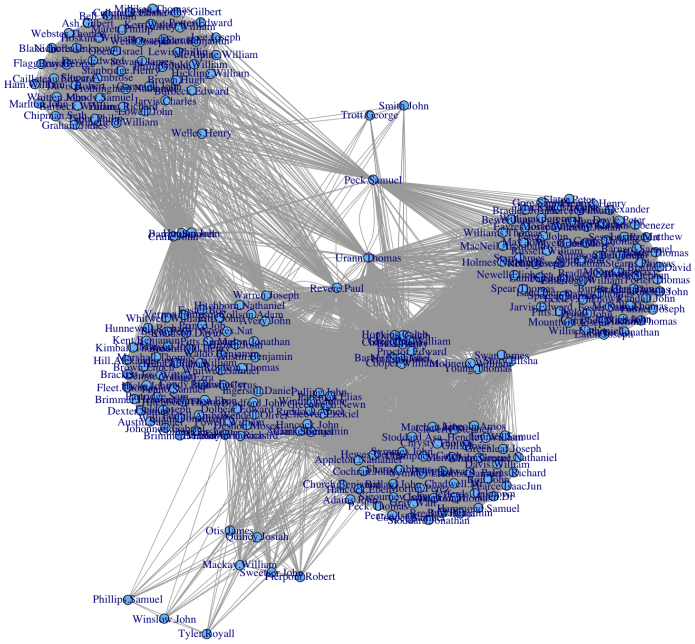
Section 702

- Section 702 of the FISA Amendments Act permitted "targeting" warrants
- ☞ Pick up traffic *about* a subject, if one end of the communication is abroad
- (The NSA appears to go to considerable effort to ensure that that requirement is met)
- Just renewed by Congress

Whom You Call is Unique

- No one else calls the same numbers that you call
- This can identify you, even if you change your phone number
- This has been done experimentally
- The same analysis picked out “communities of interest”: people whose calls tend to stay within the group

Finding Paul Revere Through Metadata



(From `https://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/`)

Voluntarily Given: Samsung

"If you enable Voice Recognition, you can interact with your Smart TV using your voice. To provide you the Voice Recognition feature, some voice commands may be transmitted (along with information about your device, including device identifiers) to a third-party service that converts speech to text or to the extent necessary to provide the Voice Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition."

`https://www.samsung.com/sg/info/privacy/smarttv.html`

Voluntarily Given: Verizon Patent Application

"To illustrate, access device 402 may detect, by way of detection device 406, that two users are cuddling on a couch during the presentation of the television program and prior to an advertisement break. Based on the detected ambient action, access device 402 . . . may select an advertisement associated with the ambient action. . . . To illustrate, access device 402 and/or the corresponding server device may utilize one or more terms associated with cuddling (e.g., the terms "romance," "love," "cuddle," "snuggle," etc.) to search for and/or select a commercial associated with cuddling (e.g., a commercial for a romantic getaway vacation, a commercial for a contraceptive, a commercial for flowers, a commercial including a trailer for an upcoming romantic comedy movie, etc.)"

US Patent Application 20120304206

Wiretapping in the Digital Age

- Less than half of Americans use traditional twisted pair land line telephones
- You can't tap a cell phone with alligator clips!
- And what about data?
- The FBI understood this more than 20 years ago

Enter CALEA

- In 1994, Congress passed CALEA: *Communications Assistance for Law Enforcement Act*
- It required a standardized interface to tap calls, from the comfort of their own offices
- Applied to any "entity engaged in providing commercial mobile service" or "a replacement for a substantial portion of the local telephone exchange service" (P.L. 113-414(103)(8)(B))
- Did not apply to "entities insofar as they are engaged in providing information services" (P.L. 113-414(103)(8)(C))
- It now applies to ISPs, despite that last clause. . .

Lawful Intercept

- Most other industrialized nations have passed similar laws
- The generic concept is known as “lawful intercept”
- All major manufacturers of phone switches and IP routers support it
- Precise rules for access are different in each country

What's the Trouble?

- "It's only a software change"
- ☞ But phone switch software is *very* expensive
- Congress authorized some money for switch upgrades, but not nearly enough
- The system required complex software—and that's *always* a recipe for trouble

They Were Warned. . .

- “It’s too complex”
- “It’s vulnerable to remote hacking”
- “The real bad guys will use crypto”
- Guess what happened?

Hacking

- What if someone hacks into the wiretap platform?
- Could they delete data? Insert false data? Modify data?
- Could they use the lawful intercept mechanism to spy on someone else?

The Athens Affair

- Vodaphone Greece bought a phone switch with (legally mandated) lawful intercept capability
- Someone—just whom has never been established—installed binary patches into the phone switch to (ab)use this mechanism
- The attacker tapped about 100 cell phones belonging to senior government officials, including the Prime Minister
- One phone number on the list belonged to someone at the American embassy
- A copy of every call was relayed to another cell phone number
- These were prepaid phones, bought over the counter for cash
- A key person was found dead, an apparent suicide, just after the attacks was detected

What Happened?

- Writing the intercept software took a great deal of skill
- Planting it took a very sophisticated hacking attempt or cooperation from an insider
- Various log books were destroyed
- There was good “tradecraft”
- Was it an intelligence agency? Which one?