DIFFERENTIAL PRIVACY IN CONTEXT

Sophie Gibert, Embedded EthiCS @ Harvard

10 March 2022

PREPARING FOR DISCUSSION

Today we'll be doing some small-group discussion!

Take a minute to find a group of 2-3 people and introduce yourselves

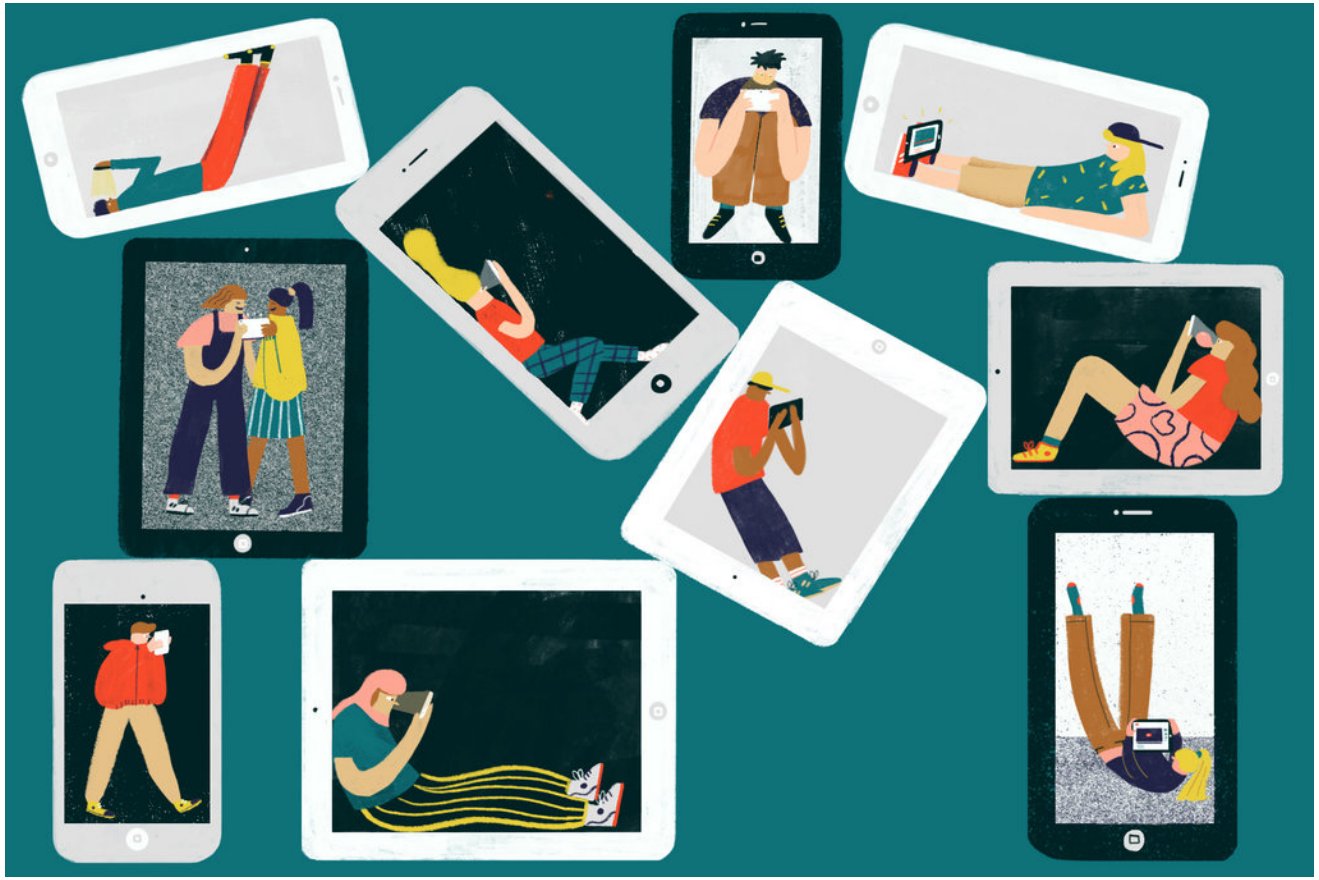


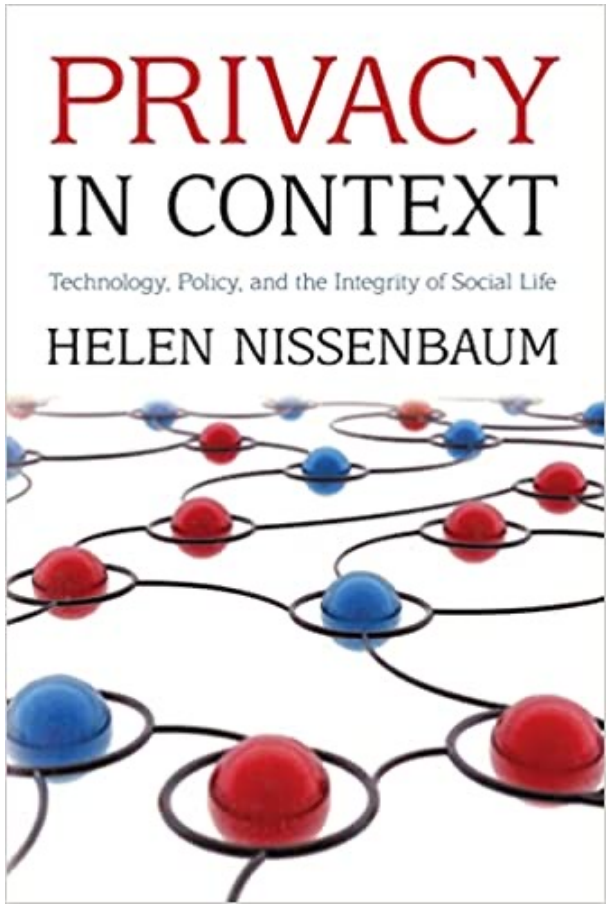
Illustration by Hannah Jacobs

TODAY'S TOPIC

Contemporary information practices can be enormously beneficial; they can also provoke intense concern about privacy.

Two questions:

- When and why do certain information practices provoke *legitimate* privacy concerns?
- When and *to what extent* do the tools of differential privacy *address* legitimate privacy concerns?



TODAY'S PLAN

1. Introduce the framework of *contextual integrity*
2. Activity: Apply the framework to a fictionalized case in which the tools of differential privacy are used
3. In light of the activity, reflect on the strengths and limitations of differential privacy when it comes to addressing privacy concerns

INTRODUCING THE FRAMEWORK OF *CONTEXTUAL INTEGRITY*

AN OBSERVATION

Information flows differently in different contexts

- Friendship: Reciprocal, voluntary, confidential
- Health care: Unidirectional, compelled, confidential within limits, restricted in scope, codified

MAIN CLAIMS

Some informational norms are appropriate to a given context, and some are not

- What makes a norm appropriate to a context is (in part) that it supports the attainment of the context-specific values and goals

Privacy is *the context-appropriate flow of information*

- Privacy is breached when and because there is a disruption in the context-appropriate flow of information—i.e., a disruption in how information *should* flow in the context
- A technology or information practice raises *legitimate* privacy concerns when and because it disrupts the context-appropriate flow of information—i.e., it causes information to flow in a way that it *shouldn't* in the context

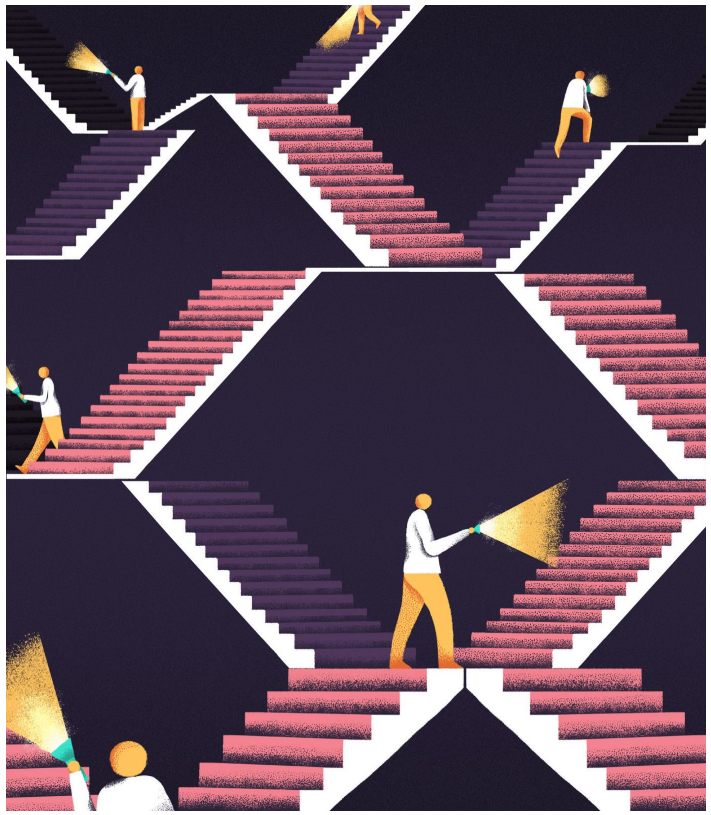


Illustration by Fran Pulido

A THREE-STEP FRAMEWORK

Suppose we want to know if there are any legitimate privacy concerns to be had about the monitoring and tracking of individuals' web searches by search engine companies such as Google and Bing

Three steps:

- **Explain** how (if at all) the technology or practice disrupts the way information is normally expected to flow in the relevant context
- **Evaluate** whether these disruptions serve general and context-specific values and goals
- **Prescribe** – make a judgment about whether the technology or practice should be abandoned or changed

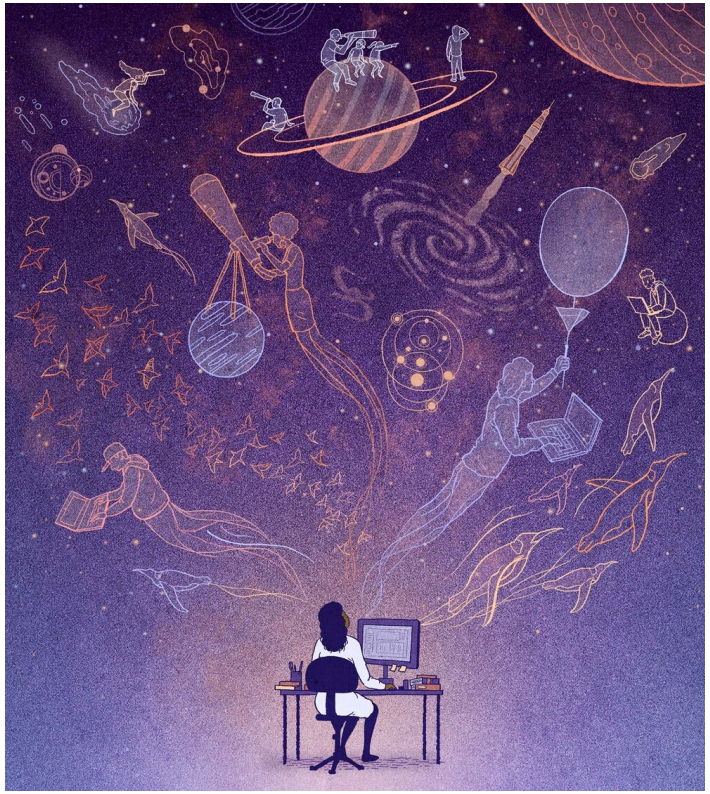
STEP 1: EXPLAIN

Explain how (if at all) the technology or practice disrupts the way information is normally expected to flow in the relevant context

a. Locate the relevant social context

- The idea: Technologies are embedded in the social world; they serve to extend existing social contexts
  - Shopping online is an extension of shopping in person
  - EZ-pass transmitter system is an extension of cash tolls
  - Searching the web is an extension of **visiting a library***

*When in doubt, look for similarity of *function*



Illustrated by Antoine Dore

Illustrated by Andrea De Santis

EXPLAIN (CONTINUED)

b. Describe how information normally flows in that context
   - *Who* shares *what kind* of information *with whom*, and *how?*
   - Strict confidentiality; Maintenance of records only for the purpose of monitoring the whereabouts of holdings; Only what you check out is recorded

c. Identify ways in which the technology or practice disrupts that information flow
   - Sharing web search information with third parties, including with government actors and advertisers
   - Micro-targeting ads based on individuals' search histories
   - Collecting much more specific information

STEP 2: EVALUATE

Evaluate whether the disruptions identified in Step 1 serve general and context-specific values and goals

Individual Values

- Liberty of thought and action
- Protection from harm and exploitation

Societal or Collective Values

- Fair distribution of power and opportunity
- Equal treatment
- Democracy

Illustration by Brian Rea

EVALUATE (CONTINUED)

Context-specific values and goals

- *Healthcare*: Curing disease, alleviating suffering, improving wellbeing
- *Commercial*: Free market, in which buyers and sellers are informed and free to choose
- *Web search:* Informing people, allowing for free speech, association, and expression, maintaining an autonomous and informed citizenry

Illustration by Davide Bonazzi

STEP 3: PRESCRIBE

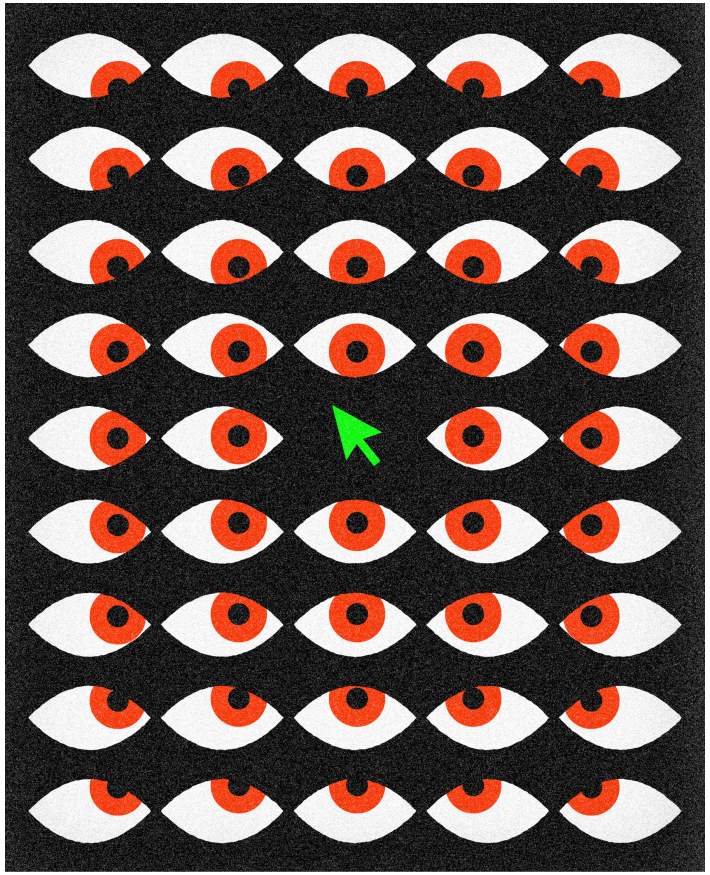
Prescribe – make a judgment about whether the technology or practice should be abandoned or changed

Nissenbaum's prescription for web search companies:

> "As long as search engines serve a critical function of finding information, people, and communities on the web, and as long as the web continues to function as a critical repository of information, a venue for self-development, inquiry, expression, association, and so forth, **confidentiality is a necessary principle for information norms governing search query logs"** (2010, p. 198).

IN SUM

According to *privacy as contextual integrity*, privacy is **breached** when and because the technology or information practice **disrupts** the way that information normally flows in the context it's embedded in, **in a way that does *not* support general and context-specific values and goals**



ACTIVITY: APPLYING THE FRAMEWORK

FICTIONALIZED CASE: “COACHABLE”

QUESTIONS 1-4

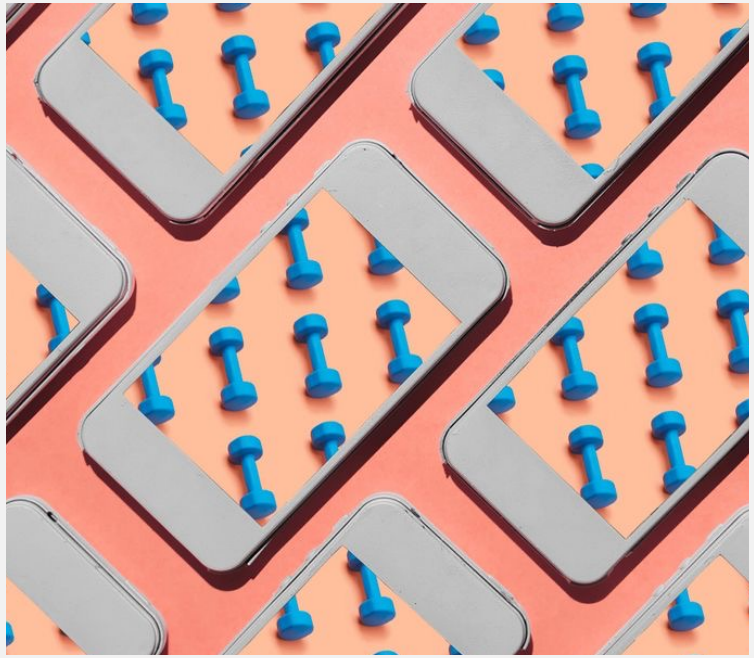
Step 1 involves describing how, if at all, Coachable's practices disrupt the way that information normally flows in the relevant social context

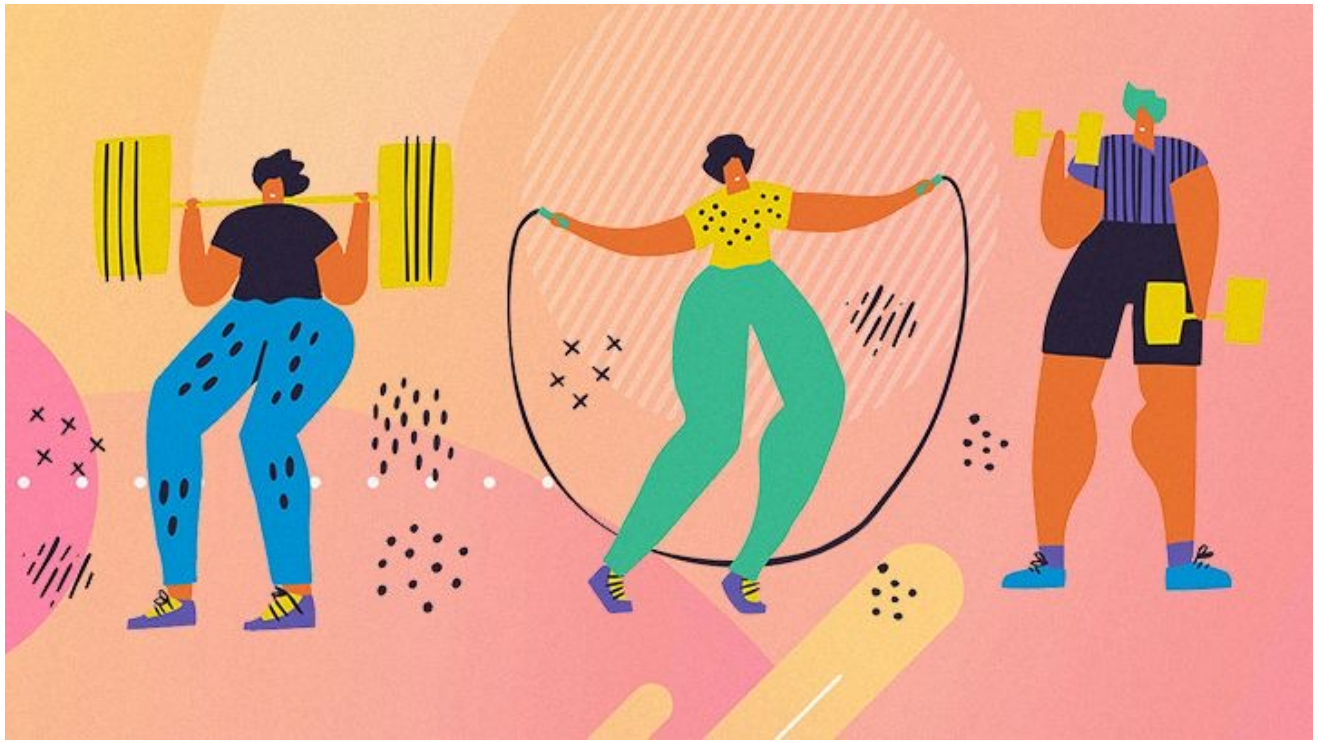
- **Question 1** asks you to describe how information flows in the case as described
- **Question 2** asks you to describe how information would normally flow in a relevant social context
- **Question 3** asks you to identify any differences
- **Question 4** asks you to think about the role differential privacy is playing

QUESTIONS 5-8

Step 2 involves evaluating any disruptions in light of general and context-specific values and goals

- **Question 5** asks you what individual values are at stake
- **Question 6** asks you what societal values are at stake
- **Question 7** asks you what context-specific values and goals are at stake
- **Question 8** asks you to make an evaluation





QUESTION 9

Prescribe! Based on your evaluation, what (if anything) should Coachable do differently?

TAKING A STEP BACK

How does the concept of differential privacy differ from the concept of privacy as the context-appropriate flow of information? When might the two come apart?

When and to what extent do the tools of differential privacy *address* legitimate privacy concerns? What kinds of privacy concerns do they tend to address?

ASSIGNMENT: EXTENSION OF THE “COACHABLE” CASE

THANK YOU!

Contact: Sophie Gibert,
sgibert@g.harvard.edu

Survey: https://tinyurl.com/CS208S22

REFERENCES

Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Nissenbaum, Helen. 2011. “A Contextual Approach to Privacy Online.” *Daedalus* 140 (4): 32-48.

Nissenbaum, Helen. 2016. “Differential Privacy in Context: Conceptual and Ethical Considerations.” Talk at the *Institute for Advanced Study at Princeton University*: https://www.youtube.com/watch?v=Nefc4ey9XMU