


# CS 4873: Computing, Society & Professionalism

Munmun De Choudhury | Assistant Professor | School of Interactive Computing

Week 6: Privacy II  
February 12, 2020



# Perspectives on Privacy



\* Today's Class – why violation of privacy is an ethical challenge



# Class Discussion 1: Secret Monitoring

# Rule Utilitarian Evaluation

- If everyone monitored nannies, it would not remain a secret for long
- Consequences
  - Nannies would be on best behavior in front of camera
  - Might reduce child abuse and parents' peace of mind
  - Would also increase stress and reduce job satisfaction of child care providers
  - Might result in higher turnover rate and less experienced pool of nannies, who would provide lower-quality care
- Harms appear greater than benefits, so we conclude action was wrong

# 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
- The parents' 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 the parents 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





# Information Disclosures

# 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

# Data Gathering and Privacy Implications

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



But where to draw the line?

# 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?

# Facebook Tags

- Facebook allows users to tag people who are on their list of friends
- New feature from couple of years ago – automatic tagging
- 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?

# 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
- Can body scanners be misused?

# 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”
- What kind of privacy violations are possible with implanted chips?



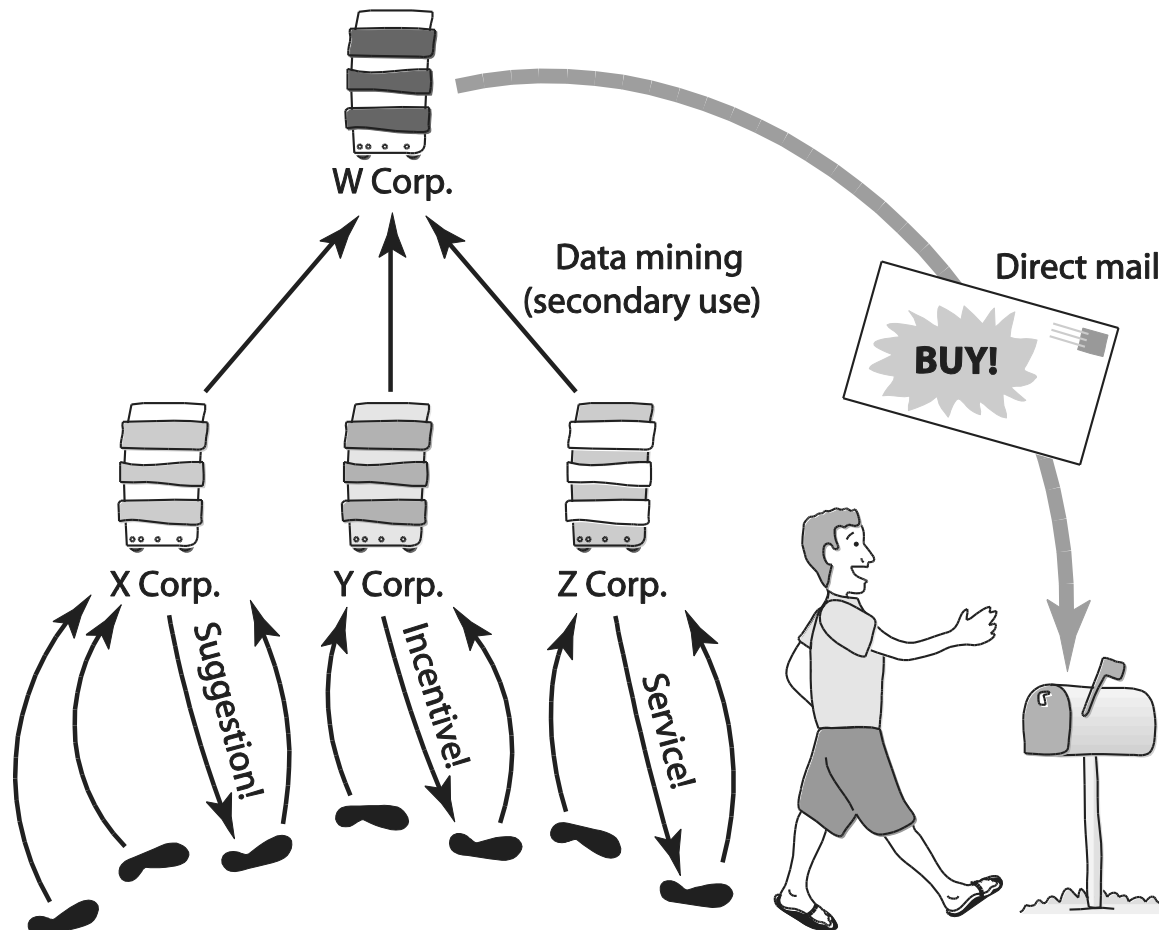



# AI/Machine Learning

# AI/Machine Learning

- Searching records in one or more databases, looking for patterns or relationships
- Can be used to profile individuals
- Allows companies to build more personal relationships with customers

# Secondary Uses of Information





How is secondary information  
used? Some examples...

# Google's Personalized Search

- Secondary use: Information collected for one purpose use 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

# 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

# Microtargeting

- Started before 2004 US Presidential elections
- 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

# 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



# How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

- “[Pole] ran test after test, analyzing the data, and before long some useful patterns emerged. Lotions, for example. Lots of people buy lotion, but one of Pole’s colleagues noticed that women on the baby registry were buying larger quantities of unscented lotion around the beginning of their second trimester. Another analyst noted that sometime in the first 20 weeks, pregnant women loaded up on supplements like calcium, magnesium and zinc.”
- As Pole’s computers crawled through the data, he was able to identify about 25 products that, when analyzed together, allowed him to assign each shopper a “pregnancy prediction” score.
- More important, he could also estimate her due date to within a small window, so Target could send coupons timed to very specific stages of her pregnancy.

# Class Discussion

- If you voluntarily have your body scanned at a departmental store, who should own that information: you or the store?
- Should the store have the right to sell your body measurements to other business? Explain your reasoning.



# Sharing of Anonymized Datasets

POLICY —

# “Anonymized” data really isn’t—and here’s why not

Companies continue to store and sometimes release vast databases of " ...

NATE ANDERSON - 9/8/2009, 7:25 AM



The Massachusetts Group Insurance Commission had a bright idea back in the mid-1990s—it decided to release "anonymized" data on state employees that showed every single hospital visit. The goal was to help researchers, and the state spent time removing all obvious identifiers such as name, address, and Social Security number. But a graduate student in computer science saw a chance to make a point about the limits of anonymization.

Latanya Sweeney requested a copy of the data and went to work on her "reidentification" quest. It didn't prove difficult. Law professor Paul Ohm describes Sweeney's work:

“


At the time GIC released the data, William Weld, then Governor of Massachusetts, assured the public that GIC had protected patient privacy by deleting identifiers. In

# 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
  - Movie ratings predicted political leanings and sexual orientation
- U.S. Federal Trade Commission complaint and lawsuit
- Netflix canceled sequel to Netflix Prize

# AOL Search Dataset

- In 2006, AOL research team released three months worth of search queries from 650K AOL users
  - Support university research
- Anonymization using a random integer identifier for each user
- But aggregation of queries by a single identifier revealed a lot about the person, even without PII
- Queries also contained personal info – address, SSN
- NYT identified several of the users
- Following public backlash, the dataset was taken down after 3 days
- Where did AOL go wrong?



Almost all information can be “personal”  
when combined with enough other  
relevant bits of data




\* Privacy from the Individual  
Perspective (Acquisti et al 2015)

What should the individual be doing?



# \* Individualistic Approach – privacy is a private good

- Trust people's ability to make self-interested decisions
  - The “Get over it” brigade
  - Zuckerbollocks – privacy is a private good (O'Hara 2013)



\* Are individuals up to the challenge of navigating privacy in the information age?

# Privacy as a public good?

- Even when the individual would rather be transparent and open to scrutiny, exposure will affect others.
- Accountability
- Profiling
- Security
- Trading data and market efficiency
- Chilling effects

# Is policy/regulation the solution?

- With respect to the individualistic approach, scholars question people's ability to manage privacy amid increasingly complex trade-offs
  - Choice and consent are not always an option
  - Regulatory intervention may be needed

# \* EU's "Right to be Forgotten"

- Also known as the "right to erasure", the rule gives EU citizens the power to demand data about them be deleted.

← → ↻ 🔒 [newyorker.com/magazine/2014/09/29/solace-oblivion](http://newyorker.com/magazine/2014/09/29/solace-oblivion)

Subscribe for \$4 a month.

THE  
NEW YORKER

ANNALS OF LAW SEPTEMBER 29, 2014 ISSUE

## THE SOLACE OF OBLIVION

*In Europe, the right to be forgotten trumps the Internet.*



By Jeffrey Toobin

September 22, 2014

# EU's "Right to be Forgotten"

- Google had argued that the obligation could be abused by authoritarian governments trying to cover up human rights abuses were it to be applied outside of Europe.

 [bbc.com/news/technology-49808208](https://www.bbc.com/news/technology-49808208)

## Technology

# Google wins landmark right to be forgotten case

By Leo Kelion  
Technology desk editor

 24 September 2019



 Share

# Privacy as a public good

- Need to balance the interests of the subjects of data against the power of commercial entities and governments holding that data