Ethics: The right to privacy

Defining privacy

- Discussions about privacy revolve around the idea of "access"
  - physical proximity to a person
  - knowledge about that person
- There is a conflict between the rights/desires of a person who wants to restrict access to himself, and those of outsiders wishing to gain access
- Where should the line be drawn between what is private and what is public (known to all)?

Some simple examples

- Privacy as a good to society
  - A friend invites you to look at something that they've found on the web. You go into the lab, and she begins to log on. While it is her responsibility to keep her password private, it's generally accepted that you should avert your gaze while she enters it.

- Privacy as harmful to society
  - Suppose a group of wealthy individuals forms a private club, wherein the members share information with each other that is not generally available to the public. If the club allows them to cut business deals with each other on the basis of this information, that gives the members an unfair advantage over others in the community.

Some harms of privacy

- Some people take advantage of privacy to plan and perform illegal or immoral activities
- It has been suggested that increasing privacy has caused unhappiness by forcing nuclear families to care for all of its members
  - In the past, people received moral support from relatives, neighbors, etc. Now, they must "solve their own problems", regardless of the personal strain.
- The respect for family privacy in our culture can foster domestic violence.

Some benefits of privacy

- It has been argued that privacy is valuable because it lets us be ourselves.
  - Imagine you're in the park, playing with a child. How would you behave if you knew that you were being watched, and that others might be reviewing your behavior for suspicious actions?
- Privacy lets us remove our public persona
  - You may need to be polite/formal on the job, but you can relax and let your private face show through when you're on your own time.
- Privacy can foster intellectual activities, by allowing us to work without interruption
  - It has been argued that privacy is needed in order to live a creative life, and for spiritual growth
- Privacy has been referred to as “moral capital”, which is used in building deep personal relationships involving respect, love, friendship, and trust

Is there a right to privacy?

- English common law tradition:
  - "A man's home is his castle"
  - Not even the king could enter without probable cause of criminal activity
- US law
  - The right to privacy is considered a "derived right", based on other constitutional guarantees
  - Based on Supreme Court decisions in numerous cases
  - The Third Amendment reflects a privacy interest by prohibiting the government from housing soldiers in the homes of citizens
  - The right of privacy has also been cited as a clear implication of the Fourteenth Amendment, in the "due process" clause
"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."

- 4th Amendment to the U.S. Constitution

"The right to be left alone -- the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."


Disclosing information

• As we go through life, we leave behind a growing electronic trail of our activities
  - Credit card purchases
  - Groceries bought at a discount with loyalty cards
  - Videos rented
  - Calls made with telephones
  - etc.

• Companies collect this data for their own purposes
  - Using it to bill us for services
  - Recommendations for new services, purchases
  - "Mining" it to build profiles for targeted advertising
  - Making it available to other individuals as a part of their services

Example: Amazon Recommendations

Example: Google Phonebook

Some terminology

• Public record
  - Contains information about an incident or action reported to a government agency for the purpose of informing the public
  - Examples: birth certificates, marriage licenses, motor vehicle records, deeds to property, criminal records

• Public information
  - Information that you have provided to an organization that has the right to share it with other organizations
  - We typically do this because we feel the benefit we will derive is worth the cost to us in the form of less privacy
  - Example: a listing in a telephone directory

• Personal information
  - Information that is not public information or part of a public record
  - Once disclosed to an organization that has the right to share it, it becomes public information
Public records

- The federal government maintains thousands of databases containing billions of records about US citizens
- Some examples:
  - Census records
    - Information is supposed to be kept confidential
    - At times of national emergency, this has not been the case
  - Internal Revenue Service records
    - Information about income, assets, charitable organizations that you support, medical expenses...
    - Each year the IRS investigates 100s of employees for misusing access to these records
    - Hundreds of tapes/disks containing income tax data have been misplaced
  - FBI National Crime Information Center (NCIC) 2000
    - 59 million records
    - More than 80,000 law enforcement agencies have access to these files
    - More than 2 million information requests are processed each day, with an average response time of less than 1 second

Some laws governing privacy

- Constitutional protections
- Federal Communications Act (1934)
- Fair Credit Reporting Act (1970, 1995)
- The Privacy Act of 1974
- The Right to Financial Privacy Act (1978)
- Video Privacy Protection Act (1988)
- Health Insurance Portability and Accountability Act (1996)

What about everything else?

- The privacy of most other information is not guaranteed.
  - In 1998, the European Union severely limited the buying and selling of personal data
  - These practices have been generally allowed under U.S. law
  - Companies doing business in both the EU and US must be careful to observe all appropriate laws

Why do we let information go?

- Sometimes we release personal information in order to get a benefit
  - Examples:
    - You must disclose your Social Security number to a bank in order to get a loan
    - You must allow your belongings (and possibly your person) to be searched in order to travel by air
    - If you use TiVo, you’re providing them with detailed information on your viewing habits (and they sell this information, which they monitor down to the second)
  - Sometimes you are forced to release information
    - Example:
      - People called to testify at a trial may be forced to reveal personal information, whether or not they consent

USA PATRIOT Act

- Prompted by terrorist attacks using passenger planes as flying bombs on September 11, 2001
  - Destroyed the World Trade Center
  - Significantly damaged the Pentagon
  - Resulted in ~3,000 deaths
- Shortly after the attacks, Congress passed the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001"

- Patriot Act amended more than 15 existing laws
- Provisions fell into 4 primary categories
  - Provided federal law enforcement and intelligence officials with greater authority to monitor communications
  - Gave the Secretary of the Treasury greater powers to regulate banks, preventing them from being used to launder foreign money
  - Making it more difficult for terrorists to enter the US
  - Defining new crimes and penalties for terrorist activity
- Many provisions are scheduled to expire ("sunset") in 2005
  - Congress will debate whether some/all of them will be reenacted
Patriot Act impacts on privacy

- Various provisions of the Patriot Act have direct impacts on the privacy of persons living within the US
  - Police officers can use pen registers on the Internet to track email addresses and URLs, without demonstrating probable cause
  - Jurisdiction for court-ordered wiretaps was extended over the entire country (e.g., judges in NY could authorize a tap in CA)
  - The circumstances under which "roving surveillance" is allowed were broadened
  - Allows courts to authorize searches of a person's premises without first serving a warrant, and officers may seize property that "constitutes evidence of a criminal offense" (even if the offense is unrelated to terrorism)
  - Makes it easier for the FBI to collect business, medical, educational, library, and church/mosque/synagogue records
- Some are concerned that these items violate the 4th Amendment

Patriot Act II proposal

- Draft of the Domestic Security Enhancement Act of 2003 was leaked to the press in Feb, 2003
  - Dubbed "Patriot Act II" by the press
  - Many objections were raised (unlike for Patriot Act)
  - Congress adjourned at the end of 2003 without passing this act
- Intended to grant additional new powers to the government:
  - The ability to expatriate American citizens "convicted of giving material support to a group that's designated a terrorist organization" (even if the offense is unrelated to terrorism)
  - The ability to keep the names of people being held on suspicion of terrorism secret
  - Allowing law enforcement officers to obtain access to records held by ISPs, doctors, family members, or friends on the basis of administrative subpoenas
  - The right to collect DNA samples from suspected terrorists and to create a national DNA database accessible by federal, state, and local law enforcement
  - The right for police to wiretap suspects and intercept their email for 15 days without obtaining a warrant

National ID card controversy

- There has long been debate over the need for a national ID card
  - Initial legislation concerning the Social Security Number specified that it could not be used for identification purposes
  - In 1971, the Social Security Administration task force on the SSN rejected the extension of the SSN to the status of an ID card.
  - In 1973, the Health, Education and Welfare (HEW) Secretary's Advisory Committee on Automated Personal Data Systems concluded that a national identifier was not desirable.
  - In 1976, the Federal Advisory Committee on False Identification rejected the idea of an identifier.
  - In 1981, the Reagan Administration stated that it was "explicitly opposed" to the creation of a national ID card.
- The events of September 11, 2001 renewed the debate, and changed some of the terms on which it took place

Arguments made by those in favor of national ID cards include:
- We currently rely on second-rate identification methods, such as SSNs and driver's licenses: more modern cards could include fingerprints or other biometrics, making them harder to forge
- It would make it much more difficult for people to enter the US illegally, helping to prevent terrorist attacks
- Requiring employers to check the ID card would prevent illegal aliens from working in the US
- Giving police the ability to positively identify people would reduce crime
- Many democratic countries already use national ID cards, including Belgium, France, Germany, Greece, Luxembourg, Portugal, and Spain

Arguments made by those opposing the use of national ID cards include:
- A national ID card does not guarantee that the apparent identity of an individual is that person's actual identity
- It is impossible to create a biometric-based national ID card that is 100% accurate
- There is no evidence that the institution of a national ID card actually leads to a reduction in crime
- A national ID card makes it simpler for government agencies to perform data mining on the activities of its citizens
- While most people feel that they have nothing to fear from a national identification card system, since they are law-abiding citizens, even law-abiding people are subject to fraud and the indiscretions and errors of others

Some discussion questions
Logistics

• Project
  - Part 4 (clock variant) due Sunday, Nov 13th
  - Individual submission
  - Recommended: Submit by Nov 6th

• Scoring
  - Functionality (10)
  - Use of framework (5)
  - Code Style (5)
  - Memory Management (5)

• Questions?

Logistics

• Final exam
  - Good news...bad news
  - Good news
    - Last day of finals, November 18th
    - Bad news
      - 8am-10am
      - Room
        • 01-3338

• Final Exam Review
  - Tuesday, November 15th
    - 5-6pm
    - 70-1400

• Final Exam

Some links on national ID Card


• Critics of grocery club cards give examples of card-member prices being equal to the regular prices at stores without customer loyalty programs. (In other words, those without a card, or who don’t want to use it are charged extra fees.) Is it fair for a store to charge us more if we don’t want to use its loyalty card? Explain your reasoning.

• Some consumers give phony personal information when they apply for rewards/loyalty cards at stores. Others take it a step further by regularly exchanging their cards with those held by other people. Are these people doing anything wrong? Why?

• In a recent study, people in subway stations were ordered a cheap pen in return for disclosing their passwords. About 90 percent offered their passwords in return for the pen.

  Do people really value privacy?

• Think about what you do when you get up in the morning. How would you act differently if you knew that you were being watched? Would you feel uncomfortable? Do you think you would get used to being watched?
• Take a side (pro and con) on the debate that every citizen of the US ought to carry a national ID card.

• The Dept. of Homeland Security is interested in using computers to identify suspected terrorists operating within the US.
  - It would like to mine databases containing information about purchases and travel to detect patterns that may identify individuals who are engaged in (or planning) terrorist activities.
  - The Dept. asks a panel of computer scientists to determine the feasibility of this project, and a panel member suggests that the most difficult problem will be determining what patterns of transaction to look for.
  - It is further suggested that it might be possible to construct a computer program that uses AI to mimic a terrorist organization. The program would determine the actions needed to execute an act of terror; once these actions are identified, it would be possible to search database records to find evidence of these actions.

• Debate:
  - the wisdom of developing a computer program capable of planning the steps needed to execute an act of terror
  - the ethics of the Department's plan for mining commercial databases for the purpose of detecting potential terrorists' patterns

Some additional resources

• Right to privacy:
  - http://www.fontanalib.org/Constitutional%20Origin%20of%20the%20Right%20to%20Privacy.html
  - http://www.ala.org/ala/washoff/oidt/emailtutorial/privacya/05.html

• National ID cards:
  - http://www.epic.org/privacy/id_cards/
  - http://www.privacy.org/pl/activities/id_card/
  - http://www.time.com/time/nation/article/0,8599,181857,00.html
    - "The national ID card that isn't, yet"

• Privacy issues
  - http://www.aclu.org/Privacy/Privacylist.cfm?c=130
  - http://www.privacy.org/