DS 593: Privacy in Practice

Privacy Harms and Group Privacy

Instructor: Alishah Chator

News?

Today

- More about privacy harms

- Group privacy

Civil Liberties: Right-to vs Right-from

- Liberties are often thought of as the “right to” something

- In legal traditions, it is often more useful to consider these from the perspective of being a “right from” some harms

Example: Right to Free Speech

- The right to free speech may be described as the freedom to express yourself without retaliation
  - Is this precise?
  - Is this broad enough?

- Could say it is the *right from*
  - Censorship
  - Penalizing disagreement
  - Fear of retaliation
  - Fear of judgment

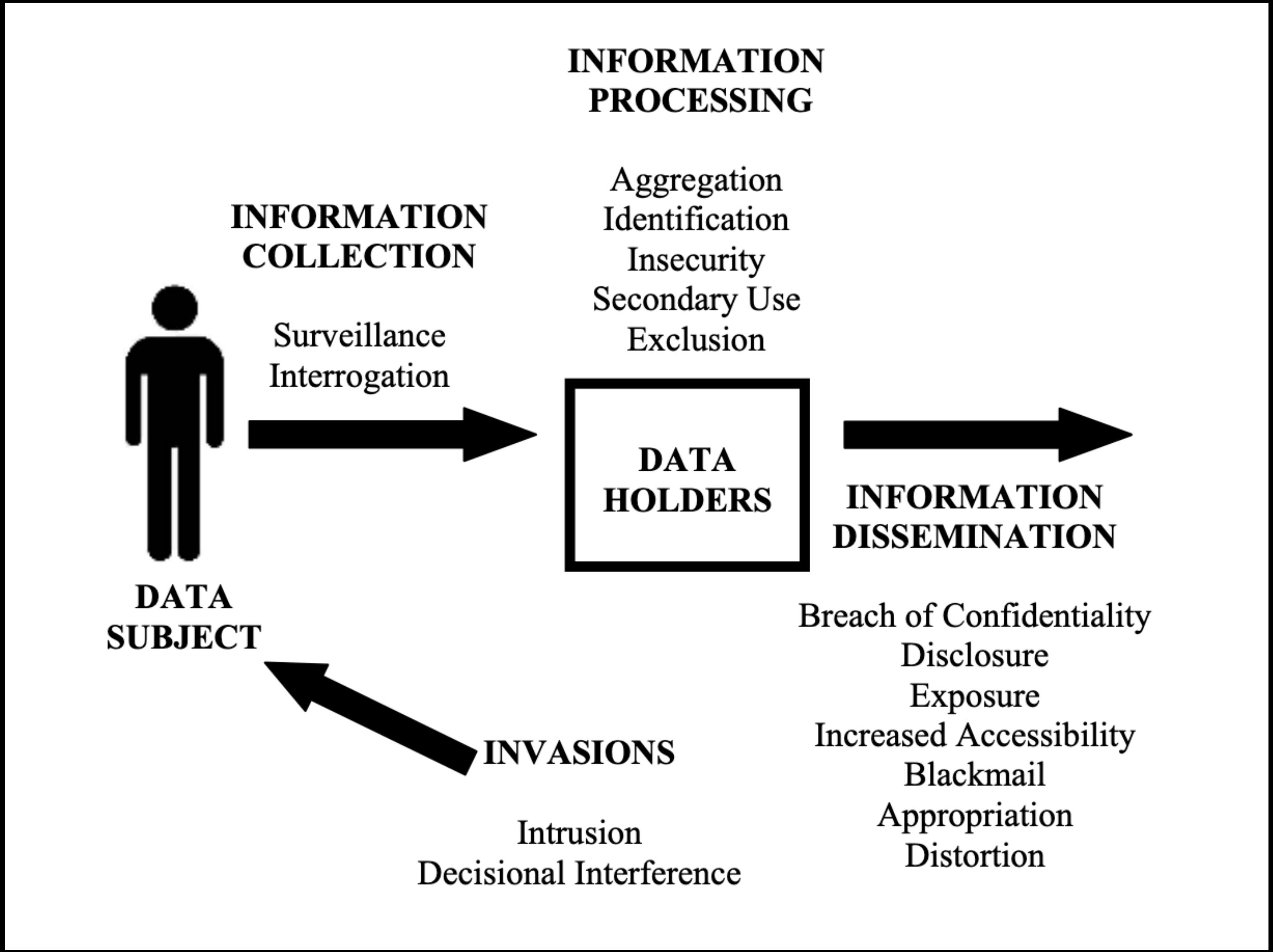
- The right to free speech is *all* of the mechanisms that prevent these harms

Right to Privacy

- In a similar sense, *privacy* can be better understood as a specific quality, but all of the mechanisms that serve to prevent what we consider privacy harms

- Many challenges for privacy arise when the harms are not what is being centered
  - i.e. *reasonable expectation of privacy*

Applying this idea to Solove’s Taxonomy



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

Privacy Harms and Individual Privacy

- Individual privacy is the specific focus on the privacy rights of individuals
    - EX:
        - Individual Consent
        - Individual Data Autonomy
        - Individual Secrecy
- Premise is that privacy harms can only affect an individual who has been identified

Predictive Privacy Harms

- Big Data and Machine Learning have vastly improved our capabilities of creating powerful predictive models

- A consequence of this is the new practice of “imagined PII”
    - Models can correlate public data with sensitive or even regulated features
    - Models make predictions beyond what is in the training set
    - Models can re-identify anonymized data by combining multiple data sources
    - Recall: mosaic theory

Imagined PII Consequences

- Enables several harms:
  - Identification
  - Secondary Use
  - Exclusion
  - Disclosure
  - Exposure
  - Distortion
  - Decisional Interference
- In particular, this imagined PII is being used to make decisions!

- The imagined PII might be wrong!
  - Still being used to make decisions

Barocas and Nissenbaum: *“Even when individuals are not ‘identifiable’, they may still be ‘reachable’, may still be comprehensibly represented in records that detail their attributes and activities, and may be subject to consequential inferences and predictions taken on that basis”*

Considering the potential for (re)identification we don’t even have sufficient mechanisms for *Individual Privacy*

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

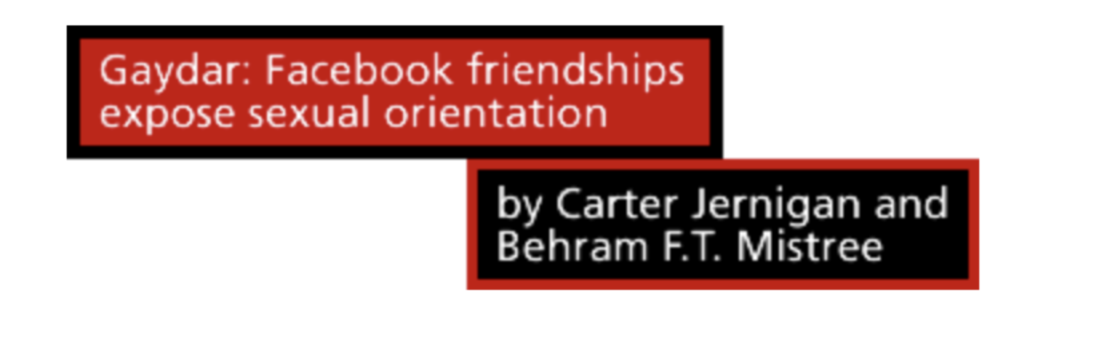
- However, the inclusion of a specific individual element in a training set rarely impacts the goal of whatever model is being trained

- What type of privacy impacts can these models have beyond leaking a training input?

“The search for group privacy can be explained in part by the fact that with big data analyses, <u>the particular and the individual is no longer central</u>. In these types of processes, data is no longer gathered about one specific individual or a small group of people, but rather about large and undefined groups. <u>Data is analysed on the basis of patterns and group profiles</u>; the results are often used for general policies and applied on a large scale. The fact that the individual is no longer central, but incidental to these types of processes, challenges the very foundations of most currently existing legal, ethical and social practices and theories.” – Luciano Floridi

Group Privacy and Predictive Models

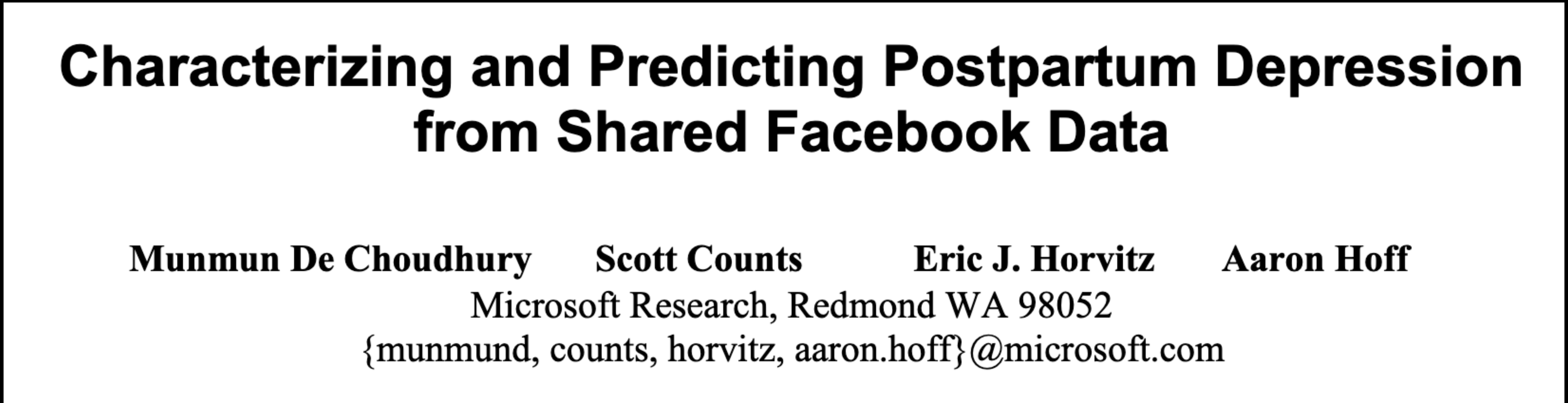
- Concerns:
  - Models that use public social media data to decide whether to give loans
  - Models that uses visual and behavior data to decide whether to perform extra security screening
  - Target predicting pregnancy
  - Using Facebook data to infer sexual orientation or likelihood of postpartum depression



Gaydar: Facebook friendships expose sexual orientation

by Carter Jernigan and Behram F.T. Mistree

https://firstmonday.org/ojs/index.php/fm/article/download/2611/2302



Characterizing and Predicting Postpartum Depression from Shared Facebook Data

Munmun De Choudhury Scott Counts Eric J. Horvitz Aaron Hoff
Microsoft Research, Redmond WA 98052
{munmund, counts, horvitz, aaron.hoff}@microsoft.com

https://dl.acm.org/doi/pdf/10.1145/2531602.2531675

Example: Targeted Ads

Example: LLM Detection

Group Privacy for Individual Privacy

- Group privacy is not just an approach to account for predictive privacy harms
- Inherently it is a necessary condition for any notion of individual privacy as well
- https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy
    - Only need 33 bits of information to uniquely identify somone

How to protect Group Privacy?

- How to identify the potential for risk or harm?

- How to establish consent?

- How to enforce?

Next Time

- Foundations of our digital world