DS 593: Privacy in Practice

Understanding Privacy Harms

Instructor: Alishah Chator

Last time

- Privacy and Regulation

Today

- Privacy Harms

Contextual Integrity

- Norms of Appropriateness
- Norms of information Flow
- Privacy is when both are upheld and is violated if either is violated

Contextual Integrity

- Key Parameters:
  - Data Subject (About what/whom)
  - Sender
  - Receiver
  - Information Type (What is being sent)
  - Transmission Principle (What are the constraints)

Health Data of 1 Million Americans Stolen By Hackers

Published Jan 31, 2025 at 11:26 AM EST | **Updated** Jan 31, 2025 at 7:14 PM EST

https://www.newsweek.com/health-data-1-million-americans-stolen-hackers-2024142

Wiz Research Uncovers Exposed DeepSeek Database Leaking Sensitive Information, Including Chat History

A publicly accessible database belonging to DeepSeek allowed full control over database operations, including the ability to access internal data. The exposure includes over a million lines of log streams with highly sensitive information.

https://www.wiz.io/blog/wiz-research-uncovers-exposed-deepseek-database-leak

ICE WANTS TO KNOW IF YOU'RE POSTING NEGATIVE THINGS ABOUT IT ONLINE

ICE wants to hire contractors to monitor social media for threats. Those who criticize the agency could be pulled into the dragnet.

https://archive.ph/lEENq

EFF Sues OPM, DOGE and Musk for Endangering the Privacy of Millions

Lawsuit Argues Defendants Violated the Privacy Act by Disclosing Sensitive Data

PRESS RELEASE | FEBRUARY 11, 2025

https://www.eff.org/press/releases/eff-sues-opm-doge-and-musk-endangering-privacy-millions

Scenario: Hospital Study

- A hospital is researching an emerging genetic disease in a small population of patients.
- Patients are advised that the system will allow researchers to analyze data about them without revealing sensitive information about their disease status.
- The patients consent, and the researchers analyze and publish their findings.

- A few months after the study is published, an insurance company combines the published data with consumer spending information to identify people with the disease and raises their rates

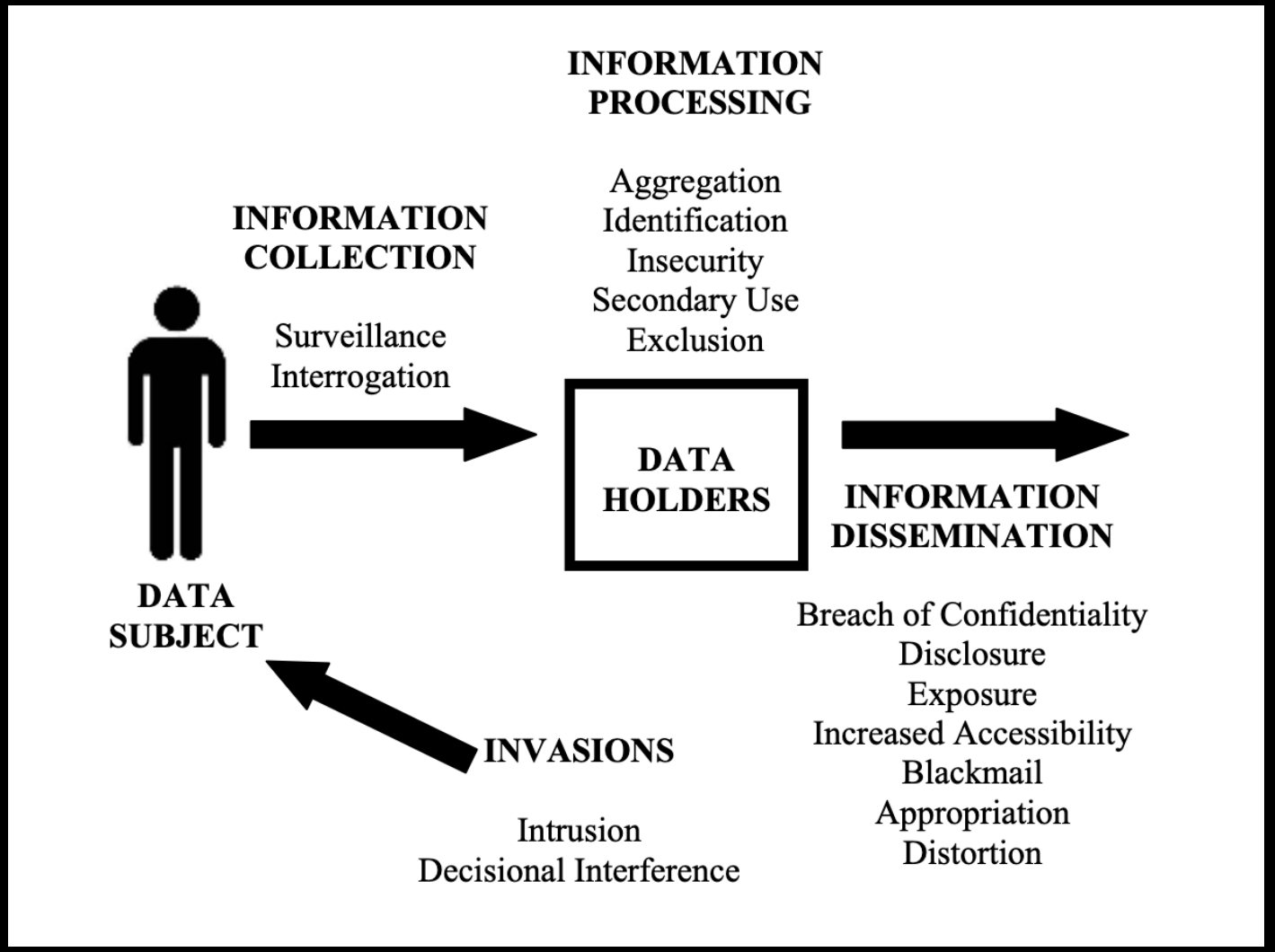
Scenario:

- Suppose the incidence of some sensitive attribute (pre-existing condition, political affiliation, etc) is 2% in the general population
- A survey is conducted in a room of 10 people, that finds that the incidence is 40% for that population.
- Is there a privacy harm here?
- Does it change if the incidence was even higher?

Dimensions of Harm

- Action Against Privacy
- Offender Against Privacy
- Privacy From-Whom

Applying this idea to Solove's Taxonomy



Individual Privacy Harms

- Loss of Agency
- Loss of Trust
- Loss of Narratives
- Loss of Intimacy
- Loss of Self-Discovery

Chilling Effect

In the context of privacy and surveillance the *Chilling Effect* refers to to how feeling excessively scrutinized or monitored will cause individuals to change their behavior, leading to self-censorship or other hesitations to exercise a legal right

Privacy Harms and Societal Impact

- Generally those holding marginalized identities are most susceptible to the chilling effect
- Chilling effect may also limit the discussion of diverse ideas or pursuit of new information
- Having a just democratic society is thus threatened by this chilling effect

Group Privacy

- Theory that groups have a separate right to privacy that also needs to be protected
- Predicated on the idea that there are harms that simply protecting individual privacy rights is not sufficient for
- Similarly, argues that individual privacy can not be guaranteed without group privacy

Group Privacy and Predictive Models

- Individual Privacy may focus on consenting to whether to be included in a training set or not
- However, the inclusion of a specific individual element in a training set rarely impacts the goal of whatever model is being trained
- What type of privacy impacts can these models have beyond leaking a training input?

Group Privacy and Predictive Models

- Concerns:
  - Models that use public social media data to decide whether to give loans
  - Models that uses visual and behavior data to decide whether to perform extra security screening
  - Target predicting pregnancy
  - Using Facebook data to infer sexual orientation or likelihood of postpartum depression
- In general, the issue is that models are imagining sensitive characteristics based on provided non-sensitive features

How to protect Group Privacy?

- How to identify the potential for risk or harm?
- How to establish consent?
- How to enforce?