CIS 381: Social & Ethical Issues of Computing

Privacy

Dr. David Koop
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?
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
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
Term Paper Topic Selection

• Important: **Redo** if you did this before I changed this to a "Test"
• Rank (at least) top three topics
• If you have a topic not covered, please specify as Other
• Due this afternoon
• Plan to get topics out over the break
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
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
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

- After March 11, 2004 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
- Spanish authorities match fingerprint with an Algerian
  - Judge orders Mayfield released
  - FBI apologizes
- Civil rights groups: Mayfield was targeted for his religious beliefs
Patriot Act Renewal

- Nearly all provisions have been made permanent
- Four-year sunset clause on two provisions
  - Roving wiretaps
  - FBI ability to seize records from financial institutions, libraries, doctors, and businesses with approval from secret Foreign Intelligence Surveillance Court
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
Code of Fair Information Practices

• "Bill of Rights for the Information Age" (1970s)

• Code
  - 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

[M. J. Quinn]
Data Mining by the Government

• Data mining: Process of searching through one or more databases looking for patterns or relationships among the data

• Examples:
  - IRS Audits: match information from different sources and find returns that appear likely to have errors resulting in underpayment
  - Syndromic Surveillance Systems: search for patterns indicating the outbreak of an epidemic or bioterrorism
  - NSA Telecommunications Records Database: analyze calling patterns to detect terrorist networks
  - Predictive Profiling
Predictive Policing

• Theory: 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

• Do you see any issues with this?
Potential Harms of Profiling

- 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
- How can innocent people clear their names?
- What data exists (and what doesn't exist)?
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

• 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

• 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

• 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
Invasion

- Government actions to prevent invasion
  - Do Not Call Registry: shielding people from telemarketers judged to be greater than harm caused by limiting telephone advertising
  - CALM Act: ensure television commercials are played at same volume as programs they are interrupting

- Invasive government actions
  - Requiring identification for pseudoephedrine purchases
    - used to make meth
    - require identification/signature and limit amount
  - Advanced Imaging Technology scanners at airports
    - initially created revealing images
    - TSA develops new software to show generic outlines

[M. J. Quinn]
Data Gathering and Privacy Implications

- Facebook tags
- Enhanced 911 services
- Rewards or loyalty programs
- Body scanners
- RFID tags
- Implanted chips
- Mobile apps
- OnStar
- Automobile “black boxes”
- Medical records
- Digital video recorders
- Cookies and flash cookies
Zuckerberg's Privacy Manifesto

• Posted on Wednesday (good timing for this course)
• https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/

• Private interactions
• Encryption
• Reducing Permanence
• Safety
• Interoperability
• Secure data storage
"I might buy that this is a sincere pivot to privacy and a realization that this is a good way to communicate, if it weren't for the fact that Mark Zuckerberg himself seems to have known for all of his adult life that this is a good way to communicate. This is a guy who mocked his users in college for sharing their personal information. This is a guy who covers his own laptop microphone and camera with tape. This is a guy who bought up all the property around his house so he could have more privacy. This is a guy who granted himself disappearing messages on Facebook when no one else had them. If your measure of trusting someone is based on how they act and not based on what they say, which I find is a good rule in life, then approach this new embrace of privacy for what it is: it’s not philosophy, it's business."

— Molly Wood, Marketplace Tech
The Data Brokers

• "Today we are giving up more and more private information online without knowing that it's being harvested and personalized and sold to lots of different people...our likes and dislikes, our closest friends, our bad habits, even your daily movements, both on and offline. Federal Trade Commissioner Julie Brill says we have lost control of our most personal information."

• Were you aware of these companies?

• What evidence have you seen of the impact of these data brokers?
What does Acxiom Know?

[Diagram showing various personal data points collected by Acxiom, including age, gender, education, employment, political views, relationship status, number of children, purchases, activities, media usage, loans, income, net worth, vehicles owned, properties owned, details about banking and insurance policies, range of new credit granted, socioeconomic status, economic stability, one of nearly 200 “ethnic codes,” assimilation score, religious beliefs, health interests, alcohol & tobacco interests, casino gaming & lottery interests, likelihood that someone is a heavy Facebook user, is a social influencer, is socially influenced, has no formal banking relationships, has no major medical insurance, details about someone’s home, including the number of bedrooms, type of home, multi-family, mobile home, prison, planning to have a baby, planning to adopt a child, filing taxes in April.]

[Cracked Labs]