

CS 4873-A: Computing and Society


Munmun De Choudhury | Associate Professor | School of Interactive Computing



Week 6: Privacy

February 21, 2021





With your permission, you give us more permission. If you give us information about who some of your friends are, we can probably use some of that information, again, with your permission, or improve the quality of our searches. We don't need you to type at all, because we know where you are, with your permission. We know where you have been, with your permission. We can more or less guess what you are thinking about. – *Eric Schmidt, Google CEO (The Atlantic)*

Technology Erodes Privacy

- Information collection, exchange, combination, and distribution easier than ever means less privacy
- Scott McNealy (Sun Microsystems) in 1999: “You have zero privacy anyway. Get over it.”
- Zuckerberg in 2010 said that the social norm is to share everything, so people are little concerned about their privacy.



Perspectives on Privacy

An Old Definition of Privacy

- Privacy rights have evolved from property rights: “a man’s home is his castle”; no one should be allowed in without permission
- Privacy: “right to be left alone”
 - Samuel Warren (Harvard graduate businessman) and Louis Brandeis (Boston attorney; later Supreme Court justice)
 - Influential paper from 1890
- This led to 3rd Amendment to U.S. Constitution – principle of home as a sanctuary in the Bill of Rights:

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.

Is There a Natural Right to Privacy?

- Judith Jarvis Thomson: the definition of privacy as “the right to be left alone” is problematic
 - Smith being monitored at his home with a video camera without his knowledge – he is left alone technically, but it is a privacy violation
- Judith Jarvis Thomson: “Privacy rights” overlap other rights; violation of privacy is often a violation of some other right in this cluster
- *Conclusion: Privacy is not a natural right, but it is a prudential right*

Modern Definition of Privacy

- Privacy is a “zone of inaccessibility”
- Privacy related to notion of access
 - Privacy is not “being alone”, but defining who has access to what
- Access
 - Physical proximity to a person
 - Knowledge about a person
- Regarding access – where to draw the line between private and public
- *Privacy is a social arrangement that allows individuals to have some level of control over who is able to gain access to their physical selves and their personal information*

Alternative Definitions of Privacy


- Privacy violations are an affront to human dignity
 - You violate privacy when you treat a person as a means to an end.
 - Some things ought not be known – you look away when your friend is typing their password

Benefits of Privacy

- Individual growth
 - Necessary to blossom into a unique individual
- Individual responsibility
- Freedom to be yourself
 - Nobody likes to be videotaped all the time
- Intellectual and spiritual growth
- Development of loving, trusting, caring, intimate relationships

Harms of Privacy

- Cover for illegal or immoral activities
- Burden on the nuclear family
- Hidden dysfunctional families
 - Incidents of domestic violence
- Ignored people on society's fringes
 - People with disability e.g., with mental illness



Class Discussion: 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



Data Gathering and Privacy Implications



But where to draw the
line?

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



Rewards or Loyalty Programs



Facebook Tags




Body Scanners



Medical Records




Implanted Chips



The newfound privacy conundrum presented by installing a device that can literally listen to everything you're saying represents a chilling new development in the age of internet-connected things. By buying a smart speaker, you're effectively paying money to let a huge tech company surveil you. And I don't mean to sound overly cynical about this, either. Amazon, Google, Apple, and others say that their devices aren't spying on unsuspecting families. The only problem is that these gadgets are both hackable and prone to bugs.

– Gizmodo about Amazon Echo/Google Home etc.

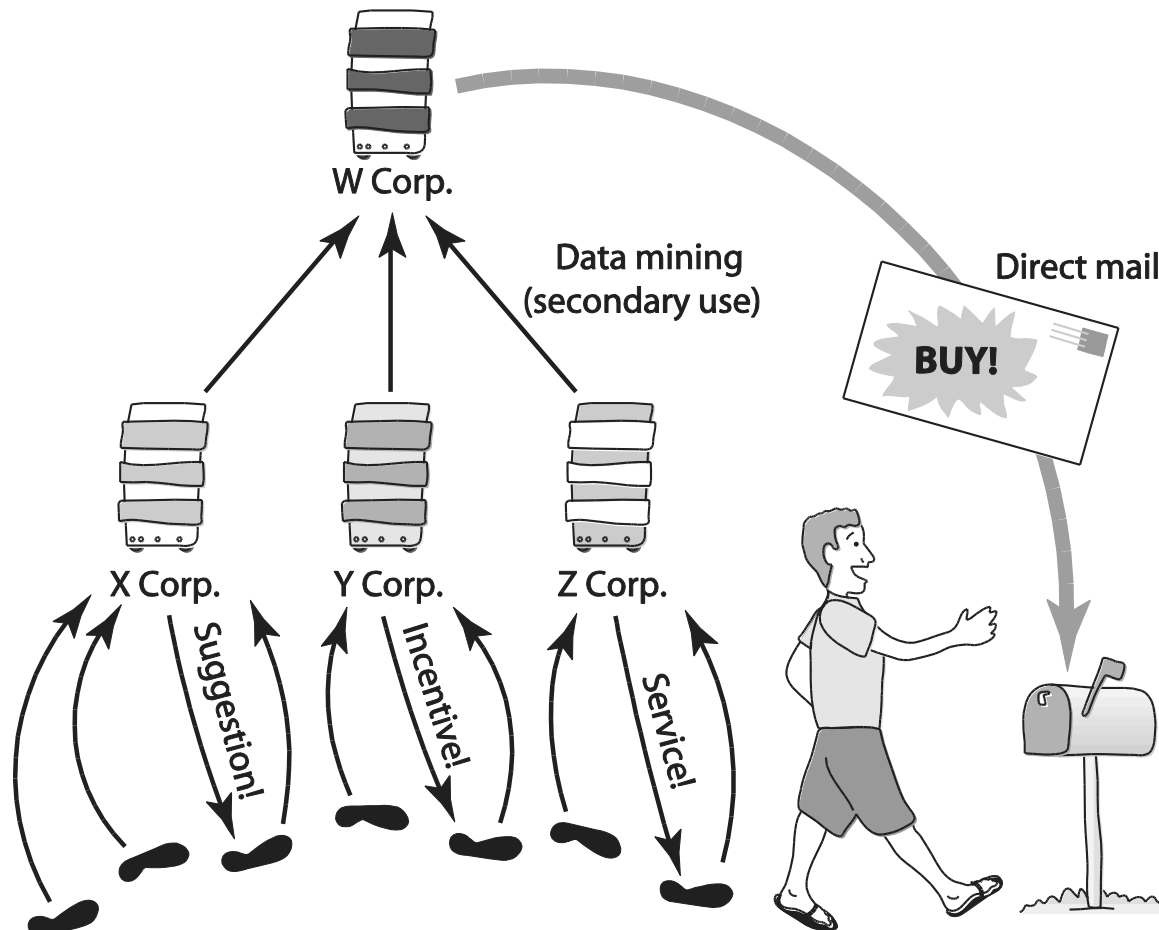



Is using Alexa or Google
Home a violation of
privacy?



AI/Machine Learning

Secondary Uses of Information





How is secondary information
used? Some examples...



Google's Personalized Search



Collaborative Filtering



Microtargeting



Credit Reports

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?

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


41

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



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)

Individualistic Approach – privacy is a private good

- With respect to the individualistic approach, scholars question people's ability to manage privacy amid increasingly complex trade-offs



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
- Security
- Trading data and market efficiency
- Chilling effects

* 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

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