

CS 4001: Computing, Society & Professionalism

Munmun De Choudhury | Assistant Professor | School of Interactive Computing

Week 7: Privacy and the
Government
February 23, 2017

A Balancing Act

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

Privacy Post 9/11

- (2006 poll) 70% Americans supported “expanded camera surveillance on streets and in public places”
- 62% supported “law enforcement monitoring of Internet discussions in chat rooms and other forums”
- 61% supported “closer monitoring of banking and credit card transactions to trace funding sources”
- 52% supported “expanded governmental monitoring of cell phones and emails to intercept communications”

Solove's Taxonomy of Privacy

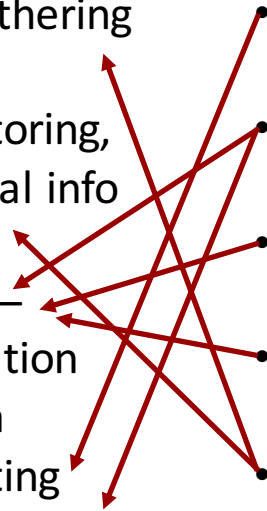
- **Information collection:** Activities that gather personal information
- **Information processing:** Activities that store, manipulate, and use personal information that has been collected
- **Information dissemination:** Activities that spread personal information
- **Invasion:** Activities that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

Class Discussion: Relationship with definitions of privacy

- 1) **Information collection** – gathering personal information.
 - 2) **Information processing** – storing, manipulating, using personal info that has been collected
 - 3) **Information dissemination** – spreading personal information
 - 4) **Invasion** – intruding upon a person's daily life, interrupting someone's solitude, or interfering with decision-making
- Privacy is the right to be left alone (Warren & Brandeis).
 - Privacy is the state of being away from public attention (Gavison).
 - Privacy is control over who knows what about us (Rachels).
 - Privacy is the appropriate flow of personal information (Nissenbaum).
 - Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves (Fried).

Class Discussion: Relationship with definitions of privacy

- 1) **Information collection** – gathering personal information.
- 2) **Information processing** – storing, manipulating, using personal info that has been collected
- 3) **Information dissemination** – spreading personal information
- 4) **Invasion** – intruding upon a person's daily life, interrupting someone's solitude, or interfering with decision-making



Privacy is the right to be left alone (Warren & Brandeis).

Privacy is the state of being away from public attention (Gavison).

Privacy is control over who knows what about us (Rachels).

Privacy is the appropriate flow of personal information (Nissenbaum).

Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves (Fried).



US Legislation restricting information 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



Information Collection by the Government

Census Records

- Census required to ensure every state has fair representation
- Number of questions steadily rising
- Sometimes Census Bureau has broken confidentiality requirement
 - World War I: draft resisters
 - World War II: Japanese-Americans

Internal Revenue Service Records

- The 16th Amendment to the US 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

Closed Circuit Television Cameras

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

Surveillance Camera Images of Boston Marathon Bombing Suspects



Police Drones

- A few police departments in US operate small unmanned drones
- FAA puts restrictions on use
- Public opinion mixed
 - Yes: Search and rescue
 - No: Identify speeders
- Should police be required to get a search warrant before surveillance of a residence?



Class Activity 2 (DNA Database)



Covert Government Surveillance

Wiretapping – J. Edgar Hoover



Operation Shamrock

- Continuation of World War II interception of international telegrams
- National Security Agency (1952)
- 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

NSA Wiretapping Post 9/11

- 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



US Legislation Authorizing Wiretapping

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 US
- All companies contacted by the *Guardian* denied knowledge of the PRISM program

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



Data Mining by the Government

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

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

Predictive Policing

- 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



Class Activity 3a, 3b (Predictive Policing Technology)



National Identification Card

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



Class Activity 1 (Debating over a National ID card)

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
- Most states missed 2013 deadline; temporary deferments being granted



Information Dissemination

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

Health Insurance Portability and Accountability Act (HIPAA)

- 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



Invasion

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

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