Lecture 6: Who owns information?

(Some slides are from M. Quinn, *Ethics for the Information Age*, Pearson © 2013.)

Who owns information about you?

- Do you?
- Does the government?
- Do companies?

How do they get the information?

- Information collection: Activities that gather personal information
  - Government and business enterprises (Transactional data)
  - Websites, sensors, video camera
  - Surveillance by government* and business enterprises
- *Information processing: Activities that store, manipulate, and use personal information that has been collected
  - Databases and Data Mining
- Information dissemination: Activities that spread personal information
  - Public websites and 3rd party exchange of information

*Lecture 6 This lecture

1-3

Lecture Overview

- Government surveillance
  - Legal
  - Covert
- Data Mining
  - Regulation of public and private databases
  - Data mining by government
  - Data mining by commerce

1-4

Government Surveillance

1-5

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."

1-6

A Balancing Act

- Federal, state, and local governments in United States have had significant impact on privacy of individuals
- Government must balance competing desires
  - desire to be left alone
  - desire for safety and security
- National security concerns increased significantly after 9/11 attacks

1-7

Legal Surveillance

Wiretaps and Bugs

- *Omstead v. United States (1928)*
  - wiretapping OK
- Federal Communications Act (1934)
  - wiretapping made illegal
- *Nardone v. United States (1939)*
  - wiretapping not OK
- FBI continues secret wiretapping
- *Katz v. United States (1967)*
  - bugs not OK

1-9

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 U.S. Supreme Court again rejected warrantless wiretapping, even for national security

1-10

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)

1-11

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
- Digital Due Process organization (nearly 50 companies and privacy rights organizations) lobbying Congress to change law

1-12

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

1-13

USA PATRIOT Act October 26, 2001

- Provisions
  - Greater 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

1-14

Patriot Act Renewal

- Patriot Act renewed in 2006
- Nearly all provisions made permanent
- Four-year sunset clause on three provisions
  - Roving wiretaps
  - FBI ability to seize records from businesses with approval from secret Foreign Intelligence Surveillance Court
  - Surveillance of "lone wolves"
- Patriot Act again renewed in 2011

1-15

National Security Letters

- FBI can collect Internet, business, medical, educational, library, and church/mosque/ synagogue records without showing probable cause
- 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

1-16

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")

1-17

Patriot Act Failure

- March 11, 2004 bombings in Madrid Spain
- FBI makes Brandon Mayfield (Portland lawyer) a suspect
  - Claims partial fingerprint match
  - Conducts electronic surveillance
  - Enters home without revealing search warrant
  - Copies documents and computer hard drives
- Spanish authorities match fingerprint with an Algerian
  - Judge orders Mayfield released
  - FBI apologizes
- Civil rights groups: Mayfield was targeted for his religious beliefs

1-18

Covert Surveillance

Covert Surveillance by Federal Government

- Operation Shamrock
  - Continuation of World War II interception of international telegrams 1945
  - National Security Agency (NSA) created 1952
    - Expanded to telephone calls
    - Analyzed 150k messages/month
      - Kennedy: Organized crime figures & Cuba-related individuals and businesses
      - Johnson and Nixon: Vietnam war protesters
      - Nixon: War on drugs
  - Terminated in 1976
- 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
  - 2005 Replaced with commercial software *NarusInsight*
    - Provides real-time internet network traffic spyware

1-20

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

1-21

National Security Administration (NSA) Wiretapping

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

1-22

TALON Database

- Created by U.S. 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 TALON terminated although working on new system. However, FBI's Guardian system still collecting information.

1-23

Data Mining: Regulation of Public and Private Databases

1-24

Data Mining

- Searching records in one or more databases, looking for patterns or relationships
- Can be used to profile individuals
  - Allows government to find criminal or suspicious persons
  - Allows companies to build more personal relationships with customers

1-25

FTC Code of Fair Information Practices 1972

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

1-26

Privacy Act of 1974

- Code of Fair Information Practice
- Applies only to government databases
- Only covers records indexed by a personal ID
- No federal employee responsible to enforce Privacy Act provisions
- Allows agencies to share records with other agencies

1-27

The REAL ID Act

- Signed in May 2005
- Significantly changes driver's licenses in the United States
- New licenses
  - Issued by end of 2013
  - Required to open bank account, fly on commercial airplane, or receive government service
  - Requires applicants to supply 4 different IDs
  - Will probably contain a biometric identifier
  - Must contain data in machine-readable form
- Half of the states have resisted implementation of REAL ID; doubtful 2013 deadline will be met
- Oregon? What is the biometric identifier?

1-28

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
- New, centralized databases could lead to more identity theft

1-29

Legislation for Private Institutions

- Fair Credit Reporting Act
- Fair and Accurate Credit Transactions Act
- Financial Services Modernization Act
- Prevention of Invasion of Privacy

1-30

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

1-31

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

1-32

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

1-33

Government actions to prevent invasion of privacy

- Do Not Call Registry
- CALM Act: Turns down sound on commercials

1-34

Data Mining by the Government

1-35

IRS Audits

- IRS 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

1-36

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

1-37

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: U.S. Court of Appeals overturned ruling, saying plaintiffs did not have standing to bring suit forward

1-38

Invasive government actions

- Requiring identification for pseudoephedrine purchases
- Advanced Imaging Technology scanners at airports

Data Mining by Commerce

1-40

Google's Personalized Search

- Secondary use: Information collected for one purpose use for another purpose
- Google keeps track of your search queries and Web pages you have visited
  - It uses this information to infer your interests and determine which pages to return
  - Example: "bass" could refer to fishing or music
- Also used by retailers for direct marketing

1-41

Collaborative Filtering

- Form of data mining
- Analyze information about preferences of large number of people to predict what one person may prefer
  - Explicit method: people rank preferences
  - Implicit method: keep track of purchases
- Used by online retailers and movie sites

1-42

Ownership of Transaction Information

- Who controls transaction information?
  - Buyer?
  - Seller?
  - Both?
- Opt-in: Consumer must explicitly give permission before the organization can share info
- Opt-out: Organization can share info until consumer explicitly forbid it
- Opt-in is a barrier for new businesses, so direct marketing organizations prefer opt-out

1-43

Credit Reports

- Example of how information about customers can itself become a commodity
- Credit bureaus
  - Keep track of an individual's assets, debts, and history of paying bills and repaying loans
  - Sell credit reports to banks, credit card companies, and other potential lenders
- System gives you more choices in where to borrow money
- Poor credit can hurt employment prospects

1-44

Microtargeting

- Political campaigns determine voters most likely to support particular candidates
  - Voter registration
  - Voting frequency
  - Consumer data
  - GIS data
- Target direct mailings, emails, text messages, home visits to most likely supporters

1-45

Marketplace: Households

- Lotus Development Corporation developed CD with information on 120 million Americans
- Planned to sell CD to small businesses that wanted to create mailing lists based on various criteria, such as household income
- More than 30,000 consumers complained to Lotus about invasion of privacy
- Lotus dropped plans to sell CD

1-46

Facebook Beacon

- Fandango, eBay, and 42 other online businesses paid Facebook to do "word of mouth" advertising
- Facebook users surprised to learn information about their purchases was shared with friends
- Beacon was based on an opt-out policy
- Beacon strongly criticized by various groups
- Facebook switched to an opt-in policy regarding Beacon

1-47

Netflix Prize

- Netflix offered $1 million prize to any group that could come up with a significantly better algorithm for predicting user ratings
- Released more than 100 million movie ratings from a half million customers
  - Stripped ratings of private information
- Researchers demonstrated that ratings not truly anonymous if a little more information from individuals was available
- U.S. Federal Trade Commission complaint and lawsuit
- Netflix canceled sequel to Netflix Prize

1-48

Social Network Analysis

- Data mining now incorporating information collected from social networks
- Examples
  - Cell phone companies in India identify "influencers"
  - Banks evaluate the riskiness of loans
  - Police predict locations of big parties

1-49

Police Monitor Facebook and Twitter to Identify Locations of Big Parties

1-50

Summary & Conclusions

Who owns information?

- Do you?
  - Not if you give it away
    - Required to supply it by law to government
    - Required to supply for a credit transaction
    - Required to supply for a membership
- Does the government?
  - Yes, but it is limited in what it can do with it
    - Although it can spy on you
- Do companies?
  - Yes, if you use it for a transaction
    - Might provide policies, opt-out and opt-in
  - They can also sell it to others