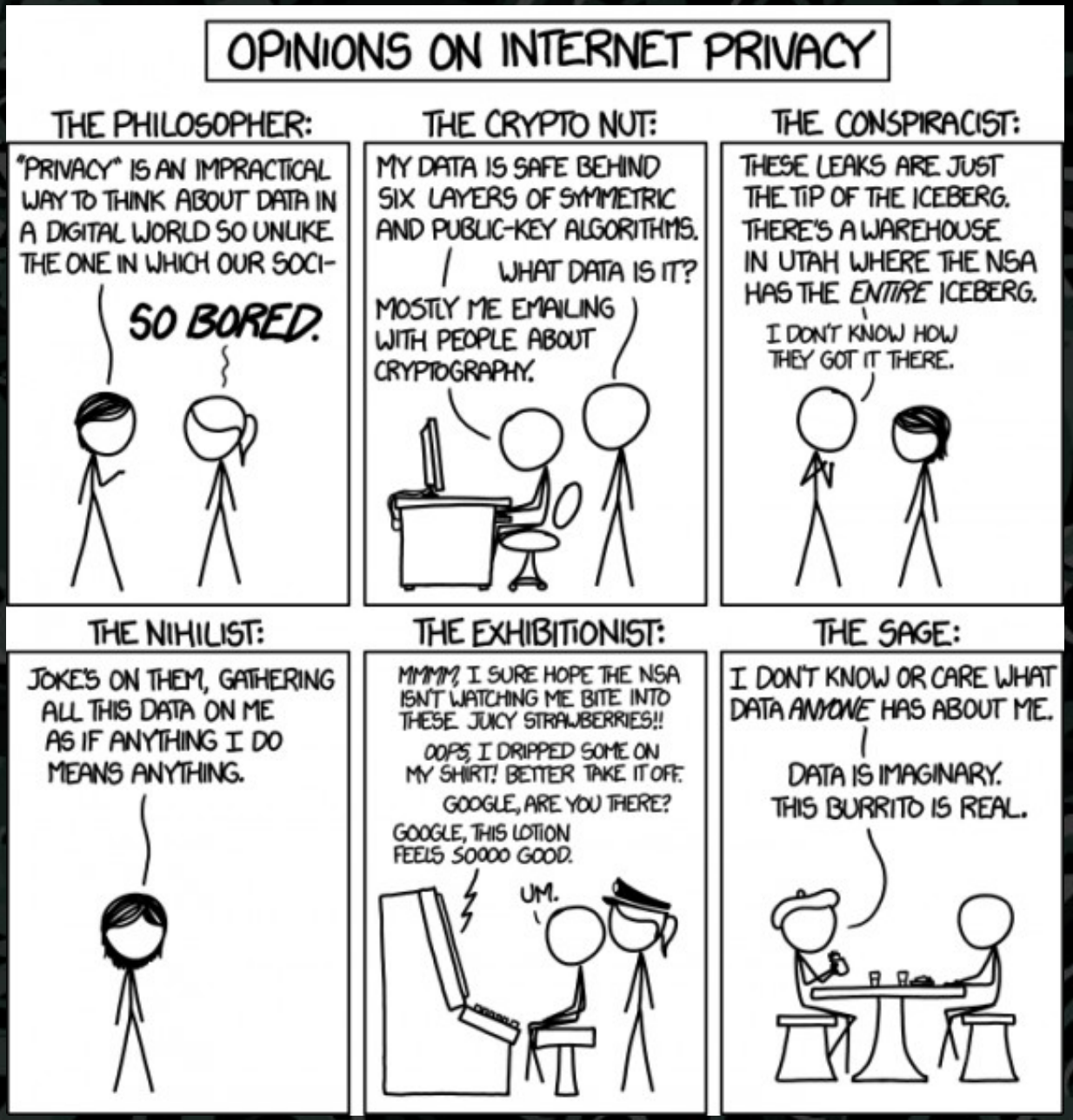
Lecture 8.1 Information Privacy



CS 230: Ethical Issues in Computing
Fall 2020
Dr. Henderson
BSU

Announcements

- Syllabus 1.6
  - Base grade changes
  - LA work updated
- LA-6 due Thursday
  - Quiz threshold adjusted to 84% (3 incorrect)
  - Short answer – 3 different licenses

Last Time

- Software licenses and EULAs
- Open Source Software (OSS)
  - FSF vs. OSI
- Creative Commons
-

Today

- What is privacy, especially in today's world?
- Information Disclosure
  - Voluntary vs. Mandatory
- Data Mining
- Consumer Backlash
- Best practices

Is There a Natural Right to Privacy?

- Judith Jarvis Thomson
  - Nobody seems to know what privacy is
  - Problems with defining privacy as “the right to be let alone”
    - On the one hand, definition is too narrow – doesn’t include covert spying
    - On the other hand, definition is too broad – does include assault
  - Whenever a right to privacy is violated, another right is violated as well
  - Therefore, no need to define privacy or privacy rights precisely
- Privacy is not a **natural** right, but it is **prudential** right
  - Rational people agree to recognize some privacy rights because granting these rights benefits society

The Circle

- Earlier societies had less privacy
  - Small villages, everyone knew each other
  - Strangers, criminals harder to be anonymous
- What would that look like today?


SoulSearch

Information Technology Erodes Privacy

- Computers, databases, and Internet enable ever-improving information
  - collection
  - exchange
  - combination
  - distribution
- Easier than ever to get information about others, including total strangers
- Is privacy important? If so, can we protect it?

The Circle

- Scott McNealy: “You have zero privacy anyway. Get over it.”

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

Information 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
- R F I D tags
- Implanted chips
- Mobile apps
- Facebook Login
- OnStar
- Automobile “black boxes”
- Medical records
- Digital video recorders
- 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?

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?

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?

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

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

Implanted 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”

Mobile Apps

- Many apps on Android smartphones and iPhones collect location information and sell it to advertisers and data brokers
  - Angry Birds
  - Brightest Flashlight
- Flurry: a company specializing in analyzing data collected from mobile apps
  - Has access to data from > 500,000 apps

Facebook Login

- Allows people to login to Web sites or apps using their Facebook credentials
- App's developer has permission to access information from person's Facebook profile: name, location, email address, and friends list

OnStar

- OnStar manufactures communication system incorporated into rear-view mirror
- Emergency, security, navigation, and diagnostics services provided subscribers
- Two-way communication and G P S
- 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”

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

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

General Data Protection Regulation

- General Data Protection Regulation (GDPR): set of rules governing collection of information from citizens of European Union
- Requires companies to…
  - Disclose information they are seeking to collect
  - Disclose why they are collecting it
  - Get permission before collecting it
- Responding to GDPR, most large American companies are adopting new privacy guidelines
  - Web-site banners informing users, asking for consent

GDPR Sample

Right of Access According to article 15 of the General Data Protection Regulation (GDPR) you have the right to demand a confirmation from our side, stating whether we are processing personal data concerning you. If that is the case, you are entitled to intelligence about these personal data and to further information, as stated in article 15 of the General Data Protection Regulation (GDPR)

Right to Rectify According to article 16 of the General Data Protection Regulation (GDPR) you are entitled to demand of us to rectify any incorrect personal data concerning you with no delay. With regard to the processing purposes you are also entitled to demand incomplete personal data to be completed – also by an additional statement.

Right to Erasure You have the right to demand of us to delete your personal data with no delay. We are obligated to delete any personal data immediately, if the relevant conditions according to article 17 of the General Data Protection Regulation (GDPR) are met. For details, we would like to refer you to article 17 of the General Data Protection Regulation (GDPR).

Right to Restrict the Processing According to article 18 of the General Data Protection Regulation (GDPR) you are entitled to demand of us to limit the processing of your personal data, provided certain pre-conditions are met.

Right of Data Portability According to article 20 of the General Data Protection Regulation (GDPR) you are entitled to receive your personal data you have provided to us in a structured, established and machine-readable format. You are also entitled to transfer the data to another responsible party without any hinderance from our side, provided the processing is based on any agreement based on article 6 paragraph 1 letter a, or article 9 paragraph 2 letter a, or on a contract according to article 6 paragraph 1 letter b, and the transfer is done via automated tools.

Right to Object According to article 21 of the General Data Protection Regulation (GDPR) you are entitled to object against your personal data's processing based on article 6 paragraph e or f of the General Data Protection Regulation (GDPR). This does also apply for profiling based on these regulations.

If we are processing your personal data for direct advertisement, you have the right to object to the processing of your personal data for the use of such advertisement at any time. This does also apply to profiling, if it is connected to such advertisement.

If you would like to exercise any of the rights you are entitled to, please contact us as the responsible party via the contact data given above, or use any of the other ways of contact provided to notify us. If you have any questions regarding this, please contact us.

Existence of a Right of Appeal to the Supervisory Authority According to article 77 of the General Data Protection Regulation (GDPR) you are entitled to the right of appeal to the supervisory authority without prejudice to any wider administrative or judicial remedy. This right applies particularly within the member state of your abode, of your working place or of the suspected contravention, if you consider the processing of your personal data to be a violation of the General Data Protection Regulation (GDPR).

Global Privacy Control

- A group of tech companies, publishers, and activist groups including the Electronic Frontier Foundation, Mozilla, and DuckDuckGo are backing a new standard to let internet users set their privacy settings for the entire web.

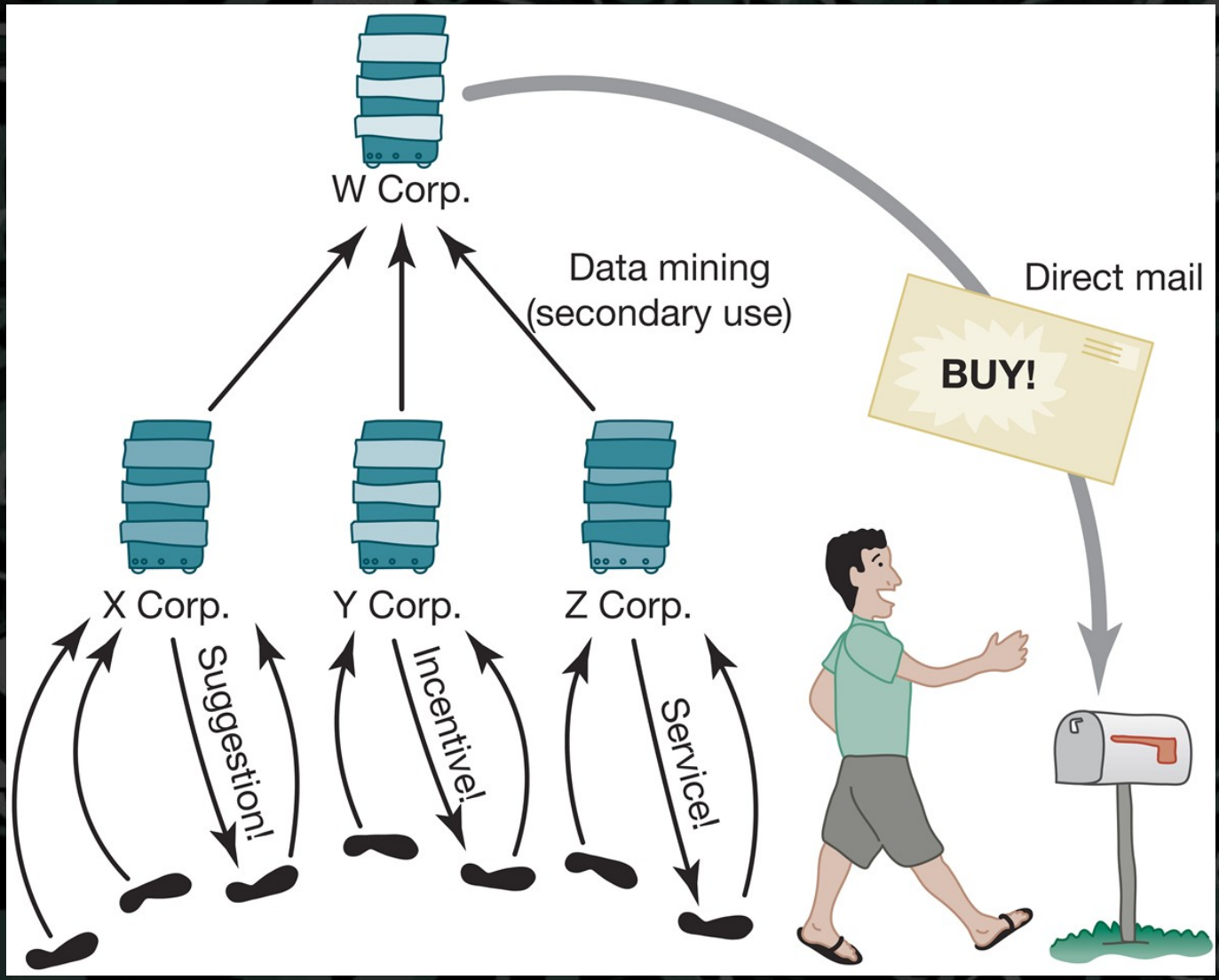
Data Mining

- 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



Limiting Information Google Saves

- You can limit amount of information Google saves about your activities
- Privacy Checkup lets you pause collection of personal information
  - Search queries and other Google activity
  - Location information collected from signed-in devices
    - Where you have gone
    - How often you have gone there
    - How long you have stayed
    - Customary routes of travel
  - Contact and calendar information
  - Recordings of your voice and accompanying audio
  - YouTube search queries
  - YouTube videos you have watched

Collaborative Filtering

- Form of data mining
- Analyze information about preferences of large number of people to predict what one person may prefer
  - Explicit method: ask people to 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

“Target”-ing Pregnant Women

- Most people keep shopping at the same stores, but new parents have malleable shopping habits
- Targeting pregnant women a good way to attract new customers
- Target did data mining to predict customers in second trimester of pregnancy
  - Large amounts of unscented lotion, extra-large bags of cotton balls, nutritional supplements
- Mailings included offers for unrelated items with offers for diapers, baby clothes, etc.

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

Targeted Direct Mail

- Businesses mail advertisements only to those most likely to purchase products
- Data brokers provide customized mailing lists created for information gathered online and offline
- Example of making inferences for targeted direct mail
  - Shopping for clothes online + frequent fast-food dining + subscribing to premium cable TV channels → more likely to be obese
- Two shoppers visiting same site may pay different prices based on inferences about their relative affluence

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

Social Network Analysis

- Collect information from social networks to inform decisions
- Bharti Airtel (India) offers special promotions to “influencers”
- Police use Facebook and Twitter posts to deploy officers on big party nights
- Banks combine social network data with credit reports to determine creditworthiness

Controlling Your Facebook Info

- You can change your Facebook settings to minimize who can see what you're doing
- Privacy settings
  - Who can see your friends list?
  - Who can see your future posts?
  - Who can look you up using your email address?
  - Who can look you up using your phone number?
  - Do you want search engines to link to your profile?
  - Limit audience for posts you've shared?

Controlling Your Facebook Info

- Timeline and Tagging
  - Who sees tag suggestions when photos look like you?
  - Review posts you're tagged in?
  - Review tags people add to your posts?
- Location History
- Ads – Based on
  - Relationship status
  - Employer
  - Job title
  - Education
  - Data from partner
  - Activity on Facebook Company Products
  - Social actions

Anonymized Data Sets

Netflix Prize

- Netflix offered $1 million prize to any group that could come up with a significantly better algorithm for predicting user ratings (2006)
- 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 (2010)

AOL Search Dataset

- AOL researcher Dr. Chowdhury posted three months' worth of user queries from 650,000 users (2006)
- No names used; random integers used to label all queries from particular users
- Researchers identified some users from queries; e.g., many people performed searches on their own names
- New York Times investigation led to public outcry
- AOL took down dataset, but already copied and reposted
- AOL fired Dr. Chowdhury and his supervisor

Backlash

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

- 2007: Facebook announced Beacon, a targeted advertising device
  - Facebook user makes purchase
  - Facebook broadcasts purchase to user's friends
  - Based on opt-out policy: users enrolled unless explicitly asked to be excluded
- A significant source of advertising revenue for Facebook
- MoveOn.org led online campaign lobbying Facebook to switch to an opt-in policy
- Mark Zuckerberg apologized, and Facebook switched to an opt-in policy

Malls Track Shoppers' Cell Phones

- In 2011 two malls recorded movement of shopper by tracking locations of cell phones
  - How much time people spend in each store?
  - Do people who shop at X also shop at Y?
  - Are there unpopular areas of mall?
- Small signs informed shoppers of study
- After protest, mall quickly halted study

iPhone Apps Upload Address Books

- In 2012 a programmer discovered Path was uploading iPhone address books without permission
- Internet community pointed out this practice violated Apple’s guidelines
- CEO of Path apologized; app rewritten
- Twitter, Foursquare, and Instagram also implicated for same practice

Instagram's Proposed Change to Terms of Service

- Late 2012: Instagram announced changes
  - Privacy policy
  - Terms of service
- Legal experts: Instagram and Facebook would have right to use photos in ads without permission
- Instagram C E O: New policy misunderstood
- Changed advertising section of terms of service agreement back to original version

Tools

- Osintframework.com

Best Practices

- Be very stingy with personal information
  - Use a “need-to-know” basis
- Most online forms cast a wide net but only require a narrow response
- Create alter-egos for security questions
- Be very careful with SSN
- Adjust privacy settings on social accounts

Summary

- Modern information technology makes it much easier to collect and transmit information
- Privacy a balancing act
  - Desires of individuals
  - Profit motives of companies
  - Common good
- Public records: information that communities have decided should be known to all
- Sometimes must share personal information to get something we want
  - Disclose income tax statements to get a home loan
- Companies collect more information to market more selectively – some have pushed the boundaries of what society will tolerate