CS 182: Ethics, Public Policy, and Technological Change

Rob Reich
Mehran Sahami
Jeremy Weinstein
Hilary Cohen
Data Privacy Day is a global effort — taking place annually on January 28th — that generates awareness about the importance of privacy, highlights easy ways to protect personal information and reminds organizations that privacy is good for business. Data Privacy Day began in the United States and Canada in January 2008 as an extension of the Data Protection Day celebration in Europe. Data Protection Day commemorates the Jan. 28, 1981, signing of Convention 108, the first legally binding international treaty dealing with privacy and data protection. Data Privacy Day is observed annually on Jan. 28.
Today’s Agenda

1. Orientation to Privacy
   • Zuckerberg & Sen. Durbin
   • Panopticon
   • Stanford Data Panopticon

2. What is Privacy?

3. Privacy and Big Data

4. Privacy and other values: security, transparency, consent

5. Biometrics: is there something special about the body?
Mark Zuckerberg
testifying before the United States Senate, April 2018
Who is this person?
Jeremy Bentham
1748-1832
Archive of Daily Timelapses

At the end of the South Cloisters of the main building of UCL stands a wooden cabinet, which has been a source of curiosity and perplexity to visitors. The cabinet contains the preserved skeleton of the philosopher and jurist Jeremy Bentham, (1748-1832), which dressed in his own clothes, and surmounted by a wax head, looks as if he is still alive.
Stateville Correctional Center, Illinois
Michel Foucault
(French philosopher)

- He is seen, but he does not see; he is an object of information, never a subject in communication.

*Discipline and Punish*
Power over Others

Hence the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power.

So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its action; that the perfection of power should tend to render its actual exercise unnecessary.

- Michel Foucault
The Panopticon must not be understood as a dream building; it is the diagram of a mechanism of power reduced to its ideal form. (Foucault)
PRIVACY IS POWER

WHY AND HOW YOU SHOULD TAKE BACK CONTROL OF YOUR DATA

CARISSA VÉLIZ

‘An essential guide to one of the most pressing modern issues.’

HANNAH FRY
author of Hello World
A Modern Panopticon?
The 1619 Project

Nikole Hannah-Jones

Our democracy’s founding ideals were false when they were written. Black Americans have fought to make them true.
Today modern technology has facilitated unremitting workplace supervision, particularly in the service sector. Companies have developed software that records workers’ keystrokes and mouse clicks, along with randomly capturing screenshots multiple times a day. Modern-day workers are subjected to a wide variety of surveillance strategies, from drug tests and closed-circuit video monitoring to tracking apps and even devices that sense heat and motion. A 2006 survey found that more than a third of companies with workforces of 1,000 or more had staff members who read through employees’ outbound emails. The technology that accompanies this workplace supervision can make it feel futuristic. But it’s only the technology that’s new. The core impulse behind that technology pervaded plantations, which sought innermost control over the bodies of their enslaved work force.

The Digital Panopticon

Citizens can sign up as Virtual Texas Deputies to participate in border surveillance through this social network. Virtual Texas Deputies from around the country will monitor the streaming video from these cameras 24/7 and report any suspicious activities directly to the Border Sheriffs via email. All emails regarding suspicious activity will be submitted anonymously.
CCTV in London

Greater London has an estimated **500,000** closed circuit television cameras monitoring public spaces.
The Secretive Company That Might End Privacy as We Know It

A little-known start-up helps law enforcement match photos of unknown people to their online images — and “might lead to a dystopian future or something,” a backer says.
Even if Clearview doesn’t make its app publicly available, a
copycat company might, now that the taboo is broken. Searching
someone by face could become as easy as Googling a name.
Strangers would be able to listen in on sensitive conversations,
take photos of the participants and know personal secrets.
Someone walking down the street would be immediately
identifiable — and his or her home address would be only a few
clicks away. It would herald the end of public anonymity.

Asked about the implications of bringing such a power into the
world, Mr. Ton-That seemed taken aback.

“I have to think about that,” he said. “Our belief is that this is the
best use of the technology.”
Real Time Facial Recognition for London Police?

London Police Are Taking Surveillance to a Whole New Level

The city, stepping into a debate over privacy, says it will use real-time facial recognition technology “to tackle serious crime.”
Edward Snowden: Criminal or Whistleblower?
Do we Live in an Age of Surveillance Capitalism?

An economy driven by massive data collection (and privacy violations) where a small number of companies possess vast troves of information about individual and collective experience.
US Bill of Rights *(roughly speaking)*

1A: Congress shall not limit religious freedom, or freedom of speech or of the press.

2A: The right to bear arms shall not be infringed.

3A: Govt shall not quarter soldiers in any house.

4A: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.

5A: No person shall be required to be a witness against himself; no private property shall be taken for public use without due compensation.
1A: Government can learn where/how you worship, what you say, with whom you meet or communicate.

2A: Government can discover who has bought Arms and can keep track of those persons.

3A: Government can “quarter” in any house, “without the consent of the Owner,” ways to learn any digitized activity by any person or thing in the house.

4A: Government can search any device, without a warrant or having any reason to believe any such person has committed or intends to commit a crime.

5A: Any person’s digital information can be taken and used against such person, without compensation or any legal process.

Adapted, Reed Hundt, Boston Review
You have zero privacy. Get over it.

Scott McNealy, CEO Sun Microsystems
Tim Berners-Lee, founder of the web

The right of people to have a private conversation is really important for democracy. People in the same family who live in different cities need to be able to communicate privately without it being intercepted. Really, it is a human right.

*Wired Magazine 2017*
6.1.1 Privacy and Access to Electronic Information

Last updated on: 10/04/2016

Formerly Known As Policy Number: 61

This guide memo establishes a policy on privacy in Electronic Information and the circumstances under which Electronic Information may be accessed and/or disclosed without User Consent.

Authority:
Approved by the President of the University.

Jump To:

1. Summary
2. Definitions
3. Privacy and Confidentiality
4. Access Without User Consent
5. Additional Procedures
6. Retention and Disposition
8. Appendix B: Information Available to the University

1. Summary

a. Purposes of Policy
Establish a policy on privacy in Electronic Information and the circumstances under which Electronic Information may be accessed and/or disclosed without User Consent.
Third Provocation: Stanford data collection policies

*Spend 7-10 minutes:*

Create a shared google doc of all the data that you believe Stanford has collected about you in the past 7 days.

Make 2 lists: ordinary on campus life, and another of off-campus virtual life.
## First 9 Sources of Stanford’s Personal Data Collection

<table>
<thead>
<tr>
<th>SYSTEM</th>
<th>BUSINESS PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFS</td>
<td>Provides general purpose online file storage hosted entirely at Stanford</td>
</tr>
<tr>
<td>BigFix</td>
<td>Software updates for your laptop/desktop computer, provides software and hardware inventory capabilities.</td>
</tr>
<tr>
<td>DHCP logs</td>
<td>assigns network addresses and provides key network configurations to the vast majority of laptops, desktops and mobile devices used on the campus network.</td>
</tr>
<tr>
<td>Door Access Logs</td>
<td>Controls card access to most of the campus buildings. Logs are used for troubleshooting and for maintaining a record of accesses.</td>
</tr>
<tr>
<td>Email, Contacts, Calendar, Office 365</td>
<td>Office 365 is the University's primary electronic collaboration system.</td>
</tr>
<tr>
<td>Email</td>
<td>Processes all incoming and outgoing email, spam detection and filtering, automatically blocking unencrypted messages containing known High Risk Data</td>
</tr>
<tr>
<td>Stanford ID Card</td>
<td>Meal plans, purchases, library services</td>
</tr>
<tr>
<td>Server Logs</td>
<td>Generate Logs of Stanford Server Activity</td>
</tr>
<tr>
<td>Network Activity Logs</td>
<td>Network activity logs are used to detect network intrusions and identify compromised systems. They are also used for forensic investigations of past intrusions, and sometimes to locate missing students.</td>
</tr>
</tbody>
</table>
This is a list of 40 the ways in which Stanford Collects your data (Sources of Stanford’s Personal Data Collection)

<table>
<thead>
<tr>
<th>Laptop/Desktop Anti-Malware for Mac</th>
<th>AFS (online file storage)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop/Desktop File Backups (Crashplan)</td>
<td>Authentication Logs</td>
</tr>
<tr>
<td>Medicine Box</td>
<td>BigFix Configuration Management</td>
</tr>
<tr>
<td>Mobile Device Management</td>
<td>Box</td>
</tr>
<tr>
<td>MyDevices</td>
<td>Centralized Logging for Servers (Splunk)</td>
</tr>
<tr>
<td>NetDB</td>
<td>Departmental Firewalls</td>
</tr>
<tr>
<td>Network Activity Logs</td>
<td>DHCP Logs</td>
</tr>
<tr>
<td>Network Equipment</td>
<td>Domain Name Service (DNS) Logs</td>
</tr>
<tr>
<td>Network Registration</td>
<td>Door Access System Logs</td>
</tr>
<tr>
<td>Paging System</td>
<td>Email, Calendar, Contacts, OneDrive: Office 365</td>
</tr>
<tr>
<td>People Soft</td>
<td>Email Data Loss Prevention (Code Green)</td>
</tr>
<tr>
<td></td>
<td>Email Logs</td>
</tr>
<tr>
<td></td>
<td>Google Apps</td>
</tr>
<tr>
<td></td>
<td>IPM</td>
</tr>
<tr>
<td></td>
<td>Laptop/Desktop Anti-Exploit for Windows (EMET)</td>
</tr>
<tr>
<td></td>
<td>Registry</td>
</tr>
<tr>
<td></td>
<td>Server Logs</td>
</tr>
<tr>
<td></td>
<td>Server Vulnerability Scanning</td>
</tr>
<tr>
<td></td>
<td>Software Vendors</td>
</tr>
<tr>
<td></td>
<td>Stanford ID Card Financial Transactions and Library Usage</td>
</tr>
<tr>
<td></td>
<td>Stanford Whole Disk Encryption (SWDE)</td>
</tr>
<tr>
<td></td>
<td>SUNet Account Password and Two-Step Authentication Resets</td>
</tr>
<tr>
<td></td>
<td>Telephone Service for Students</td>
</tr>
<tr>
<td></td>
<td>Two-Step Authentication (Duo)</td>
</tr>
<tr>
<td></td>
<td>Video Cameras and Monitoring</td>
</tr>
<tr>
<td></td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td></td>
<td>Very Lightweight Reporting Engine (VLRE)</td>
</tr>
<tr>
<td></td>
<td>Voicemail</td>
</tr>
</tbody>
</table>
The Worst Product Name in History?

There's nothing you can't capture.

Every class is different. In ECON 201, you only need to capture audio and the professor’s PowerPoint slides. In STAT 390, you also need to record a document camera. In BIO 453, there are two fixed IP cameras, a wireless mic system, two laptops, and a polarizing microscope.

Panopto is the only lecture capture system built with the flexibility to record any combination of video sources, in any configuration, in classrooms of any size. And Panopto scales with ease to meet your institution's needs — from small departmental deployments to campus-wide installations.

We wrote the complete guide to implementing lecture capture anywhere on campus, from content considerations to equipment configuration and more.

Download your copy of How To Set Up Any Room For Lecture Capture >
Panopto on campus

TECHNOLOGY
Panopto software glitch temporarily grants 660 Stanford students ‘creator’ status
Discussion Question

• Imagine that Stanford is seeking a new revenue stream to support financial aid for needy students.
• Suppose it also wants to help job placement for its grads.

**Solution**: Monetize the data it possesses about student learning by selling data profiles to prospective employers.

• A form of ”targeted” or “personalized” recruitment.
• Not ”ad tech” but “placement tech.”

**Discuss**: Do you support? Why or why not?
Today’s Agenda

1. Introductory Provocations
   • Zuckerberg & Sen. Durbin
   • Panopticon
   • Stanford Data Panopticon

2. What is Privacy?

3. Privacy and Big Data

4. Privacy and other values: security, transparency, consent

5. Biometrics: is there something special about the body?
What is Privacy?

Few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists.

“Alan Westin, 1967
What is Privacy?

The most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is.

What is Privacy?

Privacy is a concept in disarray.

Daniel Solove
Georgetown Law Professor
Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.

Robert Post, Yale Law Professor
So, What is Privacy?

Aristotle provides us an early view:

The Public Sphere: politics and commerce

X

The Private Sphere: domestic life, family and friends

Individuals have interests in shielding the public (politics and commerce) from seeing/hearing what happens in private.
So, What is Privacy?

But the public/private sphere distinction is crude.

**Social context** is what’s important, whether in the public or private sphere (Nissenbaum). We want to be able to control what is known about us, how we present ourselves, whether we are in public or private spheres.

Individuals have privacy interests even when in public!
Privacy is multi-dimensional (Solove)

Privacy concerns control over information about ourselves (self-determination), and about the pursuit of relationships with others (intimacy).

- **Individuals have privacy interests even when in public!**

Privacy is not about hiding things that are wrong or embarrassing.

It is about protecting intimacy, freedom, and control. (Solove, “Nothing to Hide Argument”)
Modern view is concerned with both private and public spheres

Privacy is central to *individual autonomy* or *self-determination*:

*The claim of individuals to determine for themselves when, how, and to what extent information about them is shared with or communicated to others.*

Violations of privacy impose *harms*:

Loss of freedom, intimacy, control over self and future.
Four Categories of Privacy Harms

1. **Information Collection** (e.g., surveillance)
2. **Information Processing** (e.g., aggregation and inferences made from big data)
3. **Information Dissemination**
   A. Breach of confidentiality
   B. Disclosure to third parties
   C. Blackmail
4. **Invasion of Privacy**
   A. Intrusion
   B. Decision interference

(Solove, A Taxonomy of Privacy)
Question:

- Should privacy be treated differently depending on whether it is the government or a company that collects data?

- Different privacy standards for different agents?
Today’s Agenda

1. Introductory Provocations
   • Zuckerberg & Sen. Durbin
   • Panopticon
   • Stanford Data Panopticon
2. What is Privacy?
3. Privacy and Big Data
4. Privacy and other values: security, transparency, consent
5. Biometrics: is there something special about the body?
Privacy and Big Data

When interacting with digital devices and the web, individuals give up information about themselves, creating digital exhaust streams.

Then algorithms can make **inferences and predictions** about people from these data.
Predictive Analytics at Target
(and every other big company)

Data Collected by Target on shoppers, all linked to unique “Guest IDs”:

- Purchases made
- Coupons used
- Credit cards used/owned
- Surveys completed
- Emails opened
- Website visits
- Other websites visited
- Customer service calls

Plus data purchased from data brokers or acquired through surveys:

- Age
- Marriage status
- Income
- Zip code
- Race/ethnicity/religion
- Alma mater
- Magazine/newspaper subs
- Job history
- And much more
Create a “Pregnancy Prediction” Score

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.

One Target employee I spoke to provided a hypothetical example. Take a fictional Target shopper named Jenny Ward, who is 23, lives in Atlanta and in March bought cocoa-butter lotion, a purse large enough to double as a diaper bag, zinc and magnesium supplements and a bright blue rug. There’s, say, an 87 percent chance that she’s pregnant and that her delivery date is sometime in late August. What’s more, because of the data attached to her
Free $20 Target GiftCard™
with select baby department purchase of $100 or more

- Wipes
- Diapers & training pants
- Infant formula
- Baby food
- Baby toys

Category Offer: Must be used in store. This offer cannot be combined with other department/coordinates offers, excluding gift cards. Gift cards and cash will not be paid. In determining purchase total, from the free offers, the purchase price does not include sales tax or shipping and handling. Offers are not valid on gift cards, gift cards, or gift certificates. You may not assign, sell, or otherwise transfer this offer. The offer may be void where prohibited by law. The offer may not be used in combination with any other offers. Void if transferred, sold, or purchased. See store for complete details.

Find this offer in Wallet in the Target app

Free stuff Finder.com
Questions:

- Should the information about the women private information?
- Did Target do something wrong?
A Digression: Ad Tech and You

This is the surveillance capitalism economy.

This is ad tech.

This is what many jobs at Facebook and Google and Amazon are.

"The best minds of my generation are thinking about how to make people click ads."

--Jeff Hammerbacher, a 28-year-old Silicon Valley tech whiz who went from being an early employee at Facebook to co-founding the data analysis start-up Cloudera, in Ashlee Vance's BusinessWeek story about the advertising and social-media driven bubble in Silicon Valley.
1. Encryption
Protect information collection, processing, and dissemination

2. Differential Privacy
Retaining predictive accuracy while also protecting individual privacy.
➢ Mehran to discuss soon.
Today’s Agenda

1. Introductory Provocations
   • Zuckerberg & Sen. Durbin
   • Panopticon
   • Stanford Data Panopticon
2. What is Privacy?
3. Privacy and Big Data
4. Privacy and other values: security, transparency, consent
5. Biometrics: is there something special about the body?
Rival Values?

Privacy versus National Security?

Does national security and safety override concerns about privacy?
Privacy vs. Security?

Apple vs the FBI:

Should the government be able to compel Apple to unlock the iPhone of a suspected terrorist?

In Apple Debate on Digital Privacy and the iPhone, Questions Still Remain

By Eric Lichtblau

March 28, 2016

WASHINGTON — A furious legal battle over digital privacy in the age of the iPhone ended on Monday with no clear winner — only lingering questions over what will happen the next time the government tries to force Apple to help break into one of its own phones.

The Justice Department on Monday announced that it had gotten what it wanted most immediately in the case of the San Bernardino terrorist attack: a way to unlock the iPhone used by one of the shooters to determine what evidence it might hold, even without Apple's assistance.

But that development forestalls a court ruling on the bigger legal questions that have been so hotly debated since the case erupted last month when a judge in California ordered Apple to unlock the phone used by Syed Rizwan Farook.

The legal debate in that state offered what many legal analysts saw as a powerful test case for the Justice Department to establish its position. But that verdict will now have to wait for another day.
Privacy vs. Security?

White Supremacists move to Signal and Telegram

Very limited capacity to monitor what happens on end-to-end encrypted platforms.

Is 100% privacy the right trade-off?
Today’s Agenda

1. Introductory Provocations
   • Zuckerberg & Sen. Durbin
   • Panopticon
   • Stanford Data Panopticon
2. What is Privacy?
3. Privacy and Big Data
4. Privacy and other values: security, transparency, consent
5. Biometrics: is there something special about the body?
Biometric data:
You can’t change your faceprint.