Lecture 8.2 Information Privacy

CS 230: Ethical Issues in Computing
Fall 2020
Dr. Henderson
BSU

Announcements

- LA-6 due tonight
- LA-7 due Thursday, Oct 22 @ midnight
  - Quiz only
- LA-7 Challenges
  - A: Investigate your personal digital footprint
  - B: Privacy ladder

Last Time

- Privacy difficult to define precisely
  - Other natural rights cover privacy
  - Privacy a prudential right
- Information disclosure necessary
  - We should be stringent with personal data
  - Vigilant in our IT privacy settings
- What if we have nothing to hide?

Today

- Government balances privacy against security
- Four modes of privacy
  - Collection
  - Processing
  - Dissemination
  - Invasion

A Balancing Act

- Ben Franklin famously said those who would trade essential liberty for temporary safety deserve neither.
- Federal, state, and local governments in United States have had significant impact on privacy of individual Americans
- Government must balance competing desires of citizens
  - desire to be left alone
  - desire for safety and security
- Impact of attacks of September 11, 2001
  - Public concerns about national security rose sharply
  - Less concern about abuses of presidential power, as in Watergate scandal

Solove's Taxonomy of Privacy

- Information **collection**: Activities that gather personal information
- Information **processing**: Activities that store, manipulate, and use personal information that has been collected
- Information **dissemination**: Activities that spread personal information
- **Invasion**: Activities that intrude upon a person's daily life, interrupt someone's solitude, or interfere with decision-making

Invasion

Invasion

- Government actions to prevent invasion
  - Do Not Call Registry
  - CALM Act
- Invasive government actions
  - Requiring identification for pseudoephedrine purchases
  - Advanced Imaging Technology scanners at airports

National Do Not Call Registry

- FTC responded to public opinion
  - Created Do Not Call Registry in 2003
  - More than 50 million phone numbers registered before it even took affect
- Example of how privacy is treated as a prudential right
  - Benefit of shielding people from telemarketers judged to be greater than harm caused by limiting telephone advertising

CALM Act

- Television watchers complained to FCC about loud commercials for 50 years
- CALM Act signed by President Obama in 2010
- Required FCC to ensure television commercials are played at same volume as programs they are interrupting

Requiring ID for Pseudoephedrine Purchases

- Pseudoephedrine an ingredient of Sudafed and other cold medications
- It is also an ingredient of methamphetamine (“meth”)
- Federal and state governments have passed laws limiting access to pseudoephedrine
  - Limits quantity that can be purchased in a month
  - Identification and signature required for purchase in most states

Advanced Imaging Technology Scanners

- Transportation Security Administration began installing AIT scanners in 2007
- AIT scanners revealed anatomical features
- Electronic Privacy Information Center sued government in 2010, saying systems violated 4th Amendment and various laws
- TSA announced it would develop new software that would replace passenger-specific images with generic outlines
- All body scanners producing passenger specific images removed in 2013

Dissemination

Information Dissemination

- Legislation to restrict information dissemination
  - Family Education Rights and Privacy Act
  - Video Privacy Protection Act
  - Health Insurance Portability and Accountability Act
- Examples of information dissemination
  - Freedom of Information Act
  - Toll booth records used in court

Family Education Rights and Privacy Act (FERPA)

- Rights given to
  - Students 18 years and older
  - Parents of younger students
- Rights include
  - Reviewing educational records
  - Requesting changes to erroneous records
  - Preventing release of records without permission

Video Privacy Protection Act

- Videotape service providers cannot disclose rental records without consumer's written consent
- Rental stores must destroy personal information related to rentals within a year of when it is no longer needed

Health Insurance Portability and Accountability Act

- Limits how doctors, hospitals, pharmacies, and insurance companies can use medical information
- Health care providers need signed authorization to release information
- Health care providers must provide patients with notice describing how they use medical information

Freedom of Information Act

- Federal law designed to ensure public has access to US government records
- Signed by President Johnson (1966)
- Applies only to executive branch
- Nine exemptions
  - Classified documents
  - Trade secrets or financial information
  - Documents related to law enforcement investigations

Toll Booth Records Used in Court

- E-ZPass: an automatic toll-collection system used on most toll roads, bridges, and tunnels between Illinois and Maine
- Drivers with E-ZPass tags pass through without stopping to pay attendant
- Records have been provided in response to court orders in criminal and civil cases

Carpenter v. United States

- Series of nine armed robberies in 2010-11
  - Radio Shack and T-Mobile stores in Detroit area
  - Gangs made off with sacks of cell phones
- Police arrested four suspects in 2011
  - One confessed and named Timothy Carpenter as ringleader
- Police obtained Carpenter's cell phone records under the Stored Communications Act (no warrant required)
  - Two wireless providers supplied 127 days of location records
  - 12,898 location points in all (101 points per day)

Carpenter v. United States

- Prosecutors charged Carpenter with 6 counts of robbery, 6 counts of possessing a firearm during a violent crime
  - Used cell phone location evidence to show Carpenter was near stores that were robbed
- Carpenter's lawyer argued seizure of cell phone location records violated the 4th amendment to the U S Constitution, but judge denied the motion under third party doctrine, namely:
  - Can't expect information voluntarily given to third parties to remain private
- Carpenter found guilty and sentenced to more than 100 years in prison

Carpenter v. United States

- Appeal to US Supreme Court
- Supreme Court ruled 5-4 in favor of Carpenter
- Majority: Prosecutors erred when “mechanically applying third-party doctrine to this case”
- Cell phone numbers not “shared” in normal sense of word
- Location information obtained from Carpenter’s wireless carriers was a search
  - Prosecutors should have had a warrant
  - They violated Carpenter’s 4th Amendment rights

Processing

Genesis of Code of Fair Information Practices

- 1965: Director of Budget asked committee of economists to look at problems caused by decentralization of statistical data across federal agencies
- Committee recommended creation of a National Data Center
- Citizens and legislators expressed concerns about possible abuses of such a system
- Another group formed to draft guidelines for government databases

Code of Fair Information Practices

- No secret databases
- People should have access to personal information in databases
- Organizations cannot change how information is used without consent
- People should be able to correct or amend records
- Database owners, users responsible for reliability of data and preventing misuse

Privacy Act of 1974 Falls Short

- Applies only to government databases
- Only covers records indexed by a personal ID
- No federal employee responsible to enforcing Privacy Act provisions
- Allows agencies to share records with other agencies

Legislation for Private Institutions

- Fair Credit Reporting Act
- Fair and Accurate Credit Transactions Act
- Financial Services Modernization Act

Fair Credit Reporting Act

- Promotes accuracy and privacy of information used by credit bureaus
- Major credit bureaus: Equifax, Experian, Trans Union
- Negative information kept only 7 years
- Exceptions
  - Bankruptcies: 10 years
  - Criminal convictions: indefinitely

Fair and Accurate Credit Transactions Act

- Passed in 2004
- Requires three major credit bureaus to provide consumers a free copy of their credit report every 12 months
- Not automatic: consumers must request credit reports
- Provisions to reduce identity theft

Financial Services Modernization Act

- Also called Gramm-Leach-Bliley Act of 1999
- Creates “financial supermarkets” offering banking, insurance, and brokerage services
- Privacy-related provisions
- Privacy policies must be disclosed to customers
- Notices must provide an opt-out clause
- Companies must develop procedures to protect customers’ confidential information

Internal Revenue Service Audits

- Internal Revenue Service uses computer matching and data mining to look for possible income tax fraud
- Computer matching: matching tax form information with information provided by employers, banks, etc.
- Data mining: searching through forms to detect those that appear most likely to have errors resulting in underpayment of taxes

Syndromic Surveillance Systems

- Syndromic surveillance system: A data mining system that searches for patterns indicating the outbreak of an epidemic or bioterrorism
- 911 calls
- emergency room visits
- school absenteeism
- Internet searches
- Example: A system in New York City detected an outbreak of a virus in 2002

Telecommunications Records Database

- Created by National Security Agency after 9/11
- Contains phone call records of tens of millions of Americans
- NSA analyzing calling patterns to detect terrorist networks
- Phone records voluntarily provided by several major telecommunications companies
- USA Today revealed existence of database in May 2006
- Several dozen class-action lawsuits filed
- August 2006: Federal judge in Detroit ruled program illegal and unconstitutional
- July 2007: US Court of Appeals overturned ruling, saying plaintiffs did not have standing to bring suit forward

Predictive Policing

- Hypothesis: Criminals behave in a predictable way
  - Times of crimes fall into patterns
  - Some areas have higher incidence of crimes
- Predictive policing: use of data mining to deploy police officers to areas where crimes are more likely to occur
- Police in Santa Cruz and Los Angeles saw significant declines in property crime

Potential Harms of Profiling

- Government security agencies supposed to protect nation from harm
- What if an erroneous profile characterizes an innocent citizen as a potential terrorist?
- May be impossible to explain how an algorithm has put someone on the watch list
- U S government’s terrorist watch list now contains 1.5 million names
- How can innocent people clear their names?

Social Security Number

- Social Security cards first issued 1936
- Originally used only for Social Security purposes
- Use of SSN has gradually increased
- SSN is a poor identification number
  - Not unique
  - Rarely checked
  - No error-detecting capability

Arguments for National ID Card

- Current ID cards are second-rate
- Would reduce illegal entry to US
- Would prevent illegal aliens from working
- Would reduce crime
- Other democratic countries have national ID cards

Arguments Against National ID Card

- No card positively guarantees identification
  - Even a hard-to-forge ID card can be compromised by insiders
- No biometric-based system is 100% accurate
- No evidence it will reduce crime
- Makes government data mining simpler
- Make law-abiding people more vulnerable to fraud and indiscretions

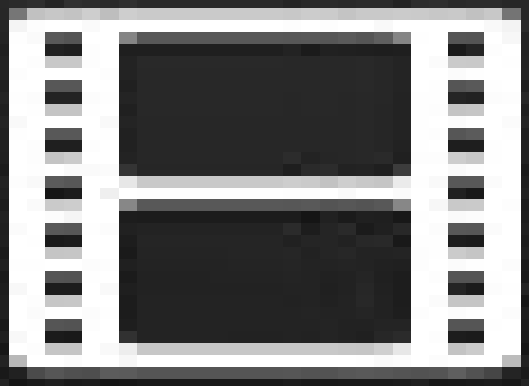
The Real ID Act

- Signed in May 2005, but implementation has been slow
- Significantly changes driver's licenses in the United States
- New licenses
  - Required to open bank account, fly on commercial airplane, or receive government service
  - Requires applicants to supply 4 different IDs
  - Contains a biometric identifier
  - Must contain data in machine-readable form
- Most states have come into compliance; rest have received extensions from the Department of Homeland Security
- Real ID-compliant driver's licenses needed by October 2020 in order to use as them as IDs for domestic airline flights

Possible Consequences of New Licenses

- Better identification means better law enforcement
- People won’t be able to change identities
  - Parents ducking child support
  - Criminals on the run
- Could centralized databases lead to more identity theft?

Collection



Employee Polygraph Protection Act

- Passed in 1988
- Prohibits private employers from using lie detector tests under most conditions
- Cannot require test for employment
- Exceptions
  - Pharmaceutical companies and security firms may give test to certain classes of employees
  - Employers who have suffered a theft may administer tests to reasonable suspects
  - Federal, state, and local governments exempt

Children's Online Privacy Protection Act

- Reduces amount of public information gathered from children
- Online services must gain parental consent before collecting information from children 12 and under

Genetic Information Nondiscrimination Act

- Health insurance companies
  - Can’t request genetic information
  - Can’t use genetic information when making decisions about coverage, rates, etc.
  - Doesn’t apply to life insurance, disability insurance, long-term care insurance
- Employers
  - Can’t take genetic information into account when hiring, firing, promoting, etc.
  - Small companies (< 15 employees) are exempt

Census Records

- Census required by U S Constitution to ensure every state has fair representation
- Number of questions steadily rising
- Statistical sampling used since 1940 – about 5% of population gets a form with more questions
- Sometimes Census Bureau has broken confidentiality requirement
  - World War I: draft resistors
  - World War II: Japanese-Americans

Internal Revenue Service Records

- The 16th Amendment to the U S Constitution gives the federal government the power to collect an income tax
- IRS collects more than $2 trillion a year in income taxes
- Income tax forms contain a tremendous amount of personal information: income, assets, to whom you make charitable contributions, medical expenses, and more

FBI National Crime Information Center 2000

- NCIC
  - Collection of databases related to various crimes
  - Contains > 39 million records
- Successes
  - Helps police solve hundreds of thousands of cases every year
  - Helped FBI tie James Earl Ray to assassination of Dr. Martin Luther King, Jr.
  - Helped FBI apprehend Timothy McVeigh for bombing of federal building in Oklahoma City

One DOJ Database

- Database being constructed by US Department of Justice
- Gives state and local police officers access to information provided by five federal law enforcement agencies
  - Incident reports
  - Interrogation summaries
  - Other information not available through NCIC
- Criticisms
  - One DOJ gives local police access to information about people who have not been charged with a crime
  - There is no way to correct misinformation in raw police reports

Closed-Circuit Television Cameras

- First use in Olean, New York in 1968
- Now more than 30 million cameras in U S
- New York City's effort in lower Manhattan
  - $201 million for 3,000 new cameras
  - License plate readers
  - Radiation detectors
- Effectiveness of cameras debated

License-Plate Scanners

- More than 70% of police departments in United States use license-plate scanners
  - Mounted on police cars, parking enforcement vehicles, road signs, toll gates, bridges
- ACLU: Wrong for police to collect data about citizens who are not criminal suspects
- How long information kept varies
  - Minnesota state patrol: 48 hours
  - Milpitas, California: indefinitely
- A few states restrict use of scanners

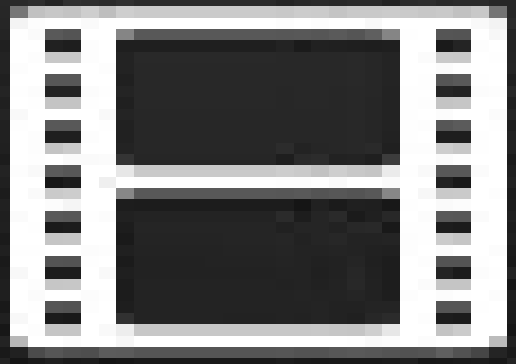
Police Drones

- Hundreds of police departments in US operate small unmanned drones
- FAA puts restrictions on use
  - Weigh no more than 25 pounds
  - Fly no higher than 400 feet
  - Be flown during daylight within view of operator
- Public opinion mixed
  - Yes: Search and rescue
  - No: Identify speeders
- Should police be required to get a search warrant before surveillance of a residence?

Covert Surveillance

4th Amendment to 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.”



Wiretaps and Bugs

- Omstead v. United States – Supreme Court rules wiretapping without a search warrant OK
- Federal Communications Act - wiretapping made illegal without a search warrant
- Nardone v. United States – Supreme Court rules search warrant needed for wiretapping
- Attorney General declared FBI would cease wiretapping
- FBI continues secret wiretapping
- Katz v. United States – Supreme Court rules search warrant needed in order to place a bug (hidden microphone)

Operation Shamrock

- National Security Agency created in 1952, took over operation
- Expanded to telephone calls
- Kennedy
  - Organized crime figures
  - Cuba-related individuals and businesses
- Johnson and Nixon
  - Vietnam war protesters
- Nixon
  - War on drugs

Carnivore Surveillance System

- Created by FBI in late 1990s
- Monitored Internet traffic, including email exchanges
- Carnivore = Windows PC + “packet-sniffing” software
- Captured packets going to/from a particular IP address
- Used about 25 times between 1998 and 2000
- Replaced with commercial software

Covert Activities After 9/11

- September 11, 2001 attacks on World Trade Center and Pentagon
- President Bush authorized new, secret, intelligence-gathering operations inside United States

National Security Administration Wiretapping

- President Bush signed presidential order
  - OK for NSA to intercept international phone calls & emails initiated by people inside US
  - No search warrant required
- Number of people monitored
  - About 500 people inside US
  - Another 5,000-7,000 people outside US
- Two al-Qaeda plots foiled
  - Plot to take down Brooklyn bridge
  - Plot to bomb British pubs and train stations

TALON Database

- Created by US Department of Defense in 2003
- Supposed to contain reports of suspicious activities or terrorist threats near military bases
- Reports submitted by military personnel or civilians
- Reports assessed as “credible” or “not credible” by military experts
- Reports about anti-war protests added to database
- Many of these reports later deleted from database
- In 2007 new Under Secretary of Defense for Intelligence recommended that TALON be terminated

Title III

- Part of Omnibus Crime Control and Safe Streets Act of 1968
- Allows a police agency with a court order to tap a phone for up to 30 days
- In 1972 US Supreme Court again rejected warrantless wiretapping, even for national security

Foreign Intelligence Surveillance Act

- FISA provides judicial and congressional oversight of covert surveillance of foreign governments and agents
- Allows electronic surveillance of foreign nationals for up to one year without a court order
- Amended in 2007 to allow government to wiretap communications to/from foreign countries without oversight by FISA Court

PRISM Program

- Documents provided by Edward Snowden revealed NSA had obtained access to servers at Microsoft, Yahoo, Google, Facebook, YouTube, Skype, AOL, and Apple
- PRISM program enabled NSA to access email messages and monitor live communications of foreigners outside United States
- All companies contacted by the Guardian denied knowledge of the PRISM program

Electronic Communications Privacy Act

- Passed by Congress in 1986
- Allows police to attach two kinds of surveillance devices to a suspect's phone line
- Pen register: displays number being dialed
- Trap-and-trace device: displays caller's phone number
- Court order needed, but prosecutors do not need to show probable cause
- Allows police to do roving wiretaps (following suspect from phone to phone)

Stored Communications Act

- Part of Electronic Communications Privacy Act
- Government does not need a search warrant to obtain from an Internet service provider email messages more than 180 days old
- Advent of cloud computing raises new privacy concerns
  - Most people now allow their ISP to store their email
- Digital Due Process organization (nearly 50 companies and privacy rights organizations) lobbying Congress to change law

Communications Assistance for Law Enforcement Act

- Passed in 1994
- Designed to ensure police can still do wiretapping as digital networks are introduced
- FBI asked for new abilities, such as ability to intercept digits typed by caller after phone call placed
- Federal Communications Commission included these capabilities in its guidelines to phone companies
- Privacy-rights advocates argued that new capabilities went beyond Congress's intent

USA PATRIOT Act

- Passed after terrorist attacks of September 11, 2001
- Provisions
  - Greater police authority to monitor communications
  - Greater powers to regulate banks
  - Greater border controls
  - New crimes and penalties for terrorist activity
- Critics say Act undermines 4th Amendment rights
  - Pen registers on Web browsers
  - Roving surveillance
  - Searches and seizures without warrants
  - Warrants issued without need for showing probable cause

National Security Letters

- FBI can collect Internet, business, medical, educational, library, and church/mosque/ synagogue records without showing probable cause
- FBI issues a National Security Letter stating the records are related to an ongoing investigation; no approval from judge needed
- Gag orders prevent recipients (e.g., libraries) from disclosing receipt
- FBI issued 50,000 National Security Letters a year between 2003 and 2006

PATRIOT Act Successes

- Charges against 361 individuals
- Guilty pleas or convictions for 191 people
- Shoe-bomber Richard Reid
- John Walker Lindh
- More than 500 people removed from United States
- Terrorist cells broken up in Buffalo, Seattle, Tampa, and Portland (“the Portland Seven”)

PATRIOT Act Failure: Case of Brandon Mayfield

- March 11, 2004 terrorist bombings in Madrid Spain
- FBI makes Brandon Mayfield a suspect
  - Claims partial fingerprint match
  - Conducts electronic surveillance
  - Enters home without revealing search warrant
  - Copies documents and computer hard drives
  - Arrests Mayfield as a material witness and detains him for 2 weeks
- Spanish authorities match fingerprint with an Algerian
- Judge orders Mayfield released
- FBI apologizes for fingerprint misidentification
- Government issues formal apology and pays Mayfield $2 million
- Civil rights groups: Mayfield was targeted for his religious beliefs

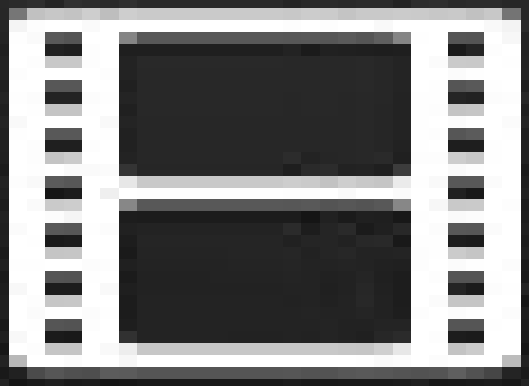
Long-Standing NSA Access to Telephone Records

- Edward Snowden leaked documents to the Guardian newspaper
- Guardian revealed Foreign Intelligence Surveillance Court had ordered Verizon to provide NSA with all of its telephone metadata for 3-month period in 2013 (date, time, location, and length of call, but not contents of call)
- Guardian critique: NSA's mission now "focuses increasingly on domestic communications"
- May 2015: Federal court ruled NSA's program was illegal
- June 2015: Congress passed a reform, called the USA Freedom Act, requiring agencies to obtain a court order before accessing metadata
- Are we making progress?


Hour
WITH BRIAN WILLIAMS
XCLUSIVE

Summary

- Constitutional guarantees in Bill of Rights sometimes conflict with desires of law enforcement agencies to gather evidence that can help them deter crime or capture criminals
- Three branches of government struggle with finding right balance between competing concerns
- Pursuing their objectives, US law-enforcement or national security agencies have sometimes broken federal laws or violated US Constitution
- Once every US state brings its driver's license into compliance with Real ID Act, United States will have de facto national identification card



Next Time

- Security
  - Read 7.1-7.2 in the text