

# CS 208: STS Perspectives on Privacy

April 19, 2022

# Agenda

- Approaches to Privacy
- STS Perspectives
- Politics of DP

Recap: 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)

“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)
- 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?

“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, and Doty 2016)

# Essentially contested concepts

W. B. Gallie (1956)

“Disputes about the concept’s ‘essence or meaning’ are both paramount and central to the concept itself”



# Essentially contested concepts

W. B. Gallie (1956)

- Democracy
- Art
- Freedom
- Privacy?

“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.”

(Mulligan, Koopman, and Doty 2016)

# STS Perspectives

# Social construction of technology (SCOT)

- 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

Trevor Pinch and Wiebe E. Bijker, "The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other."

# Politics of technology

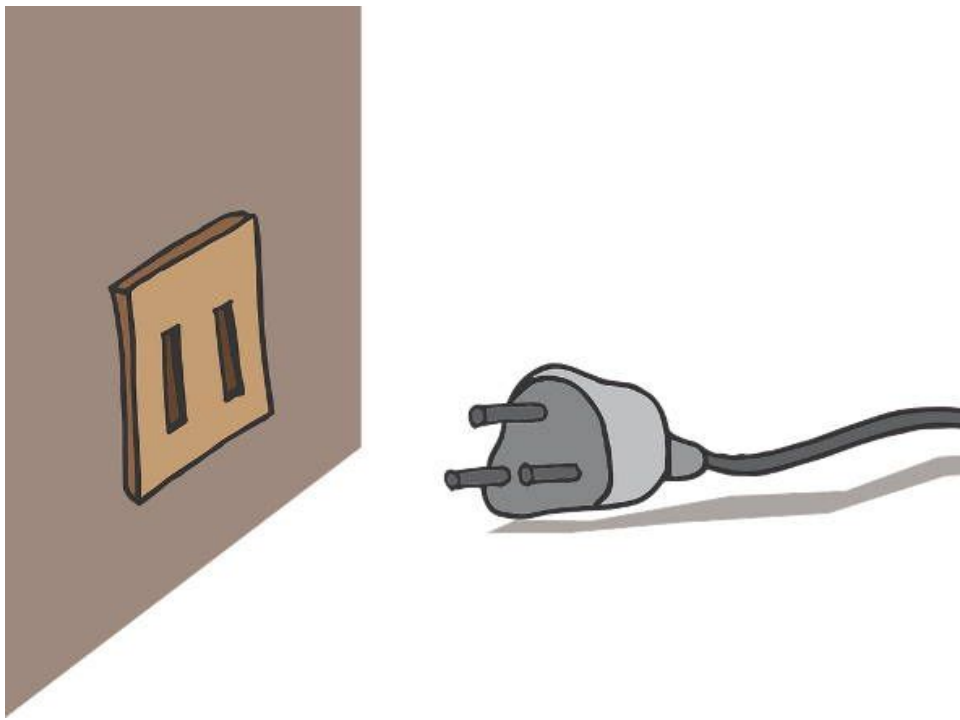
1. “Instances in which the invention, design, or arrangement of a specific technical device or system becomes a way of **settling an issue** in a particular community.”
2. “Systems that appear to require, or to be **strongly compatible with**, particular kinds of political relationships.”

# Discussion questions

- What are the social factors that shape DP?
- What are the politics of DP? How might it be used to “settle the matter,” or what political relationships might it be compatible with?
- How does DP address individual vs. collective privacy?

# The Politics of DP

- Algorithmic formalisms (Green and Viljoen 2019) of differential privacy do not account for social and contextual factors
- What are the entanglements between algorithmic privacy and institutional logics?
- What role can we play in constructing privacy-preserving sociotechnical systems?




Differential privacy

vs.

Institutional logics misaligned  
with privacy



Performing privacy

A man in a dark blue shirt and dark pants stands on a stage, gesturing with his hands. Behind him is a large screen displaying the text "Apple will not see your data" in white. The screen also features a large, faint, downward-pointing triangle in the bottom right corner.

Apple will not  
see your data

"Apple has put some kind of handcuffs on in how they interact with your data. It just turns out those handcuffs are made out of tissue paper."

- Frank McSherry, one of the inventors of differential privacy

## How One of Apple's Key Privacy Safeguards Falls Short

Apple has boasted of its use of a cutting-edge data science known as "differential privacy." Researchers say they're doing it wrong.

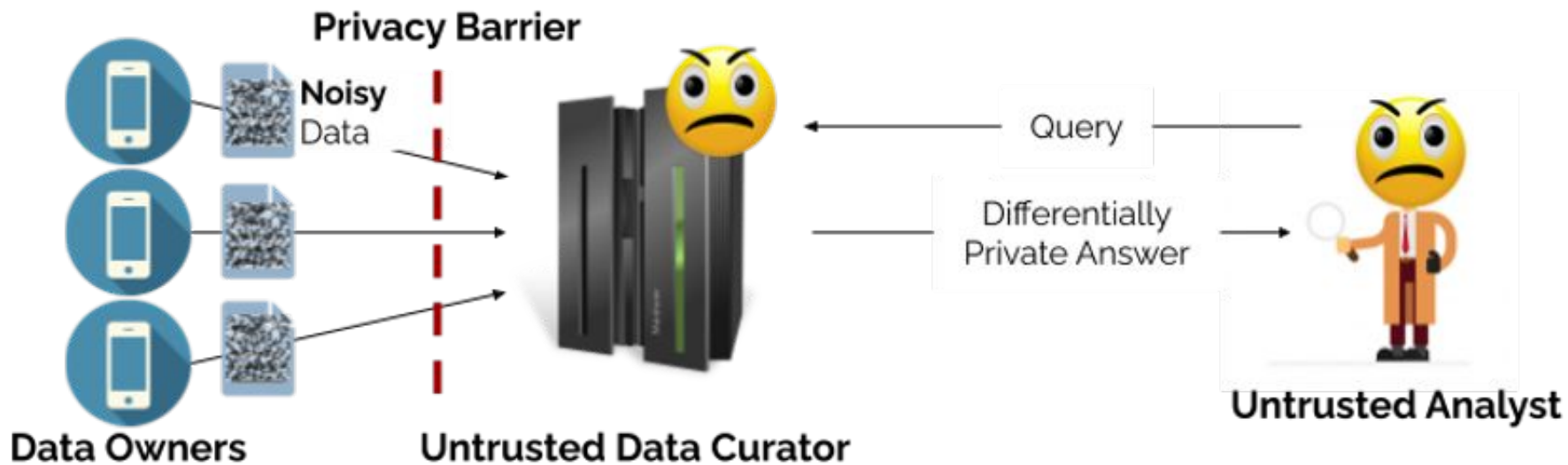
Using DP incorrectly

Foreclosing productive  
contestations

“Societal problems of data processing technologies — such as the ways they create distinctions and hierarchies that reinforce power, shape politics, or facilitate abuse — are **sidelined, redefined, or collapsed under the banner of ‘privacy’**, so that privacy-preserving computation techniques can be positioned as the solution.”

(Agrawal et al. 2021)

Reinforcing  
centralized power



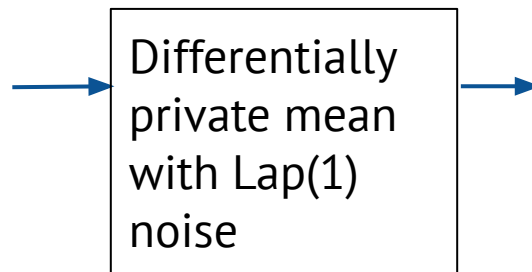
In current decentralized deployments, the central entity still controls the data flow

Incentivizing or hiding  
other privacy harms

Suppose we start with a weak DP guarantee...

Dataset d	Age	...	Sensitive status
Person 1	33	...	positive
Person 2	86	...	negative
Person 3	45	...	untested

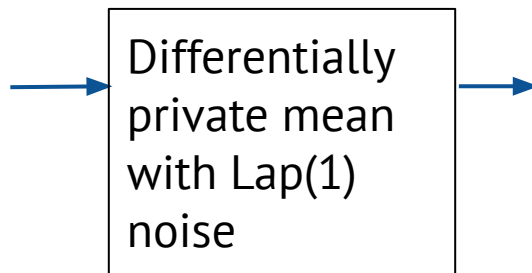
Dataset d





Dataset d	Age	...	Sensitive status
Person 1	33	...	positive
Person 2	86	...	negative
Person 3	45	...	untested
Person 1000000			positive

If we add more data as input, we will automatically get better DP guarantee. Is this desirable?



## Google COVID-19 Community Mobility Reports


The Community Mobility Reports are powered by the same world-class anonymization technology that we use in our products every day. For these reports, we use differential privacy, which adds artificial noise to our datasets enabling high quality results without identifying any individual person.

"This way, companies can still get insights about data that are valuable and useful to everybody without doing something to harm those users."

- Bryant Gipson, engineering manager at Google

Justifying collection of more  
sensitive data

Is this person a citizen of the United States?

- ☐ Yes, born in the United States
- ☐ Yes, born in Puerto Rico, Guam, the U.S. Virgin Islands, or Northern Marianas
- ☐ Yes, born abroad of U.S. citizen parent or parents
- ☐ Yes, U.S. citizen by naturalization – *Print year of naturalization*   

--	--	--	--
- ☐ No, not a U.S. citizen



Justifying collection of more sensitive data

If technology is  
political, we must  
engage in the politics.

1. Translate theoretical results into normative conclusions and collective action
2. Keep broader ethics/governance critiques in focus, even while strengthening technical architectures
3. Design protocols that are not just technically, but also institutionally, decentralized

# Conclusion

- Algorithmic privacy both reflects socio-political values and creates socio-political orders
- When institutional logics are misaligned with privacy, differential privacy can be exploited to perform trustworthiness, foreclose contestations, justify other privacy harms, and reinforce centralized power
- We must co-construct technology and society according to broader understandings of privacy