CS2080: Applied Privacy for Data Science
Science & Technology Studies for (Differential) Privacy

School of Engineering & Applied Sciences
Harvard University

April 23, 2025

Housekeeping

[repeat from last time] Remaining class schedule

- Mon 4/28: Industry & government panel
  - Jack Fitzsimons (Oblivious)
  - Badih Ghazi (Google)
  - Simson Garfinkel (Basis, formerly Census & NIST)
  - Wanrong Zhang (TikTok)
- Wed 4/30: Conclusions, draft papers due
- Thu 5/8: Poster session, revised papers due

Upcoming office hours

- Today. Salil, 1:15-2pm in person, SEC 3.327
- Today. Yanis, 5-6pm Zoom
- Thurs. Zach, 9:45-11am (SEC 4.308) and 3-4pm (SEC 3.314)

Today's agenda

- Approaches to privacy
- Science & technology studies (STS) perspectives
- Applying STS theoretical frames to DP for Census use case

What is privacy (for)?

What is privacy (for)?

“Privacy is a concept in disarray. Nobody can articulate what it means…Abstract incantations of the importance of ‘privacy’ do not fare well when pitted against more concretely stated countervailing interests.” (Solove 2006)

What is privacy (for)?

“Privacy is… an interest in breathing room to engage in socially situated processes of boundary management.” (Cohen 2011)

Approaches to privacy

- Define privacy based on a conception of self as socially situated and relational (Cohen)
- Create a more comprehensive taxonomy of privacy harms (Solove)

Approaches to privacy

- Define privacy based on a conception of self as socially situated and relational (Cohen)
- Create a more comprehensive taxonomy of privacy harms (Solove)
- Analyze privacy based on contextual norms (Nissenbaum)
- Bridge gaps between technical and legal notions of privacy (e.g. Nissim-Wood, Cohen-Nissim)
- Design and deploy robust technical frameworks of privacy (DP)

Approaches to privacy

- Define privacy based on a conception of self as socially situated and relational (Cohen)
- Create a more comprehensive taxonomy of privacy harms (Solove)
- Analyze privacy based on contextual norms (Nissenbaum)
- Bridge gaps between technical and legal notions of privacy (e.g. Nissim-Wood, Cohen-Nissim)
- Design and deploy robust technical frameworks of privacy (DP)

What is the "right" approach?

Mulligan, Koopman, Doty (2016)

"We must reflect on what gets lost when we reify privacy as just one thing—one principle, one formalization, one method of protection. **We must engage with the whole tangled, ambiguous and essentially contested terrain of privacy**."

Mulligan, Koopman, Doty (2016)

"We must reflect on what gets lost when we reify privacy as just one thing—one principle, one formalization, one method of protection. **We must engage with the whole tangled, ambiguous and essentially contested terrain of privacy**."

Essentially contested concepts (Gallie 1956)

"Disputes about the concept's 'essence or meaning' are both paramount and central to the concept itself."

For example:
Democracy, art, freedom, privacy?

Mulligan, Koopman, Doty (2016)

"We must engage with the whole tangled, ambiguous and essentially contested terrain of privacy…

And yet, at the same time, the need to **build privacy values into data science** demands that we **clarify the purposes that privacy serves, the justifications that animate it and the actions that put it at risk**.

Meeting these goals simultaneously is not easy, but it should be the central agenda of privacy research today."

STS perspectives

Social construction of technology (SCOT) – Pinch & Bijker 1984

- Science and technology are shaped by human and social factors
- Paths of scientific or technological development are not inevitable; ‘closure’ is negotiated by the different social groups involved

STS perspectives

Social construction of technology (SCOT) – Pinch & Bijker 1984

- Science and technology are shaped by human and social factors
- Paths of scientific or technological development are not inevitable; ‘closure’ is negotiated by the different social groups involved

Politics of technology – Winner 1980

- “Instances in which the invention, design, or arrangement of a specific technical device or system becomes a way of **settling an issue** in a particular community.”
- “Systems that appear to require, or to be **strongly compatible with**, particular kinds of political relationships.”

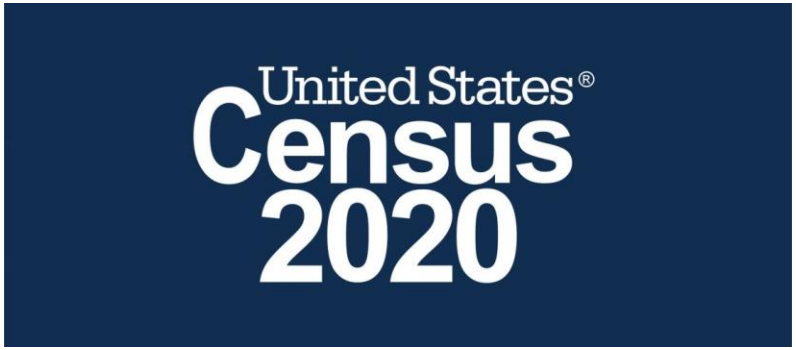
Discussion

What are the politics inherent in DP? How might it be used to “settle the matter,” or what political relationships might it be compatible with?

Abdu, Chambers, Mulligan, Jacobs 2024

- Examined how the adoption of DP (i.e., a technology shift) for the 2020 Census "[implicated] values, how such shifts can afford (or fail to afford) greater transparency and participation in system design, and the importance of localized expertise throughout."

- Relied the handoff model, a theoretical frame from STS



Handoff model (Mulligan & Nissenbaum 2020)

- A technological change in a larger system implicates values
  - "…the handoff lens highlights different ways that different types of system components operate and interoperate and shows these differences to be relevant to the configuration of values in respective systems. **The handoff lens offers a means to make ethically relevant changes salient that might otherwise be overlooked.**"

Handoff model (Mulligan & Nissenbaum 2020)

Elements of a system to examine to expose changing values:

- *Functions* of a system (what does it do?)
- *Components* involved, technical or human (what are its pieces?)
- *Modes of action* by which one component acts on or engages another (in what ways do its pieces connect?)
- *Trigger* that spurs the handoff (i.e., technological change) (why did it change?)

Adapted from Section 3.1 of Abdu, Chambers, Mulligan, Jacobs 2024

Applying the handoff model

- *Functions* of a system (what does it do?)
- *Components* involved, technical or human (what are its pieces?)
- *Modes of action* by which one component acts on or engages another (in what ways do its pieces connect?)
- *Trigger* that spurs the handoff (i.e., technological change) (why did it change?)

Applying the handoff model

- *Components* involved, technical or human (what are its pieces?)
  - Many groups stayed the same (e.g., demographers, community groups). But, there were also changes:
  - **Technical methods**
    - DAS: Statistical disclosure limitation SDL → DP
    - Introduced a new tunable parameter (epsilon) and post-processing
  - **Invariants**
    - Fewer invariants with DP
  - **Experts**
    - With DP, computer scientists introduced into discussions

Applying the handoff model

- *Modes of action* by which one component acts on or engages another (in what ways do its pieces connect?)
  - SDL → DP: "changes how the DAS *acts on the Census response data* in order to protect respondent's confidentiality, shifting the roles of *expert decision-making*"
    - Numerous swapping, rounding, suppression decisions → abstracted decisions, like setting epsilon
    - New set of experts (computer scientists) → new balance of power
  - Mode of "securing confidentiality" changed from expert evaluation → a statistical guarantee

Applying the handoff model

- *Functions* of a system (what does it do?)
  - SDL → DP: "[shifted] *how* the function of confidentiality preservation was enacted"
    1) "created new opportunities for transparency between the Bureau and interested publics"
    2) "allowed for formal, quantifiable validation f the privacy and confidentiality commitments actualized by the Bureau"
    3) "replaced one form of expertise with another" (i.e., computer scientists became integral to the decision-making process, whereas statisticians had a reduced role)

Value-laden shifts: Confidentiality

The Census Bureau… →	**Through the Handoff Lens →**	**Shifting Values & Functionality**
Switched from SDL to DP	Function of confidentiality is preserved, but how confidentiality is operationalized has changed in response to triggers	Reveals the **contested nature of confidentiality**

Slide courtesy of Amina Abdu

Value-laden shifts: Data Utility

The Census Bureau… →	**Through the Handoff Lens →**	**Shifting Values & Functionality**
Solicited feedback about what use cases data users value Reduced total number of counts not subjected to disclosure avoidance (i.e., invariants)	Changing system boundaries through decisions about what is inside and outside the scope of confidentiality protections	Demonstrates the significance of **data utility** as a function Concerns about **access to political and economic resources** are in tension with concerns about confidentiality

Slide courtesy of Amina Abdu

Value-laden shifts: Formalism

The Census Bureau… →	**Through the Handoff Lens →**	**Shifting Values & Functionality**
Framed parameter **epsilon** as locus of public participation	Functions now framed as **quantifiable trade-off** Experts evaluate and enact confidentiality through different **modes**	Prioritizes **formalized** notions of privacy and accuracy Expert decisions about data are **displaced**

Slide courtesy of Amina Abdu

Value-laden shifts: Transparency

The Census Bureau… →	**Through the Handoff Lens →**	**Shifting Values & Functionality**
Released significantly more information about disclosure avoidance system (e.g., source code, demo data, blog posts)	Transparency no longer a threat to the system's confidentiality function	**Transparency** emerges as a value of the DAS political process **Expert autonomy curtailed** by external scrutiny

Slide courtesy of Amina Abdu

Value-laden shifts: Participation

The Census Bureau… →	**Through the Handoff Lens →**	**Shifting Values & Functionality**
Attempted to solicit and scaffold both expert and public participation	Introduction of new experts and boundary objects as components in the DAS policy process	**Participation** is broadened, but with **insufficient support by trusted experts**

Slide courtesy of Amina Abdu

Lessons learned

1) The handoff lens is a critical tool for surfacing values
2) Beware objects without experts
3) Transparency and participation should center values and policy decisions

Slide adapted from Amina Abdu

Takeaways

- DP represents a useful mathematical formalization of privacy, but to fully understand its sociotechnical implications we must grapple with how it relates to privacy as an essentially contested concept
- Algorithmic privacy both reflects sociopolitical values and creates sociopolitical orders
- Frameworks from STS can help examine how DP functions in real-world contexts