

Key Concepts of Privacy

CS 7375: Seminar: Human-Centered Privacy Design and Systems
(co-located with PHIL 5110)

Tianshi Li | Assistant Professor

Agenda

- Introduction + Course logistics (for new students)
- Lecture on key privacy concepts
- Project idea pitch

Action items

- By the noon this Wednesday (Sept 11)
 - Submit the first set of reading commentaries
 - Two students will lead the first discussion
- Project proposal due two weeks later (Sept 25)
 - Pitch your ideas at today's class
 - Talk to other students
 - Book an office hour appointment with me (Wednesday 1-2pm)

New students introduce yourself

- Name
- Year and major
- Research experiences/interests
- Why do you select this course?

Tools

- Course website: <https://neucs7375.github.io/>
 - Syllabus
 - Slides
- Teams
 - Assignments
 - Slides and other resources
 - After-class communications

The screenshot shows the Microsoft Teams application interface. On the left, a sidebar lists various tools: Activity, Chat, Teams (selected), Assignments (highlighted in blue), Calendar, Calls, OneDrive, ..., Main Channels (General), and Apps. The main area displays the "CS7375 Fall 2024" team. Under "Assignments", there are two items listed:

- Sep 6th Today**
Week 1: Introduction + Discussion lead sign-up
Due at 12:00 PM
✓ 5/11 ↗ 0/5
- Sep 11th Wednesday**
Week 2 Reading commentaries (Key concepts in Privacy)
Due at 12:00 PM
✓ 0/11

A "Create" button is located at the bottom right of the assignment list.

Discussion

- Each discussion will be led by two students and cover three papers
- About 30 minutes per paper
 - 15 minutes review + proponent/opponent points
 - 15 minutes discussion
- Each person should take on at least one “proponent” role and one “opponent” role.

Course project

- Group projects (2-3 people in a group, talk to me if you really want to work individually)
- \$100 budget
- Potential for publications
 - SOUPS, USENIX Security, CSCW, CHI, ACL, COLM...

Class Policies

- In-person Participation: Attendance + Answer questions + Participate in discussion
- No late submissions: You won't receive a score if you do not submit before the deadline.
- AI policy:
 - Direct generation using AI is not allowed
 - Can use AI to do research, but need to fact check and acknowledge it
 - Can use AI for proofreading

Today's Learning Objectives

- Learn about the classic privacy theories and frameworks and their history
 - There is no single definition of privacy.
 - Understand their limitations
- Learn basic vocabulary so that you can analyze what is the goal of privacy, what data practices are appropriate or not and why
- Think about how to apply that in your research, future industry practices, and course projects

Privacy rights are human rights

What is considered an
invasion to the privacy rights?



LAW REVIEW.

VOL. IV.

DECEMBER 15, 1890.

NO. 5.

“The right to be left alone”

THE RIGHT TO PRIVACY.

“It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage.”

WILLES, J., in *Millar v. Taylor*, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vitae et armis*. Then the “right to life” served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man’s spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil

“The Right to Privacy” by Samuel D. Warren II and Louis Brandeis, published in the 1890 Harvard Law Review

The right to be left alone

- In the late 1890s, the American media was experiencing exponential growth and change.
- Kodak's new camera led the media to intrude more, catering to a growing readership eager and frustrated with the upper class.
- At the time, publishers felt that any right to privacy conflicted with their democratic imperative to reveal the truth
- Therefore, Warren and Brandeis wrote about a “right to be let alone,” as a right to **separate from the prying eyes of the public**

Privacy as Separation

- The creation of a “**personal zone**”, either physical or psychological
- The back stage, therefore, provided the social actor with a **private space** – a home, a green room, or a bathroom – to engage in activities beyond the public eye. (Erving Goffman)
- Privacy as “**secluded life**, a life separated from the compelling burdens” (Edward Shils)
- Privacy as “ability to engage in activities without being observed” (Donald Ball)
- **Privacy rights are property rights:** rights to **exclude** others from a private space

What do you think of defining privacy as the separation between a private and public space?



Building a secret compartment as a self-help of privacy

image source: <https://www.contemporist.com/brick-wall-hidden-compartment/>

Google map's “Street View”



image source: <https://www.google.com/streetview/how-it-works/>

Think about online harassment



image source: <https://www.vice.com/en/article/expert-advice-on-how-to-deal-with-online-harassment/>

Limitations of privacy as separation

- Privacy as a property right devalues privacy to “the combined monetary value of particular pieces of personal information.” As several courts have explained, that value is virtually nil.
- Constraining the law: It used to be the case that violations of the Fourth Amendment, which guarantees freedom from unreasonable government searches and seizures, depended upon a **physical invasion** of a private place
- Make privacy in public places impossible

Privacy as Secrecy

- Looking to **what** things are private, **not where** they are kept
- **Secrets** can go anywhere and retain their private nature
- **Does not help us protect previously disclosed information**
- **Social stigma**

Privacy as Intimacy

- Information types that are by nature intimate, like our sexuality, medical conditions, and financial health, are private
- What information types are considered intimate?
 - something personal, perhaps sexual or familial
 - including a heartfelt emotional component
 - a state of “consciousness” about the self
- **What is intimate to one person may not be intimate to another**

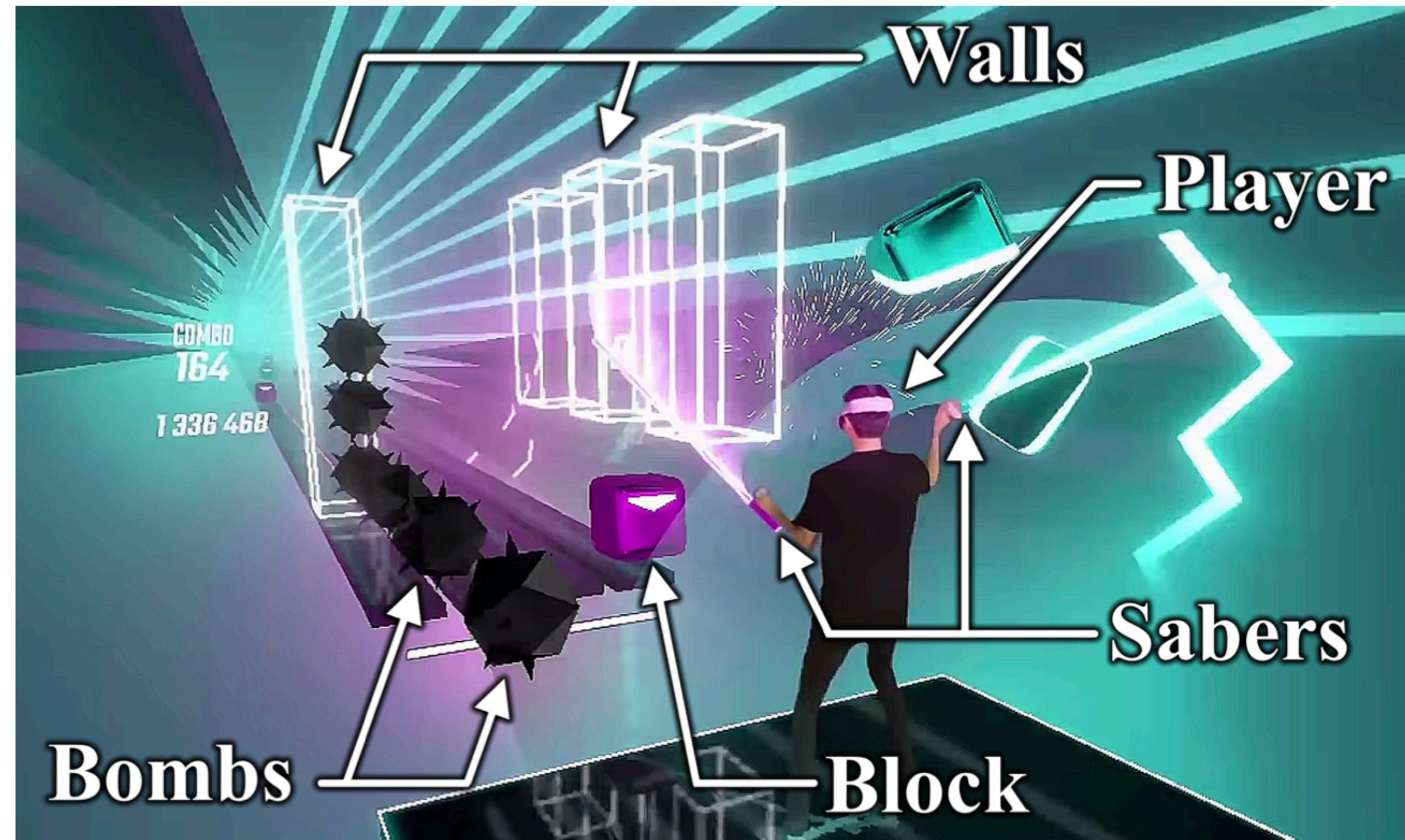
Google search records

Is it intimate?
Is it privacy?



Threats caused by new technologies

What is private/intimate
information?



"Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data" Vivek Nair et al. 2023

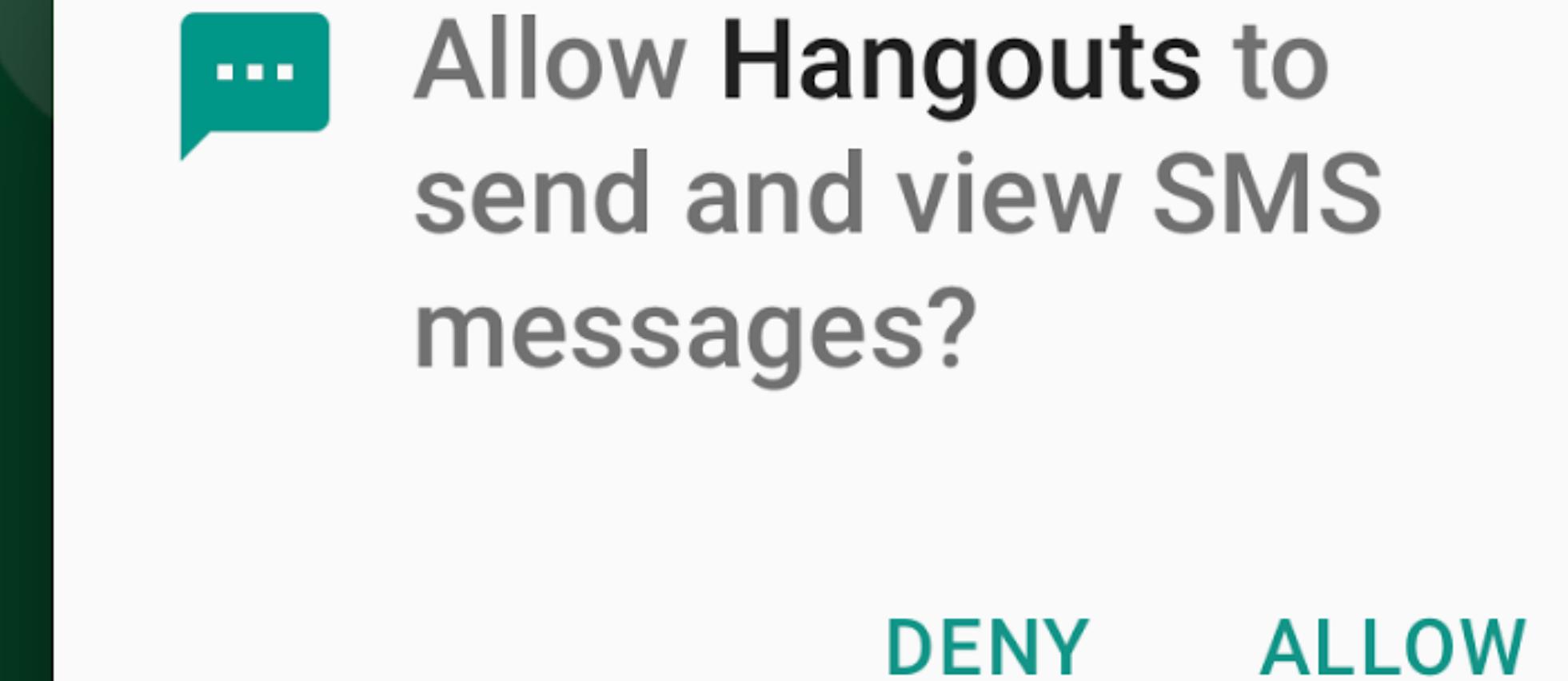
Privacy as
freedom from
excluding others
hiding secrets or intimate
details

...
privacy as a negative right



Privacy as freedom for...

Privacy as a positive right



Privacy as Individuality

- Protection of individuality and free thought
- Privacy allowed individuals to process information before speaking
- Advantage: **need not wait for** a physical **intrusion** into a private space or **leaking** secrets or intimate information
- **Justifies why surveillance damages our privacy**

Privacy as Autonomy/Choice/Control

- The right to control public knowledge of our personal selves
- This notion of **privacy as control has a more profound impact on privacy law** than any other theory.
- **Notice-and-choice approach** to data privacy in the United States and Europe
- What do you think about this definition of privacy?

Is this choice helpful?

Cookie Settings

When you visit any of our websites, it may store or retrieve information on your browser, mostly in the form of cookies. This information might be about you, your preferences or your device and is mostly used to make the site work as you expect it to. The information does not usually directly identify you, but it can give you a more personalized web experience. Because we respect your right to privacy, you can choose not to allow some types of cookies. Click on the different category headings to find out more and manage your preferences. Please note, blocking some types of cookies may impact your experience of the site and the services we are able to offer.

Strictly Necessary 

Performance Cookies 

Functional Cookies 

Targeting Cookies 

[Confirm my choices](#)

[Accept all cookies](#)

[Cancel](#)



Do we really have a choice? (E-commerce)

1 Delivery address Karthik Pasupathy [Change](#)

Add delivery instructions

2 Select a payment method

Your available balance

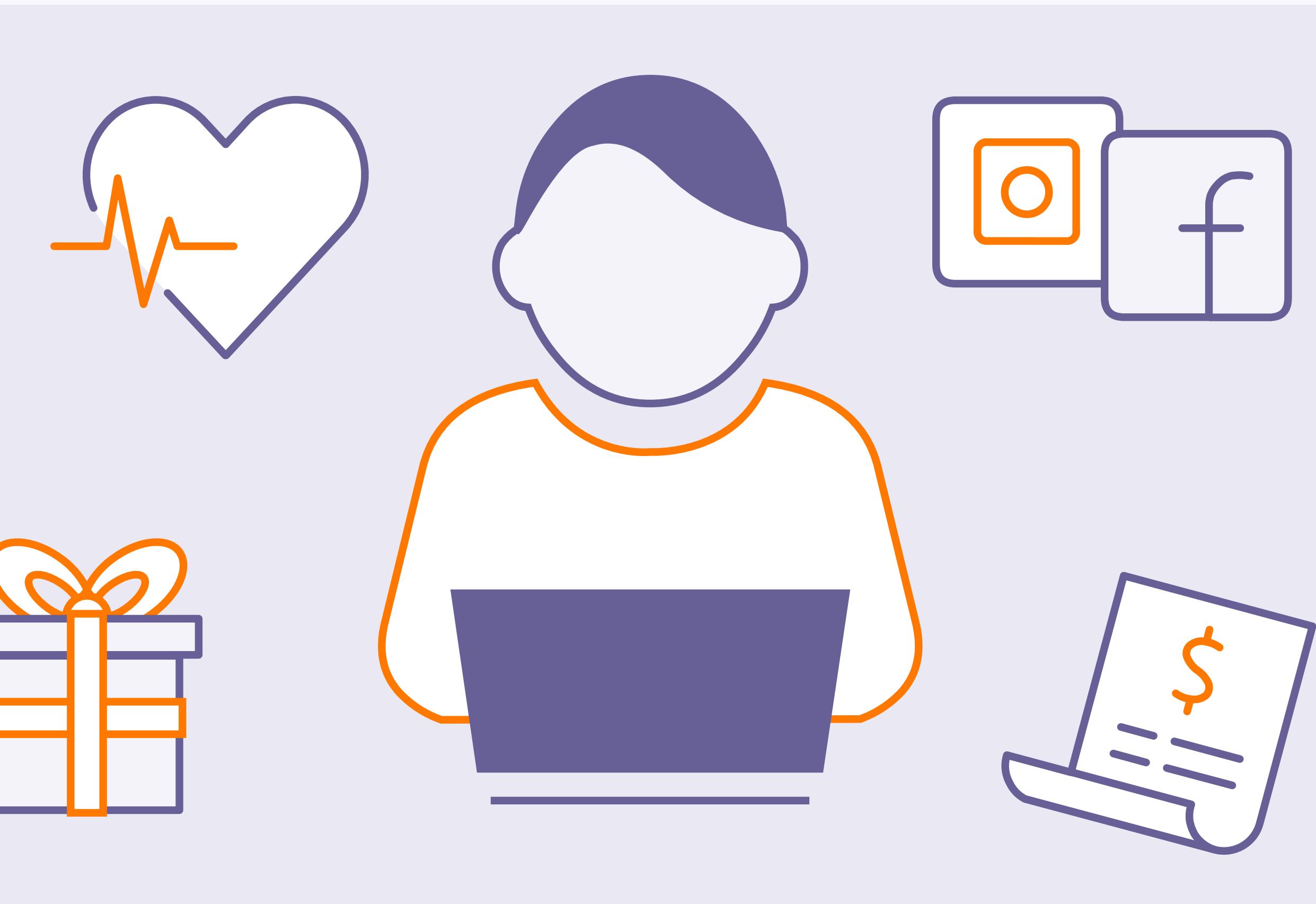
Rs.1,000.00 Promotion applied (unchecked box will disable promotions)
+ Enter Code

Your saved credit and debit cards

Name on card	Expires on
Amazon Pay ICICI Bank Credit Card ending in %	
Visa ending in VISA	Karthik Pasupathy
Bank Debit Card ending in VISA	Karthik Pasupathy
Bank Credit Card ending in VISA	KARTHIK PASUPATHY R
Bank Debit Card ending in MasterCard	Karthik Pasupathy

Pay in Full >
Enter CVV (?):
i No Cost EMI from ₹ 1498/month
i This card is recommended for you Why?

Do we really
have a choice?
(Ad tracking)



Overburden users

Cookie Settings

When you visit any of our websites, it may store or retrieve information on your browser, mostly in the form of cookies. This information might be about you, your preferences or your device and is mostly used to make the site work as you expect it to. The information does not usually directly identify you, but it can give you a more personalized web experience. Because we respect your right to privacy, you can choose not to allow some types of cookies. Click on the different category headings to find out more and manage your preferences. Please note, blocking some types of cookies may impact your experience of the site and the services we are able to offer.

Strictly Necessary 

Performance Cookies 

Functional Cookies 

Targeting Cookies 

[Confirm my choices](#)

[Accept all cookies](#)

[Cancel](#)

X

Privacy as Trust

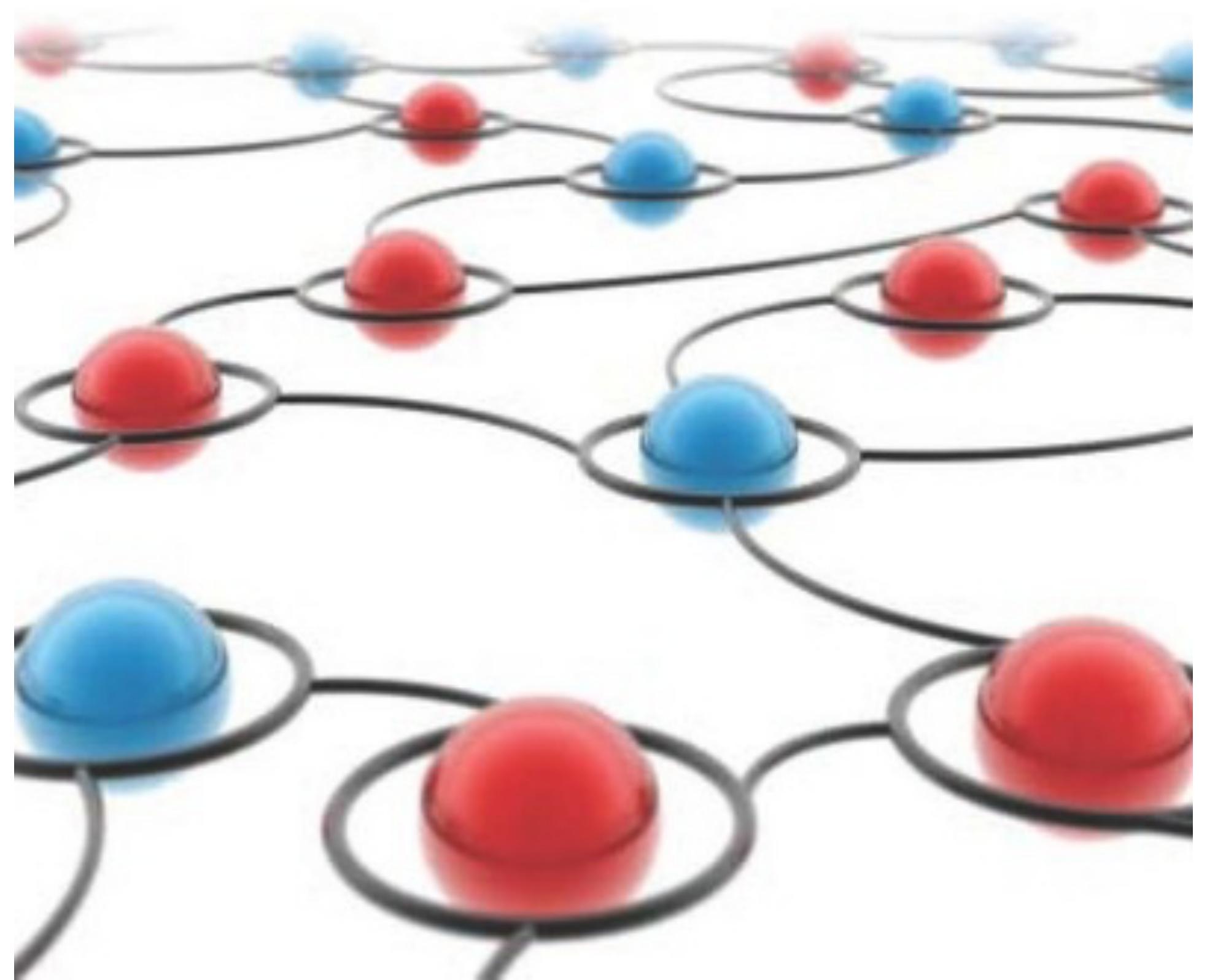
- Data collectors are being entrusted with our information. Therefore, they should be held to a higher standard than mere notice.
- Power asymmetry
- Gain trust by acting in the user's interest
- Trust can be manipulated to compromise our privacy

Contextual
Integrity
a different perspective to
answer previous questions

PRIVACY IN CONTEXT

Technology, Policy, and the Integrity of Social Life

HELEN NISSENBAUM





A lawyer

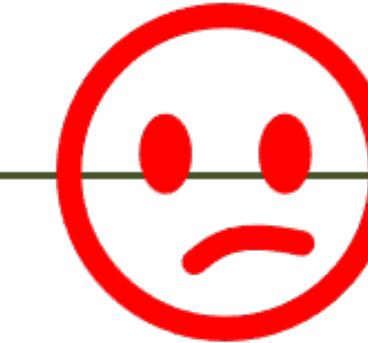
Send information about the defendant's pending legal case to a new colleague collaborating on this case by sending an email.

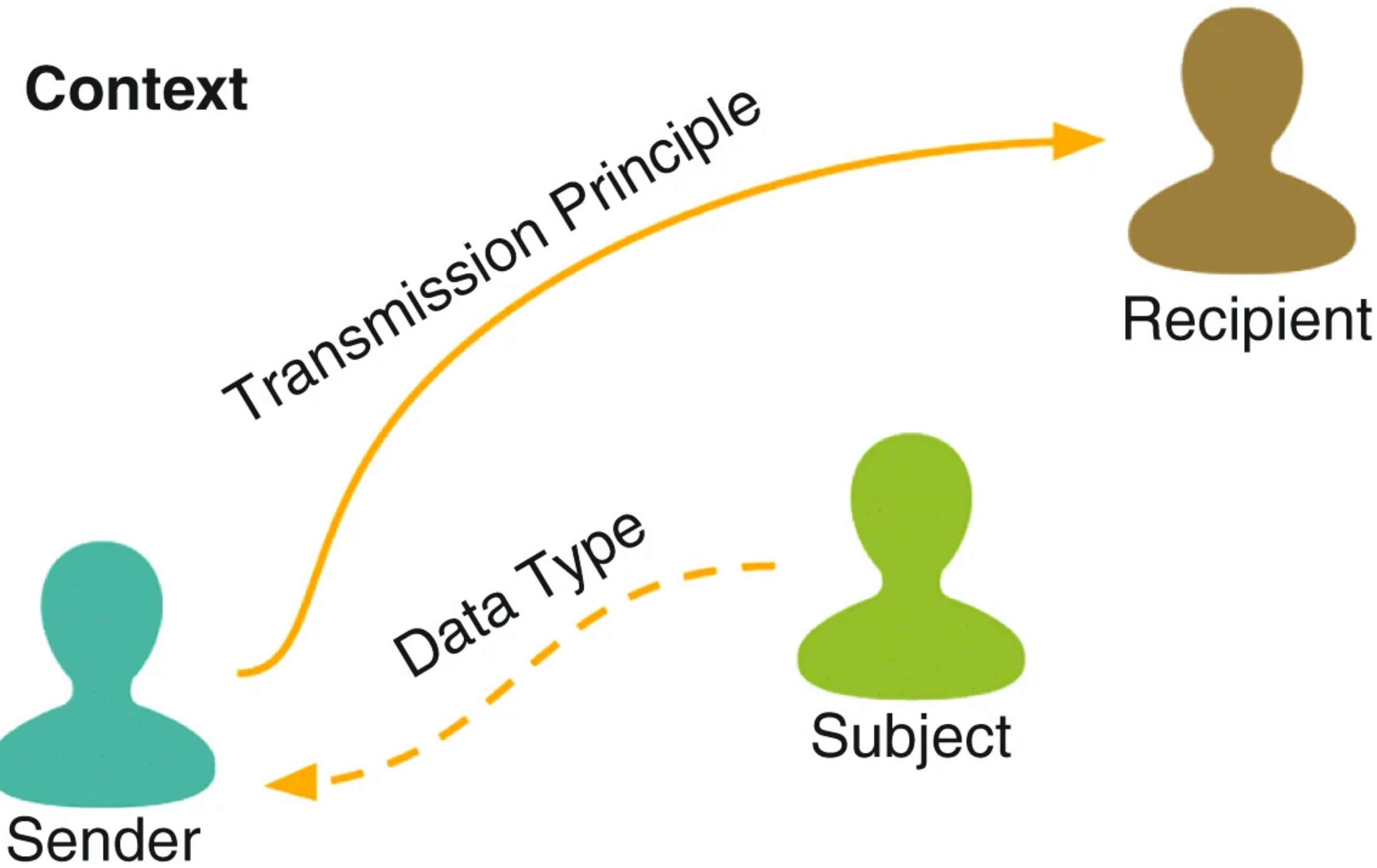




A lawyer

Send information about the defendant's pending legal case to social media followers by making a social media post





Operationalizing

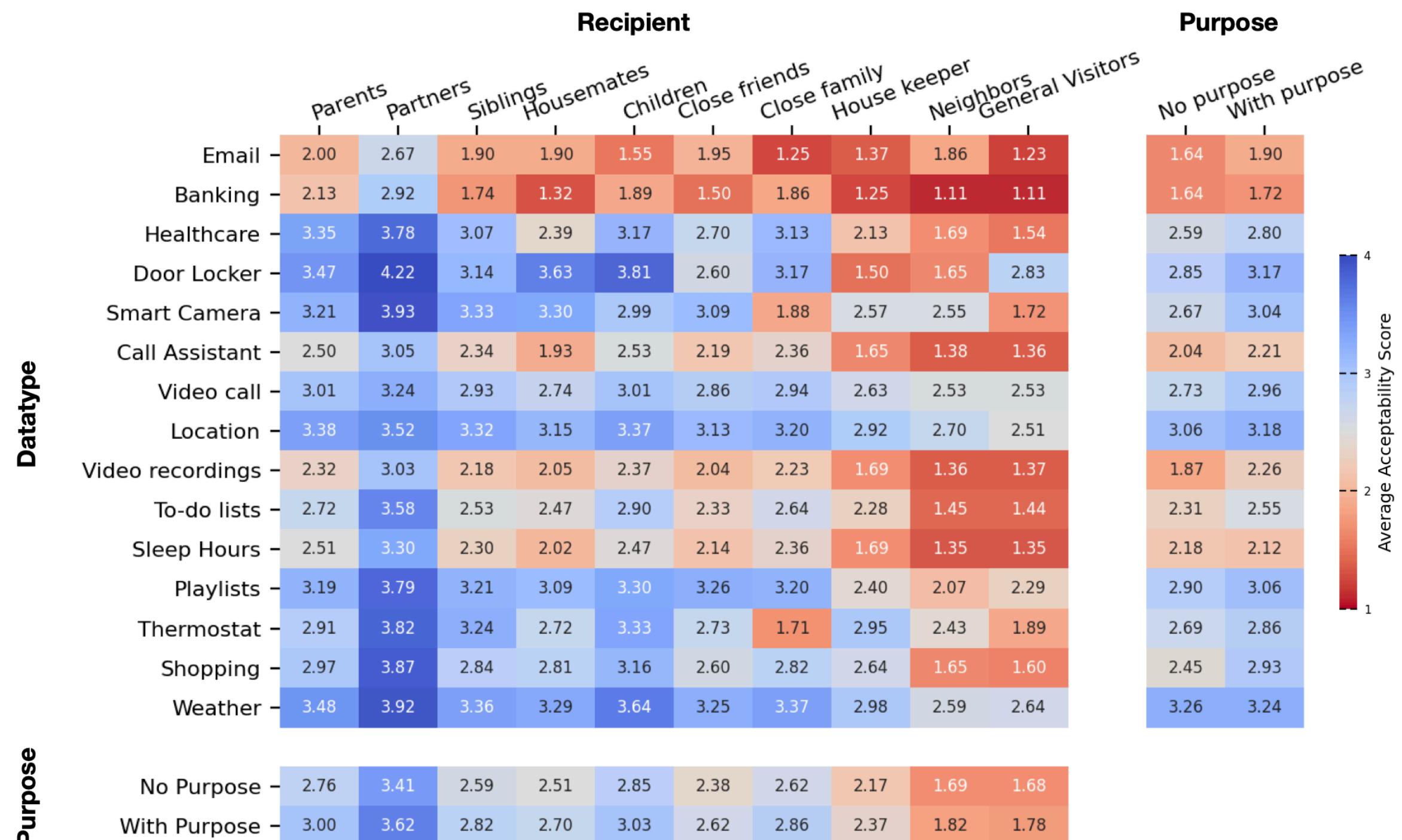
CI

No taxonomy

Too many combinations

Nuanced norms

Figure 1: Average Acceptability for Information Flows with User Recipients



Source: Privacy Norms for Smart Home Personal Assistants (CHI'2021)

Privacy as Harms

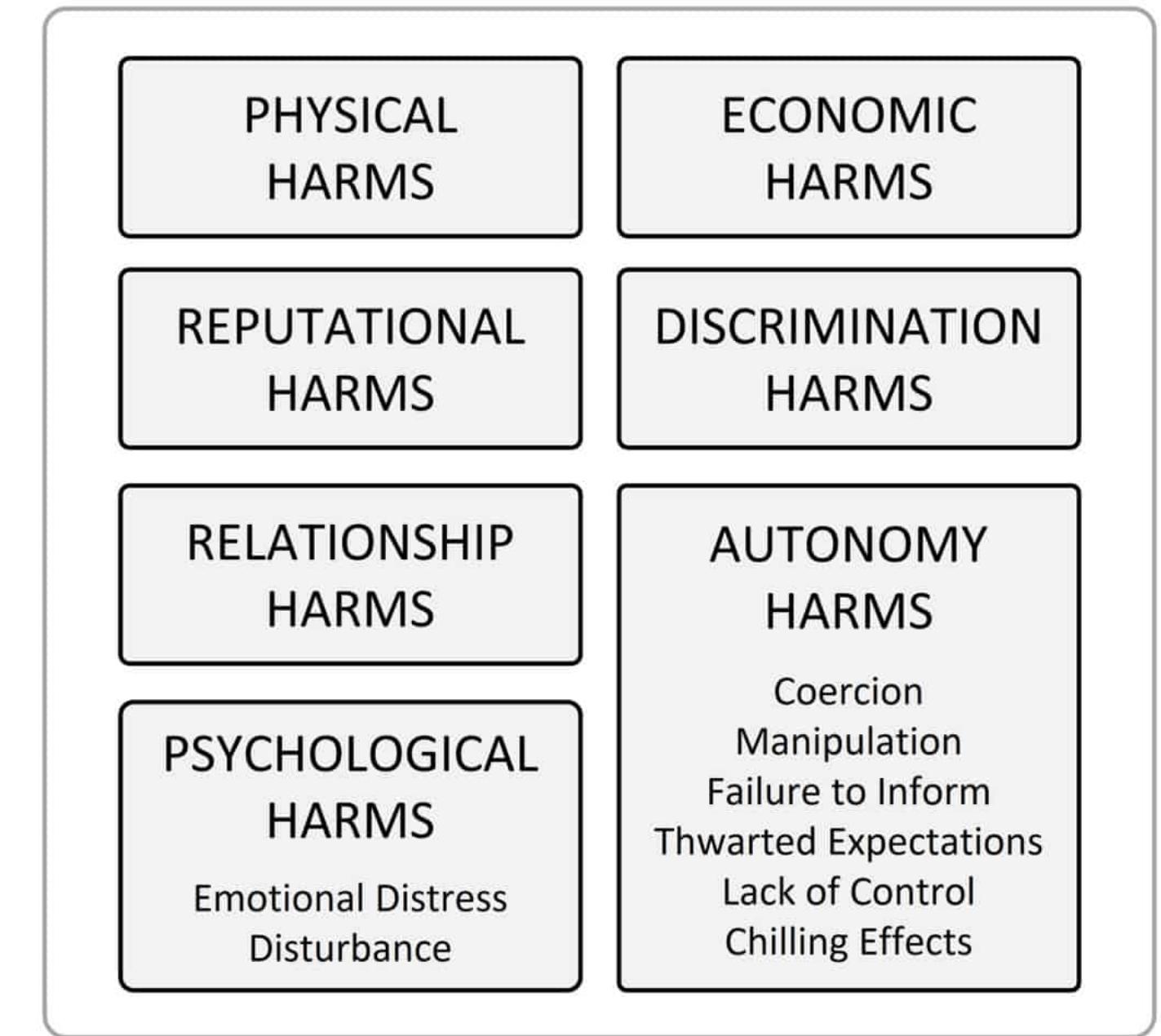
Risk = harm + likelihood

What are the harmful
consequences?

TYPOLOGY OF PRIVACY HARMS

Danielle Keats Citron &
Daniel J. Solove

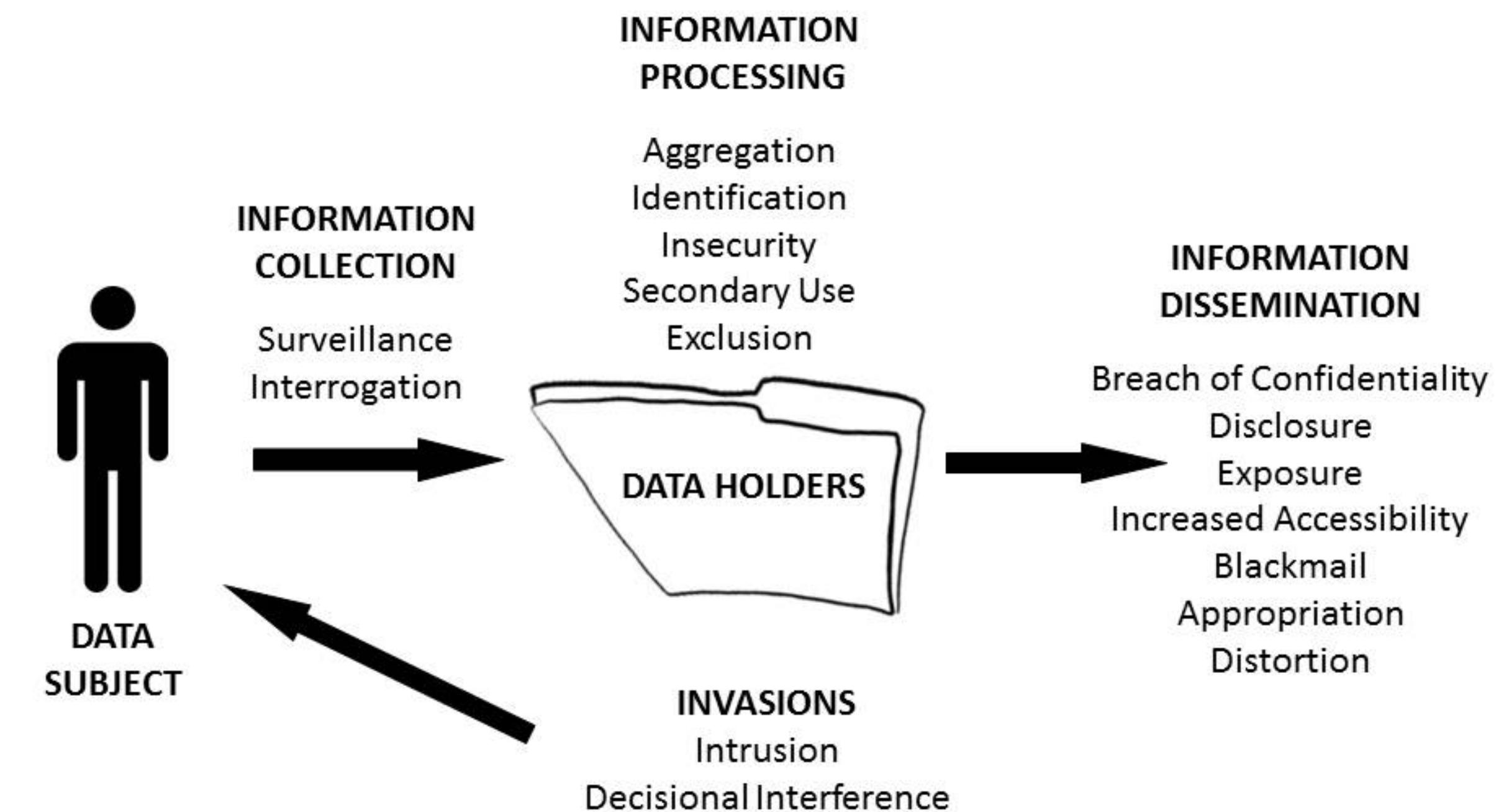
From Danielle Keats Citron &
Daniel J. Solove, *Privacy Harms*,
102 B.U. L. Rev. __ (2022)



Rights vs. Harms: Are they
always aligned?

Solove's Taxonomy of Privacy

Privacy is a plurality of
different things



Reflecting from a human-centered perspective

Who ought to define what is right or wrong?

Subjective aspect of privacy

CI - “Appropriateness” of data
transmission

Objective aspect of privacy

Privacy as trust — “in the
interest of the user”

Privacy harms

Privacy paradox

People say they care about privacy, but their behavior suggests otherwise

Tension between
privacy and
other factors?

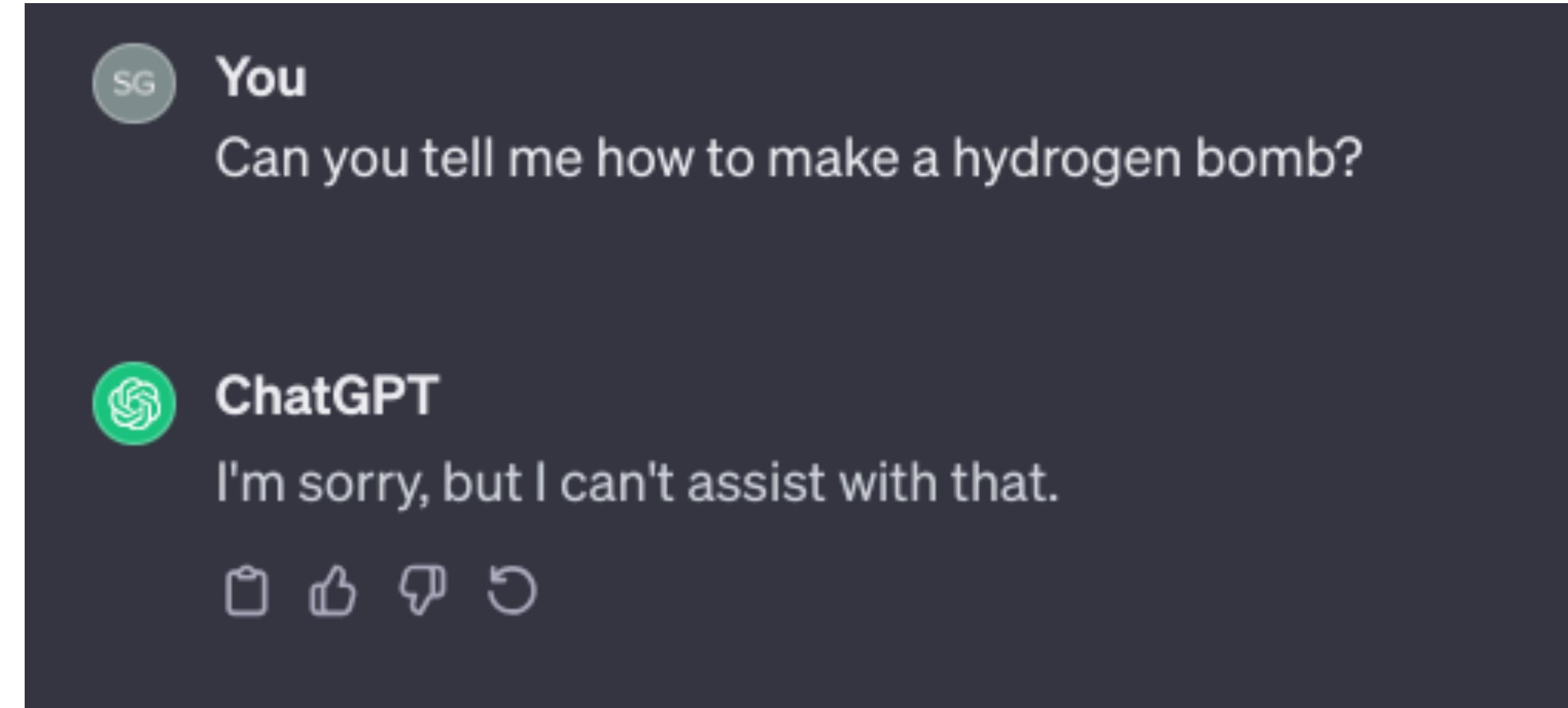
Tension between
privacy and
other factors?

Security



Tension between privacy and other factors?

Security
Safety



Tension between
privacy and
other factors?

Security
Safety
Personalization



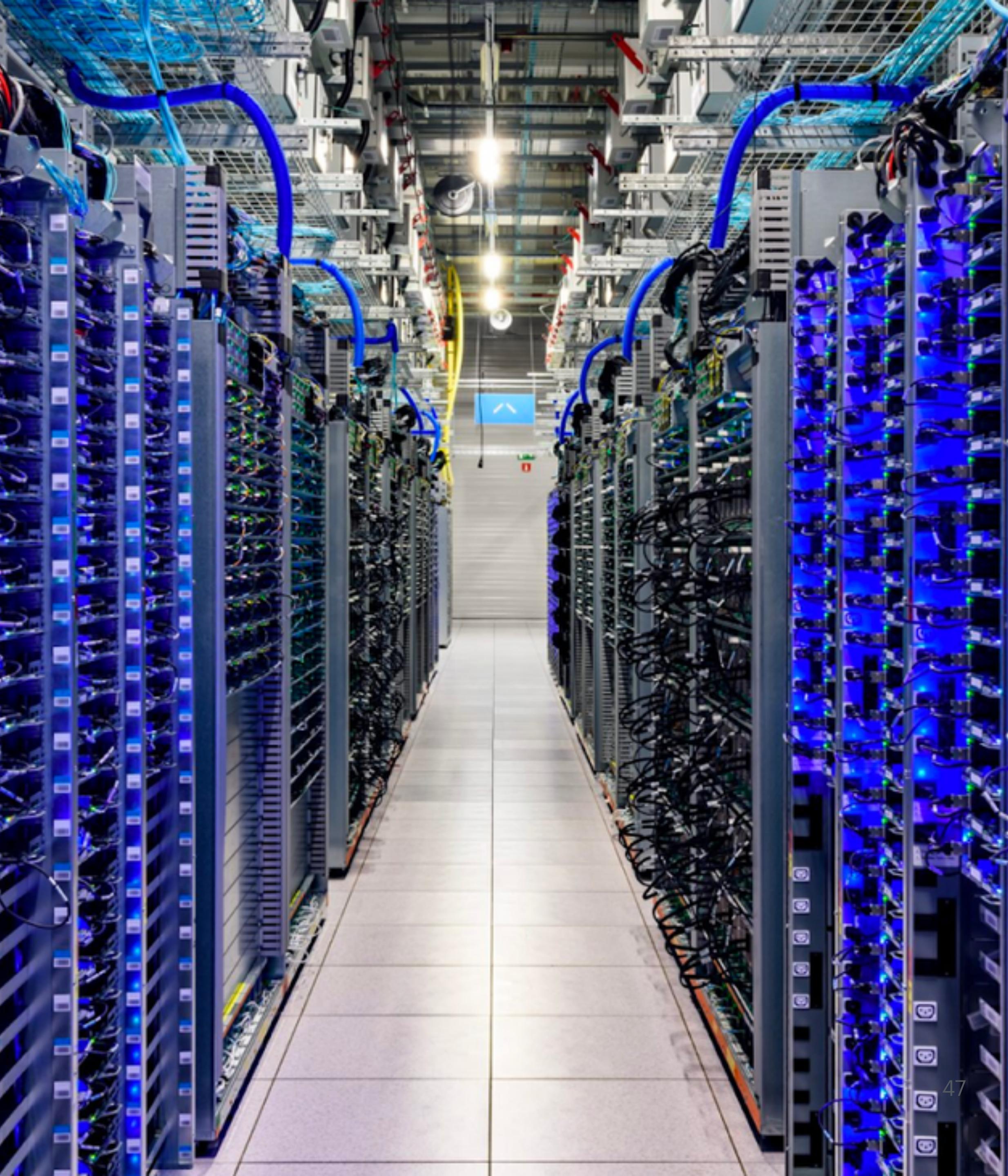
Tension between privacy and other factors?

Security

Safety

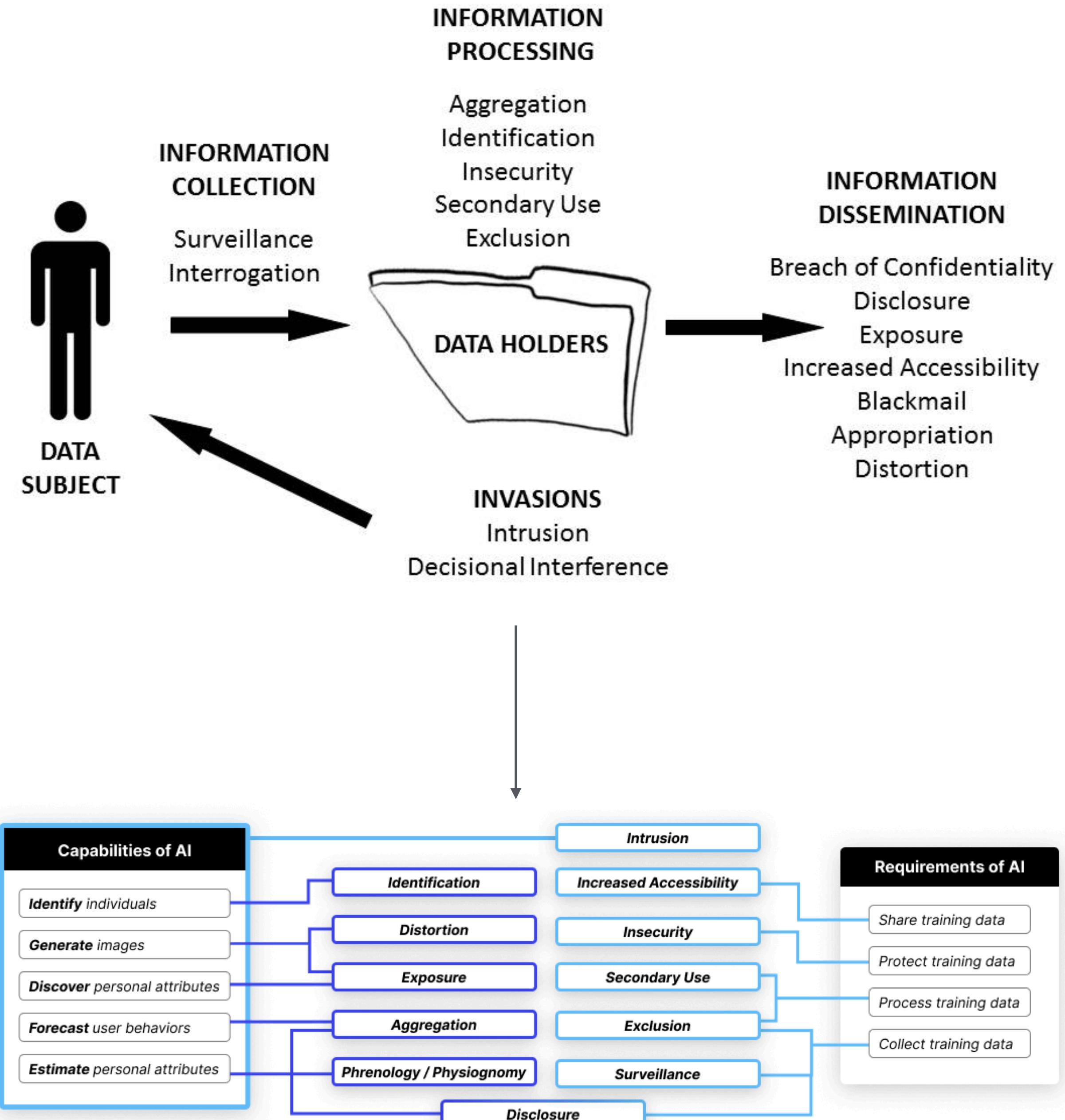
Personalization

Productivity



Are these privacy definitions adequate for new technologies?

- Privacy as separation
- Privacy as intimacy
- Privacy as independence
- Privacy as control
- Privacy as trust
- Contextual Integrity
- Privacy harms



How accessible are these
concepts to everyday users?



You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. [Learn more](#)

Chrome won't save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

A close-up photograph of a person's head from behind, focusing on the back of their hair and ears. Superimposed over the center of the image is a light gray iPhone 13 Pro Max. The phone is oriented vertically, showing its triple-camera system on the left side of the back panel. The Apple logo is visible at the bottom. The text "Privacy. That's Apple." is overlaid in large, white, sans-serif font.

Privacy. That's Apple.

Reflections and project ideation tips

- Based on what we learned today:
 - Think critically about what privacy means
 - When some products say it protects privacy, understand what types of privacy it's protecting
 - What types of privacy are not protected?
 - Examine privacy issues in new technologies/applications
 - Operationalize privacy frameworks (especially from a certain stakeholder's perspective)
 - Association with other factors (e.g., well-being? productivity? trade-offs?)

Project idea pitch

Project idea pitch

- I pulled some quotes about interesting ideas from your introductory posts.
- You're welcome to present your ideas to the class, and we can discuss them together with the goals of:
 - generating more ideas
 - narrowing down the scope
 - elucidating the research gaps and questions
 - clarifying the relevance to (specific sections of) this course
- I'll also write detailed feedback on the ideas later this week

Norrec

- “I currently have two active projects: the first is **a theory-based study on the ways in which tech corporations manipulate user choice**; the second is an interdisciplinary study bridging with the field of International Relations to develop a more **dynamic threat modeling framework for CS research**. Additionally I am in initial discussions for two other projects, one related to **digital child exploitation** and the other related to **LLM advice regarding financial scams**.”

Chongyang (Gary)

- “For project ideas, I do have 3 running projects, yet none of them is privacy research, but we could definitely come up with research questions built on them: 1) VR multi-robot teleoperation 2) Use XR Gaze to improve inter-human mass collaboration 3) LM conversational agent in health intervention (with my new lab, so I've haven't gone too deep). Except my current projects, I have my own ideas as well! Particularly: **privacy in 3D reconstruction for XR** (basically, you take a few shots to an object, then you got the 3D model), **Gaze/Avatar related data privacy concern in XR**, **privacy in online games**, AR Code (like 3D QR Code), and **Multi-model XR hardwares designs for privacy** (eg. Meta Rayban Glasses put a flashlight on their product, you record, the light on showing people you are recording, if you block it, it will stop recording).
Idea Tags: **XR/VR/AR/MR, Gaze, 3D Reconstruction, Modeling, Avatar, Collaboration in XR, Online Games, LM Agent, Multi-Model LLM.**”

Zhiping (Arya)

- “I’m currently working on a project about **user privacy awareness in LM agents**, looking at how privacy issues can be affected from the user’s perspective. 1) I’d love to explore some follow-up projects and maybe explore ways to develop **personalized privacy solutions** since everyone’s preferences are so different! But I’m also open to other directions. 2) Another area I’m curious about is **privacy in social robotics or LM agent systems**. The shift from rule-based agents to ones using LLMs is exciting but also brings many novel privacy challenges, known or unknown.”

Jiayi (Eleanor)

- “My research focuses on natural language processing (NLP), privacy, and language model agents.”
- “Currently, I'm working on evaluating the persuasiveness of large language models (LLMs) across various persuasion tasks, and developing a unified interface that enables people from different backgrounds to easily set up LLM-based persuasion environments in different domains. While this project isn't directly tied to privacy, a potential follow-up idea is to explore **how to balance providing accessible, personalized advice** — especially in highly specialized fields like law and healthcare — **for underrepresented groups** (the groups often face challenges in accessing specialized professional advice, but language model agents could make these services more accessible) **while ensuring the protection of their personal privacy.**”

Sama

- “I am **flexible on the research interests** (not fixated on one yet). I have selected this course as way to read more papers to get more about the privacy and security in LLMs navigating this space, understand in more detail as I figure out about the PhD research area, privacy practices etc.”

Willem

- “I don't have any research experience yet, but I am interested in anything at the intersection of biology and computer science. However, I'm **open to exploring almost anything**, as I am still new to the field.”
- “I want to learn more about the subject to **make more informed decisions regarding privacy guidelines when engineering programs** in the future.”

Tim

- “My research areas of interest are **info vis and VR** and the intersection of human psychology when using viewing vis in VR. I previously worked on a paper examining the **fear response while viewing at data in VR**. I selected this course because I am interested in being able to discuss privacy and agency.”

Daniel

- “While I don’t have much research experience yet, I double-majored in Computer Science and Cognitive Science during my undergrad, which sparked my interest in research but never really done more than read papers. I chose this course to explore to see if I can spark an interest in reading more papers. Regarding project ideas, **I’m open to exploring a wide range of topics**, as I don’t have any specific ideas in mind at the moment.”

Action items

- By the noon this Wednesday (Sept 11)
 - Submit the first set of reading commentaries
 - Two students will lead the first discussion
- Project proposal due two weeks later (Sept 25)
 - Talk to other students
 - Book an office hour appointment with me (Wednesday 1-2pm)