Chapter Overview

- Introduction
- Perspectives on privacy
- Information disclosures
- Data mining

What Is Privacy?

“Privacy is the claim of Individuals, Groups, or Institutions to determine for themselves when, how, and to what extent information about them is communicated to others”

- Alan Westin, Privacy and Freedom, 1967

Privacy is not absolute
We disclose, and we keep private

Privacy as a process

“Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication...”

- Alan Westin, 1967

Ways to protect privacy

There are four basic ways to protect privacy:

- Technology
- Law
- Markets
- Your choices as an individual

Types of privacy harm

Four categories of privacy harms:

- Intrusions
- Information collection
- Information processing
- Information dissemination

Intrusion

They come into your space and contact you, or tell you what to do.
Examples:

- Spam
- Unwanted phone calls
  - Technology: caller ID
  - Law: National Do Not Call List
- Parents entering a teens room without knocking
- Government saying what you can or can't do with your own body or property.
### Information Collection

They watch what you are doing more than they should.

**Surveillance and Interrogation**
- Visual, such as peeping toms
- Communications such as wiretapping your phone or email
- Government, employers, or parents ask you private information

### Information Processing

They have a lot of data, and do things with it

- **Identification** – they learn about your anonymous actions
- **Data mining** – they use patterns to determine if you are a good customer or a suspected terrorist
- **Exclusion** – they decide you are not a good potential employee or customer, or go on the no-fly list
- **Secondary use** – they collect information for one reason, but use it for others

### Information Dissemination

They disclose data, perhaps more than you think that they should

- **Breach of confidentiality** – doctors or lawyers
- **Transfer to third parties** – a company or government shares data about you to persons that you do not expect
- **Public exposure of private facts** – an intimate photo, of disclosure of intimate facts
- **Disclosure of untrue facts** – represent you in a false light
- **Appropriation** – they use your name or picture without your permission.

### Information Technology Erodes Privacy

- Information collection, exchange, combination, and distribution easier than ever means less privacy
- Scott McNealy: “You have zero privacy anyway. Get over it.”
- We will consider how we leave an “electronic trail” of information behind us and what others can do with this info

### 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?
<table>
<thead>
<tr>
<th>Harms of Privacy</th>
<th>Benefits of Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cover for illegal or immoral activities</td>
<td>• Individual growth</td>
</tr>
<tr>
<td>• Burden on the nuclear family</td>
<td>• Individual responsibility</td>
</tr>
<tr>
<td>• Hidden dysfunctional families</td>
<td>• Freedom to be yourself</td>
</tr>
<tr>
<td>• Ignored people on society’s fringes</td>
<td>• Intellectual and spiritual growth</td>
</tr>
<tr>
<td></td>
<td>• Development of loving, trusting, caring, intimate relationships</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Is There a Natural Right to Privacy?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Privacy rights stem from property rights: “a man’s home is his castle”</td>
</tr>
<tr>
<td>• Coercive Acts before American Revolution led to 3rd Amendment to U.S. Constitution</td>
</tr>
<tr>
<td>- No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.</td>
</tr>
<tr>
<td>• Samuel Warren and Louis Brandeis: People have “the right to be let alone”</td>
</tr>
<tr>
<td>• Judith Jarvis Thomson: “Privacy rights” overlap other rights</td>
</tr>
<tr>
<td>• Conclusion: Privacy is not a natural right, but it is a prudential right</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Privacy and Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Perhaps modern life is actually more private than life centuries ago</td>
</tr>
<tr>
<td>- Most people don’t live with extended families</td>
</tr>
<tr>
<td>- Automobile allows us to travel alone</td>
</tr>
<tr>
<td>- Television v. public entertainment</td>
</tr>
<tr>
<td>• Challenge: we now live among strangers</td>
</tr>
<tr>
<td>• Remedy: establishing reputations</td>
</tr>
<tr>
<td>- Ordeal, such as lie detector test or drug test</td>
</tr>
<tr>
<td>- Credential, such as driver’s license, key, ID card, college degree</td>
</tr>
<tr>
<td>• Establishing reputation is done at the cost of reducing privacy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case Study: Secret Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Sullivans have a baby girl</td>
</tr>
<tr>
<td>• Both work; they are concerned about performance of full-time nanny</td>
</tr>
<tr>
<td>• Purchase program that allows monitoring through laptop’s camera placed in family room</td>
</tr>
<tr>
<td>• They do not inform nanny she is being monitored</td>
</tr>
<tr>
<td>• Ethical?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule Utilitarian Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• If everyone monitored nannies, it would not remain a secret for long</td>
</tr>
<tr>
<td>• Consequences</td>
</tr>
<tr>
<td>- Nannies would be on best behavior in front of camera</td>
</tr>
<tr>
<td>- Might reduce child abuse and increase parents’ peace of mind</td>
</tr>
<tr>
<td>- Would also increase stress and reduce job satisfaction of child care providers</td>
</tr>
<tr>
<td>- Might result in higher turnover rate and less experienced pool of nannies, who would provide lower-quality care</td>
</tr>
<tr>
<td>• Harms appear greater than benefits, so we conclude action was wrong</td>
</tr>
</tbody>
</table>
Social Contract Theory Evaluation

- It is reasonable for society to give people privacy in their own homes
- Nanny has a reasonable expectation that her interactions with baby inside home are private
- Sullivan's decision to secretly monitor the nanny is wrong because it violates her privacy

Kantian Evaluation

- Imagine rule, "An employer may secretly monitor the work of an employee who works with vulnerable people"
- If universalized, there would be no expectation of privacy by employees, so secret monitoring would be impossible
- Proposed rule is self-defeating, so it is wrong for Sullivans to act according to the rule

Summary

- Three analyses have concluded Sullivans were wrong to secretly monitor how well their nanny takes care of their baby
- Morally acceptable options
  - Conduct more comprehensive interview of nanny
  - More thoroughly check nanny’s references
  - Spend a day or two at home observing nanny from a distance
  - Be up-front with nanny about desire to install and use surveillance software on laptop

Is there such a thing as Privacy?

Public Records

- Public record: information about an incident or action reported to a government agency for purpose of informing the public
- Examples: birth certificates, marriage licenses, motor vehicle records, criminal records, deeds to property
- Computerized databases and Internet have made public records much easier to access

Records Held by Private Organizations

- Credit card purchases
- Purchases made with loyalty cards
- Voluntary disclosures
- Posts to social network sites
# Data Gathering and Privacy Implications

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

## Facebook Tags

- **Tag**: Label identifying a person in a photo
- Facebook allows users to tag people who are on their list of friends
- About 100 million tags added per day in Facebook
- Facebook uses facial recognition to suggest name of friend appearing in photo
- Does this feature increase risk of improper tagging?
- Do the people being tagged have a right to privacy?

## Enhanced 911 Services

- Cell phone providers in United States required to track locations of active cell phones to within 100 meters
- Allows emergency response teams to reach people in distress
- What if this information is sold or shared?
- Should parents be allowed to track their children?
- Should employers be allowed to track their employees?

## Rewards or Loyalty Programs

- Shoppers who belong to store’s rewards program can save money on many of their purchases
- Computers use information about buying habits to provide personalized service
  - ShopRite computerized shopping carts with pop-up ads
- Do card users pay less, or do non-users get overcharged?
- Would you be happy if your shopping preferences were made public?

## Body Scanners

- Some department stores have 3-D body scanners
- Computer can use this information to recommend clothes
- Scans can also be used to produce custom-made clothing
- Controversy: TSA using 3-D scanners in airports.
  - Should this be an issue?

## RFID Tags

- **RFID**: Radio frequency identification
- An RFID tag is a tiny wireless transmitter
- Manufacturers are replacing bar codes with RFID tags
  - Contain more information
  - Can be scanned more easily
- If tag cannot be removed or disabled, it becomes a tracking device
## Implantied Chips

- Taiwan: Every domesticated dog must have an implanted microchip
  - Size of a grain of rice; implanted into ear
  - Chip contains name, address of owner
  - Allows lost dogs to be returned to owners
- RFID tags approved for use in humans
  - Can be used to store medical information
  - Can be used as a “debit card”

## OnStar

- OnStar manufactures communication system incorporated into rear-view mirror
- Emergency, security, navigation, and diagnostics services provided subscribers
- Two-way communication and GPS
- Automatic communication when airbags deploy
- Service center can even disable gas pedal

## Automobile “Black Boxes”

- Modern automobiles come equipped with a “black box”
- Maintains data for five seconds:
  - Speed of car
  - Amount of pressure being put on brake pedal
  - Seat belt status
- After an accident, investigators can retrieve and gather information from “black box”
- What would happen if Insurance companies had access to the data from your car?

## Medical Records

- Advantages of changing from paper-based to electronic medical records
- Quicker and cheaper for information to be shared among caregivers
  - Lower medical costs
  - Improve quality of medical care
- Once information in a database, more difficult to control how it is disseminated
- What happens when the information is disclosed (insurance company, employer)?

## Digital Video Recorders

- TiVo service allows subscribers to record programs and watch them later
- TiVo collects detailed information about viewing habits of its subscribers
- Data collected second by second, making it valuable to advertisers and others interested in knowing viewing habits

## Cookies

- Cookie: File placed on computer's hard drive by a Web server
- Contains information about visits to a Web site
- Allows Web sites to provide personalized services
- Put on hard drive without user's permission
- You can set Web browser to alert you to new cookies or to block cookies entirely
- Servers can query browser to see where you have been.
Flash Cookies

• Flash cookie: File placed on your computer’s hard drive by a Web server running the Adobe Flash Player
• Flash cookie can hold 25 times as much information as a browser cookie
• Flash cookies not controlled by browser’s privacy controls
• Some Web sites use flash cookies as a way of backing up browser cookies. If you delete browser cookie, it can be “respawned” from the flash cookie
• Half of 100 most popular Web sites use flash cookies

Data Mining

• Searching records in one or more databases, looking for patterns or relationships
• Can be used to create profiles of individuals
• Allows companies to build more personal relationships with customers

Google’s Personalized Search

• Secondary use: Information collected for one purpose used 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

Secondary Uses of Information

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

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
**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

**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

**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

**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

**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

**Social Network Analysis**

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

https://www.forbes.com/sites/cognitiveworld/2019/04/05/how-privacy-laws-are-changing-to-protect-personal-information/#3e3dbc52753d

Scenario

A student receives a midterm deficiency in a course. Parents receive a letter informing them of the deficiency. Student (and individually the parents) contact instructor asking why deficiency was issued.

Can the instructor disclose any information to the parents?

Amazon policy

Original Amazon policy:
We are committed to protecting your privacy. We use the information we collect on the site to make shopping at Amazon.com possible and to enhance your overall shopping experience. We do not sell, trade, or rent your personal information.

Amazon policy

New Amazon policy:
Business transfers: As we continue to develop our business, we might sell or buy stores or assets. In such transactions, customer information generally is one of the transferred business assets. Also, in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred assets.

Amazon policy

Automatic Information: Examples of the information we collect and analyze include the Internet protocol (IP) address used to connect your computer to the Internet; login; e-mail address; password; computer and connection information such as browser type and version, operating system, and platform; purchase history; the full Uniform Resource Locators (URL) clickstream to, through, and from our Web site, including date and time; cookie number; products you viewed or searched for; zShops you visited; your Auction history; and phone number used to call our 800 number.

Amazon policy

In addition to the policy changes, Amazon announced that it no longer allowed new customers to opt-out of arrangements that shared their data with other companies or third parties.

“Amazon says such restrictions on data-sharing would impede its budding partnerships with outfits such as toy merchant Toys R Us and Drugstore.com”
Amazon

Should Amazon be allowed to treat customer data as an asset in the case of bankruptcy?
Should users be allowed to opt-out of this practice (prevent their data from being sold off if the company slides into bankruptcy)?