Online Privacy

Module 8 of a course on *Ethical Issues in AI*

Prepared by

John Hooker

Emeritus Professor, Carnegie Mellon University

CMU Osher, February 2025

Surveillance

- Electronic surveillance is everywhere.
  - *Browsing history, cookies, keystrokes recorded.*
  - *Social media tracking data provided to advertisers.*
  - *Alexa, etc., listen in on conversations.*
  - *Shopping & purchases recorded and shared.*
  - *Embedded tracking pixels, super cookies, ip address, operating system characteristics.*

Surveillance

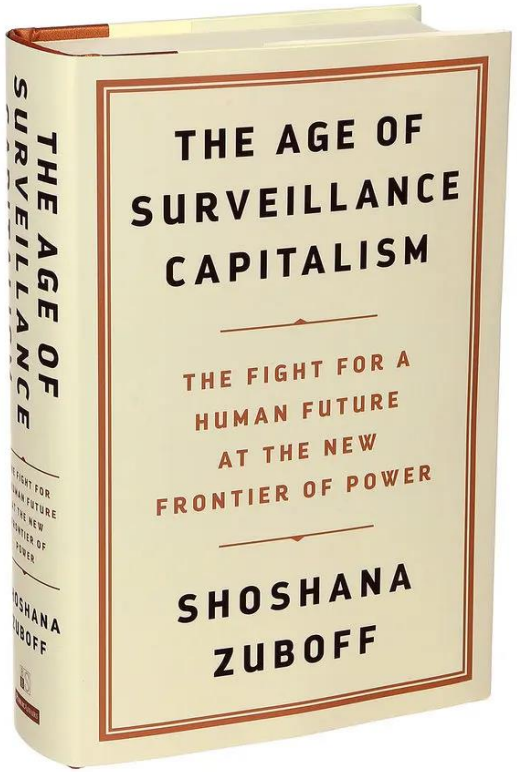
- Electronic surveillance is everywhere.
  - *Smart phone tracking, movements recorded.*
  - *Browsing tracked in shops & linked with purchase record.*
  - *Facial recognition by surveillance cameras*
  - *Vehicle tracking by parking meters, license plate readers*
  - *Individual dossiers assembled by data mining techniques.*

Surveillance

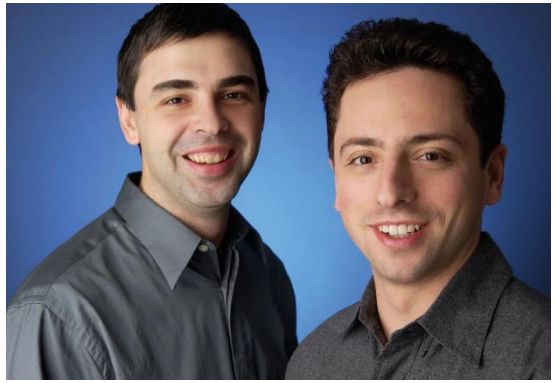
- Business is a major player.
  - *Personal data collection is **the dominant online business model**.*
  - *Big tech and government compete for control of data.*
    - Government often demands data from tech companies.

Surveillance

- Encyclopedic reference:



Data monetization



Larry Page and Sergey Brin

- How did it get started?
  - *It happened at Google*
    - According to Zuboff.
  - *Google was approaching a **financial crisis** in 2000.*
    - No profits yet. Investors were patient so far.
    - **No clear business model**. Paid subscriptions seemed impractical.
    - Page and Brin feared that ad-based revenue would lead to biased searches.
    - Google had developed AdWords to improve ad placement, but it received little emphasis.
    - Then the **dot-com bubble burst,** and Google frantically sought a solution to profitability.

Data monetization

- How did it get started?
  - *An odd turning point (2002)*
    - Google team noticed a flood of search queries on the same term 45 min after every hour for 4 hours.
    - This was due to a quiz show airing in successive time zones.
    - This revealed the **power of data harvesting to probe into people's lives**.
  - *Response to the **financial crisis**.*
    - Sheryl Sandberg, recruited in 2001, led a team to revamp AdWords to target users with ads **based on search history**. She was promoted to VP for Global Sales.
    - Google became the **dominant search engine** by mid-2000s.

Data monetization

- The rest is history
  - *Facebook takes over*
    - Facebook recruited Sandberg in 2006 as COO.
    - She became the “Typhoid Mary of surveillance capitalism” according to Zuboff.
    - Facebook became the **most aggressive user** of personal data and quickly crushed MySpace.
  - *The result?*
    - Data harvesting has **transformed the world**.

Sheryl Sandberg

Data monetization

- Focus on WhatsApp
  - *Early history (2009-2014)*
    - Acton & Koum were former Yahoo! employees.
    - Facebook rejected their job applications.
    - Founded WhatsApp, a pun on “What’s up?”
    - It quickly became an **instant messaging** service internationally, initially **free**.
    - Founders wanted to **avoid ads and data harvesting**.
    - Offered end-to-end encryption.
    - Charged $1/year fee, often not collected.
    - Relied on investors for income.

Brian Acton

Jan Koum

Data monetization

- Focus on WhatsApp
  - *Acquisition by Facebook (2014)*
    - Zuckerberg offered **$19 billion!**
    - Why?
      - Get ahead of Google offer.
      - Reduce competition.
      - Access to data.
    - Asked Acton & Koum to stay on, which they did.
    - Zuckerberg "promised" **no monetization** of user data, but abolished $1 fee.
    - Acton later said,
      - "I sold my users' privacy to a larger benefit. I made a choice and a compromise. I live with that every day." *Forbes,* 26 Sep 2018.

Data monetization

- Focus on WhatsApp
  - *Controversies*
    - Acton **quit** in 2017 due to dispute with Zuckerberg over monetization, sacrificing $850 million.
    - Koum followed in 2018.
    - Same year, Acton endowed and headed up foundation to support non-profit site **Signal**, which does not collect data.
    - In 2021, EU **fined** WhatsApp $270 million for failing to reveal how it monetizes user metadata (violation of GDPR).
    - Signal (open source software) has about 40 million users.
    - Unclear whether Facebook harvests **content** of WhatsApp messaging before “end-to-end” encryption.

Ethics of privacy

- Little consensus on ethical basis for privacy.
  - *One reason we don't agree on what to do about privacy invasion in the tech age.*
- Our approach – cycle through the ethical principles
  - *Generalization*
  - *Utilitarian*
  - *Autonomy*

Privacy and utility

- Argument 1: Surveillance is **harmless**
  - *Most online surveillance is for **commercial** purposes.*
    - It is pervasive but **harmless**.
    - It can be **beneficial** by directing ads.
    - And serve a **greater purpose** of matching supply and demand.
    - This is the primary function of **marketing**.

Privacy and utility

- Argument 2: Surveillance is **risky**
  - *Online data repositories are **hacked** all the time.*
    - 3158 reported data breaches in US in 2024, resulting in 1.7 billion victim notices (source: Identity Theft Resource Center).
    - Almost daily occurrence, leading to "data breach fatigue."
  - This imposes multiple **risks**:
    - **Consumer**: identity theft, fraudulent charges
    - **Merchant**: lawsuits, irate customers
    - **Both**: government intrusion

Privacy and utility

- Argument 3: Inconclusive, but…
  - *We can say **this much**:*
    - Businesses must **upgrade security** against data breaches.
    - Too many are **lax**, wanting to avoid trouble and expense,
    - …while **hoping** a breach doesn't happen to them.
    - This is **disutilitarian**, and **bad business**.
    - A security upgrade is necessary **insurance**.

Privacy and generalizability

- Argument 1: **Deception**
  - *Users are **misled** about the lack of privacy.*
    - "Privacy settings"
    - "We care about your privacy" notice, followed by fine print

In July 2019, FTC imposed $5 billion penalty on Facebook (largest ever) for "deceiving users about their ability to control the privacy of their personal information."

Privacy and generalizability

- Argument 1: **Deception**
  - *Social media knowingly cause users to have false beliefs about the level of privacy.*
    - Most users remain somewhat naïve about data collection.
    - This is done purely for company profit.
    - It is **not generalizable**.

Privacy and generalizability

- Argument 1: **Deception**
  - *Easy to **avoid** deception.*
    - Just be **up front** about how the site exploits user data
    - Prominently displayed.

Privacy and generalizability

- Argument 2: Privacy and **intimacy**
  - *Western culture is primarily concerned about **individual** privacy.*
  - ***Family** privacy is a more widespread concern.*
    - Families have **intimate** knowledge of each other.
    - This knowledge must be **protected** for family safety.
    - Intimacy is impossible without **privacy**.

The family is the traditional organization mode of privacy.

Privacy and generalizability

- Argument 2: Privacy and **intimacy**
  - *Some say there are cultures **without privacy**.*
    - People live in multi-family dwellings.
    - So, privacy must not be necessary.

Inside an Iroquois longhouse

Privacy and generalizability

- Argument 2: Privacy and **intimacy**
  - *Yet anthropologists tell us that **all cultures** value some form of privacy.*
  - *To satisfy generalizability…*
    - A business must respect the **essential privacy norms** of the culture in which it operates.

Privacy and culture

- **Family privacy** reflected in architecture.
  - *Homes in many cultures are built around a **private courtyard**.*
    - with few openings to the outside world.

China

Latin America

Middle East

Privacy and culture

- **Germany**:
  - *Very sensitive to **individual** privacy.*
  - *Workers prefer a **private** office or cubicle.*
    - People don't like to **share** desks, computers, or space.
    - Hotel room walls are thick and **soundproof**.

Removable partitions in a German office building

Privacy and culture

- **Germany**:
  - *Strong objections to **Google Street View.***
    - Banned in some cities
    - Many requests to blur photos online.
    - Similar problems in Greece, Canada, UK

Blurred Street View in Hamburg

Privacy and culture

- **United Kingdom**:
  - *People are OK with **shared office space.***
    - Speak in **low voices** to preserve privacy of conversations.
  - *Surveillance cameras OK in public.*
    - Especially since the Troubles in N. Ireland.

Shared office in London

Privacy and culture

- **Northern Europe**:
  - *Concern for **information privacy.***
    - Motivation for EU's **General Data Protection Regulation**
    - …advocated primarily by Germany.
    - In theory, **individuals own their data**, rather than the online sites they visit.
    - However, practical effect is disputed.

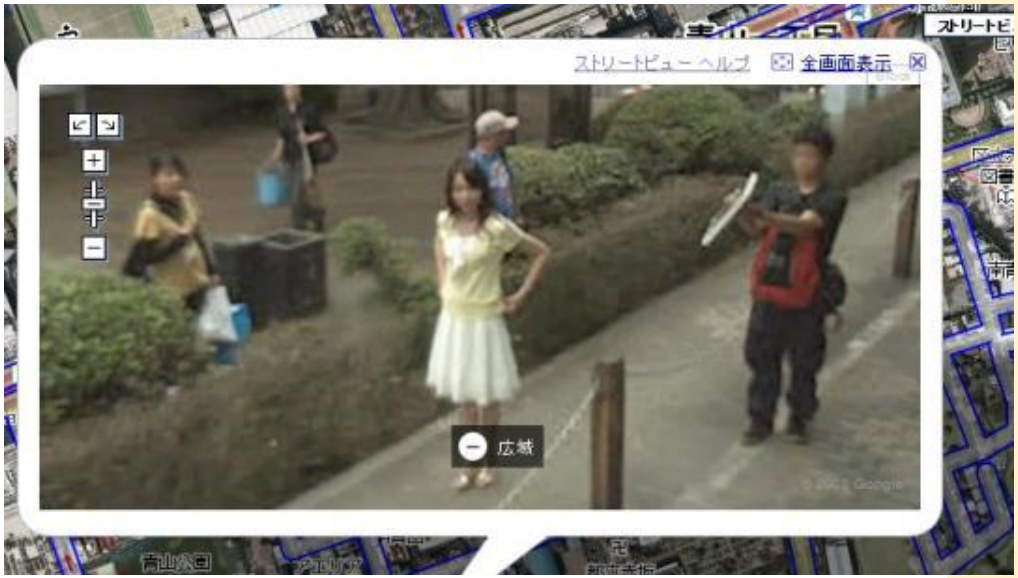
Privacy and culture

- **Japan**:
  - *People erect **invisible walls** around themselves.*
    - They pretend **no one else** is in the room.
    - Necessary due to crowded conditions.
    - Walls **paper thin** and hotels noisy.
    - Some baths are **public**.

Japanese hotel room

Privacy and culture

- **Japan**:
  - *Yet strong objections to Google Street View cameras that **peered over hedges** surrounding one's home.*
    - It is **illegal** to stare into a private yard.
    - Must pretend not to see what is in the yard.
    - Google finally moved its cameras below hedge level.



Privacy and culture

- **China**:
  - ***Family*** *privacy important.*
  - *No objections to government* ***drone surveillance****.*
    - Part of the government's **job**
    - …provided people **benefit** from it.
    - Chinese law **prohibits** privacy invasion (by business) that compromises one's "**dignity**."
  - *OK to ask personal questions*
    - If no one loses **face**.
    - A chance to brag about **age**, **salary**

Drone enforcement
in Xiangyang during Covid

Privacy and culture

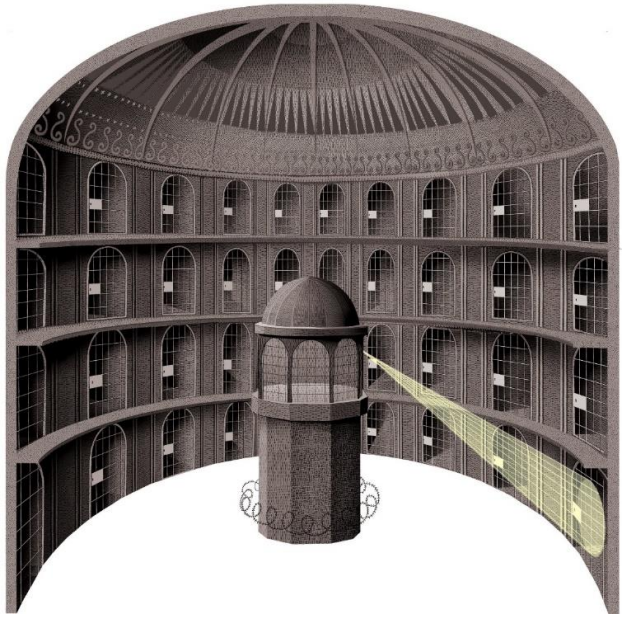
- **U.S.**
  - ***Financial, health and age*** *privacy important*
  - *People put their private lives on* ***Facebook****, but it is* ***strictly forbidden*** *to ask a person's* ***salary****.*
    - **Rude** to ask about **health** or **age** other than with friends.
    - Due perhaps to **strategic value** of salary info, youth, and fitness in a **highly competitive** economy.
    - And Facebook posts present a **sanitized & idealized version** of one's life.

Privacy and culture

- Conclusion
  - *Privacy norms **vary greatly** across cultures.*
  - *Generalization requires **respect for local privacy norms** that are essential to the functioning of the culture.*
    - Most social media companies tend to have a **US-centric** perspective that is uninformed about cultural differences.

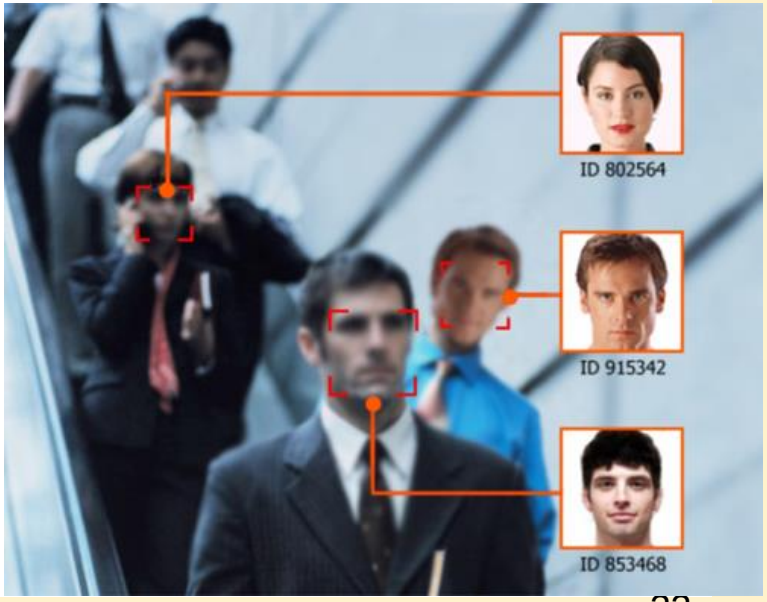
Privacy and autonomy

- Precursor of constant surveillance…
  - *Jeremy Bentham's* ***panopticon****.*
    - Prisoners never know when they are being watched.
    - "A new mode of obtaining power of mind over mind."
      - *Bentham, 1787*
    - Closely analogous to our situation.
    - If others have **power** over our minds, this sounds like violation of **autonomy**.



Privacy and autonomy

- Precursors of constant surveillance…
  - *George Orwell's* ***telescreen****.*
    - From his novel 1984.
    - His prediction was about 15 years early.
  - ***Facial recognition***
    - In use today.
  - *Online* ***data harvesting****…*



Privacy and autonomy

- Science fiction(?) scenario…
  - *Every thought is open to scrutiny.*
    - We cannot be ourselves.
    - Denial of **autonomy**.
  - *Are we approaching this?*

Conclusions…

- Utilitarian principle
  - *Utilitarian calculation **unclear**.*
  - *Business must at least **upgrade** security.*
- Generalization principle
  - *Business must fully **alert** customers to data harvesting.*
    - To avoid deception
  - *Generalized surveillance could undermine **social fabric**.*
    - By interfering with intimacy.
- Autonomy principle
  - *Sufficiently intrusive surveillance could **destroy** autonomy.*