CIS 381: Social & Ethical Issues of Computing

Privacy

Dr. David Koop
Defining Privacy

- Privacy related to notion of access
- Access
  - Physical proximity to a person
  - Knowledge about a person
- Privacy is a "zone of inaccessibility"
- Privacy violations are an affront to human dignity
- Too much individual privacy can harm society
- Where to draw the line?
Benefits & Harms of Privacy

• Benefits:
  - Individual growth
  - Individual responsibility
  - Freedom to be yourself
  - Intellectual and spiritual growth
  - Development of loving, trusting, caring, intimate relationships

• Harms:
  - Cover for illegal or immoral activities
  - Burden on the nuclear family
  - Hidden dysfunctional families
  - People on society’s fringes can be ignored

[M. J. Quinn]
Privacy and Trust

• Modern life is actually more private than life centuries ago
  - Most people don’t live with extended families
  - Automobile allows us to travel alone
  - Television instead of public entertainment
• Challenge: we now live among strangers
• Remedy: establishing reputations
  - Ordeal: lie detector test or drug test
  - Credential: driver’s license, key, ID card, college degree
• Establishing reputation is done at the cost of reducing privacy
Medical Records and Voter Registration

- 37 states have legislative mandates for hospitals to collect patient data
- Made available to researchers and individuals (anonymized data)
- Voter registration lists available for purchase
- In 1998, Researcher Latanya Sweeney linked the then-governor of Massachusetts to his medical records
- 6 voters had his birthdate, 3 were male, only 1 in his zipcode
Assignment 4

- Link
- Video: Data Brokers
- How personal information is gathered, sold, and bought
- Due March 8
Term Paper Topic Selection

• Rank (at least) top three topics
• If you have a topic not covered, please specify as Other
• Due Friday afternoon
• Plan to get topics out over the break
Government and Information Privacy

- 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
"It can't be a sustainable end state for there to be an entirely unfettered space that's utterly beyond law enforcement for criminals to hide"

—FBI Director Christopher Wray, March 5, 2019
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
US Legislation Affecting Privacy

• Employee Polygraph Protection Act
  - 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
US Legislation Affecting Privacy

- **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
    - Cannot request genetic information
    - Cannot use genetic information when making decisions about coverage, rates, etc.
    - Doesn’t apply to life/disability/long-term care insurance
  - Employers cannot take genetic information into account when hiring, firing, promoting, etc.

[M. J. Quinn]
• Census Records
  - Census required to ensure every state has fair representation
  - Sometimes Census Bureau has broken confidentiality requirement
    • World War I: Draft Resistors
    • World War II: Japanese-Americans
  - Supreme Court currently deciding a case about whether the 2020 Census should have the question "Is this person a citizen of the United States?"
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.
NCIC

- 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
NCIC

- Criticisms
  - Erroneous records can lead to arrests of innocents (e.g. people with the same name as criminals)
  - Can be used to keep records about non-criminals
  - Corrupt employees have sold information and altered records
  - People search it for personal reasons (friends, babysitters, etc.)
OneDOJ Database

• Database being constructed by US Department of Justice
• Information not available through NCIC
• Gives state and local police officers access to information provided by five federal law enforcement agencies
  - Incident reports
  - Interrogation summaries
• Criticisms
  - OneDOJ 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 US
- New York City's effort in lower Manhattan
  - $201 million for 3,000 new cameras
  - Paired with license plate readers and radiation detectors
- Most capture is not of criminal events
- "Largely ineffective for crime prevention" [M. A. Sasse]
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

- A few police departments in US operate small unmanned drones
- FAA puts restrictions on use
- Public opinion on role
  - Yes: Search and rescue
  - No: Identify speeders
- Should police be required to get a search warrant before surveillance of a residence?
4th Amendment to US 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: Wiretapping OK
- Federal Communications Act: Makes wiretapping illegal
- Nardone v. United States: Wiretapping not OK
- FBI continues secret wiretapping
- Katz v. United States: Bugs not OK
Operation Shamrock

- Continuation of World War II interception of international telegrams
- Inherited by National Security Agency after its formation (1952)
- Expanded from telegrams to telephone calls
- Political leaders added names to "watch":
  - R. F. Kennedy: organized crime figures and Cuba-related individuals and businesses
  - Johnson and Nixon: Vietnam war protesters
  - Nixon: those involved in the drug trade
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
National Security Administration Wiretapping

• September 11, 2001 attacks on World Trade Center and Pentagon

• 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

[M. J. Quinn]
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
US Legislation Authorizing Wiretapping

- **Title III**
  - 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 wiretapped communications to/from foreign countries without oversight by FISA Court

[M. J. Quinn]
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
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
- Digital Due Process organization (nearly 50 companies and privacy rights organizations) lobbying Congress to change law
CALEA

- Communications Assistance for Law Enforcement Act (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

- **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

[M. J. Quinn]