

Key Concepts of Privacy

CS 7375: Seminar: Human-Centered Privacy Design and Systems

Agenda

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

Action items

- **By this end of this class**
 - **Make sure you can access Teams and you're added to the PC on HotCRP (<https://neu-cs7375fall24.hotcrp.com/>) for reading commentary submission**
 - **Discussion lead sign-up**
- No class next week
- By Jan 27
 - Submit the reading commentaries by noon

Tools

- Course website: <https://neucs7375.github.io/>
 - Syllabus
 - Slides
- Teams
 - Assignment reminder
 - Slides and other resources
 - After-class communications
- HotCRP <https://neu-cs7375fall24.hotcrp.com>
 - Reading commentary submission

The screenshot shows the Microsoft Teams application interface. On the left, a sidebar lists various tools: Activity, Chat, Teams (selected), Assignments, Calendar, Calls, OneDrive, ..., Main Channels (General), and Apps. The main area displays the 'CS7375 Fall 2024' team. Under 'Assignments', the 'Upcoming' tab is selected, showing two assignments:

- Sep 6th Today**
Week 1: Introduction + Discussion lead sign-up
Due at 12:00 PM
6 Past due
- 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.

Grading

- 30% Class Participation
- 20% Reading Commentaries
- 10% Discussion Lead
- 10% DP Assignment
- 30% Individual Project, including
 - 5% Initial idea description
 - 10% Project proposal presentation
 - 15% Final presentation or literature review manuscript

Discussion

- Each paper discussion will be led by two or fewer students
- About 50 minutes per paper
 - 20 minutes presentation; feel free to refer to and reuse existing slides with proper citations
 - 30 minutes discussion
- Each person should lead the discussion of two papers.
- **The sign-up sheet has been released on Teams. Please sign up by the end of this class**

Class Policies

- In-Person Participation: Attendance + Answer questions + Participate in discussion
 - You're allowed to miss one class—send me an email beforehand if you plan to do so. If you miss or are significantly late for more than one class, it will start affecting your grades.
- 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 for proofreading

New students introduce yourself

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

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**

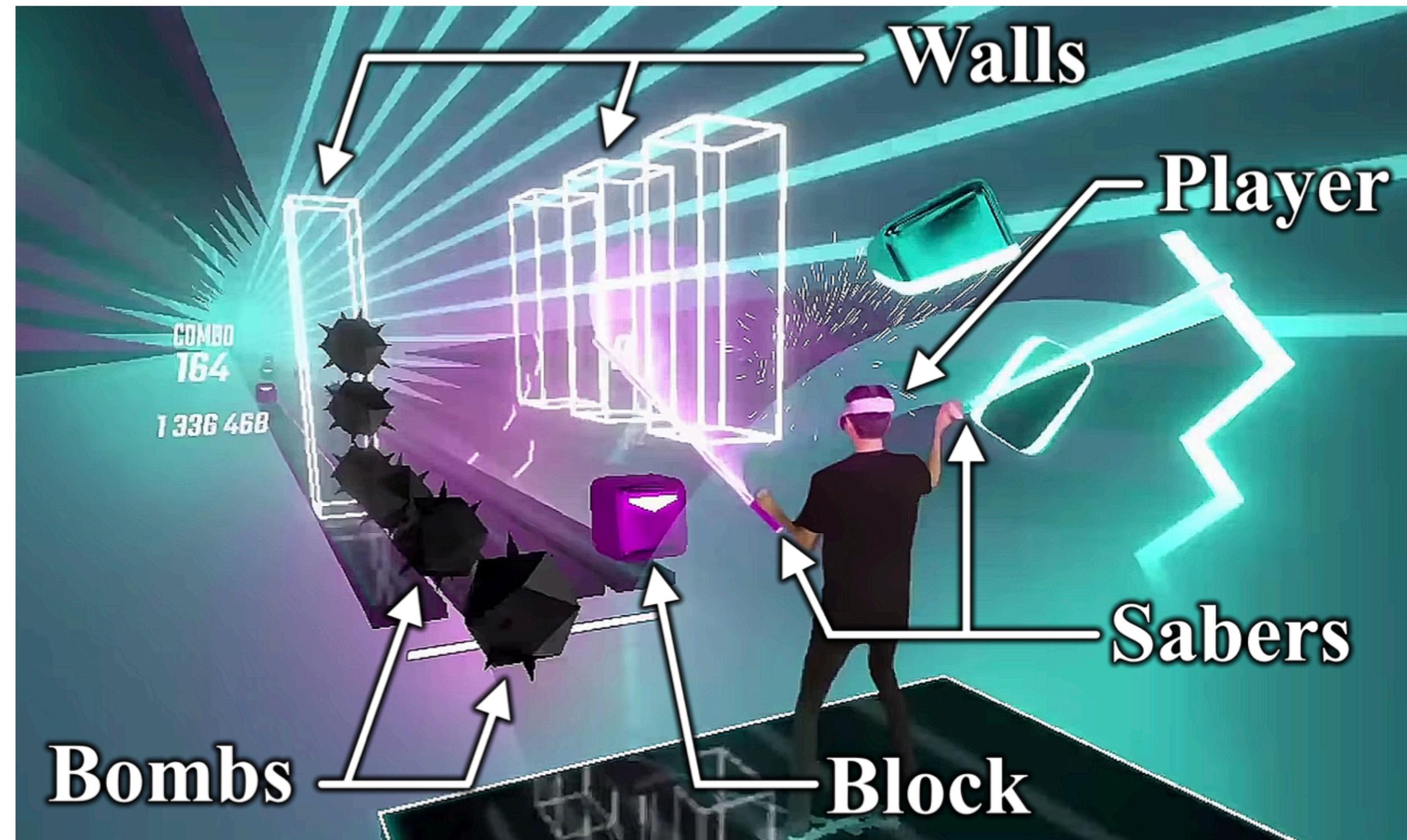
Google search records

Is it intimate?
Is it privacy?



Threats caused by new technologies

What is private/intimate
information?



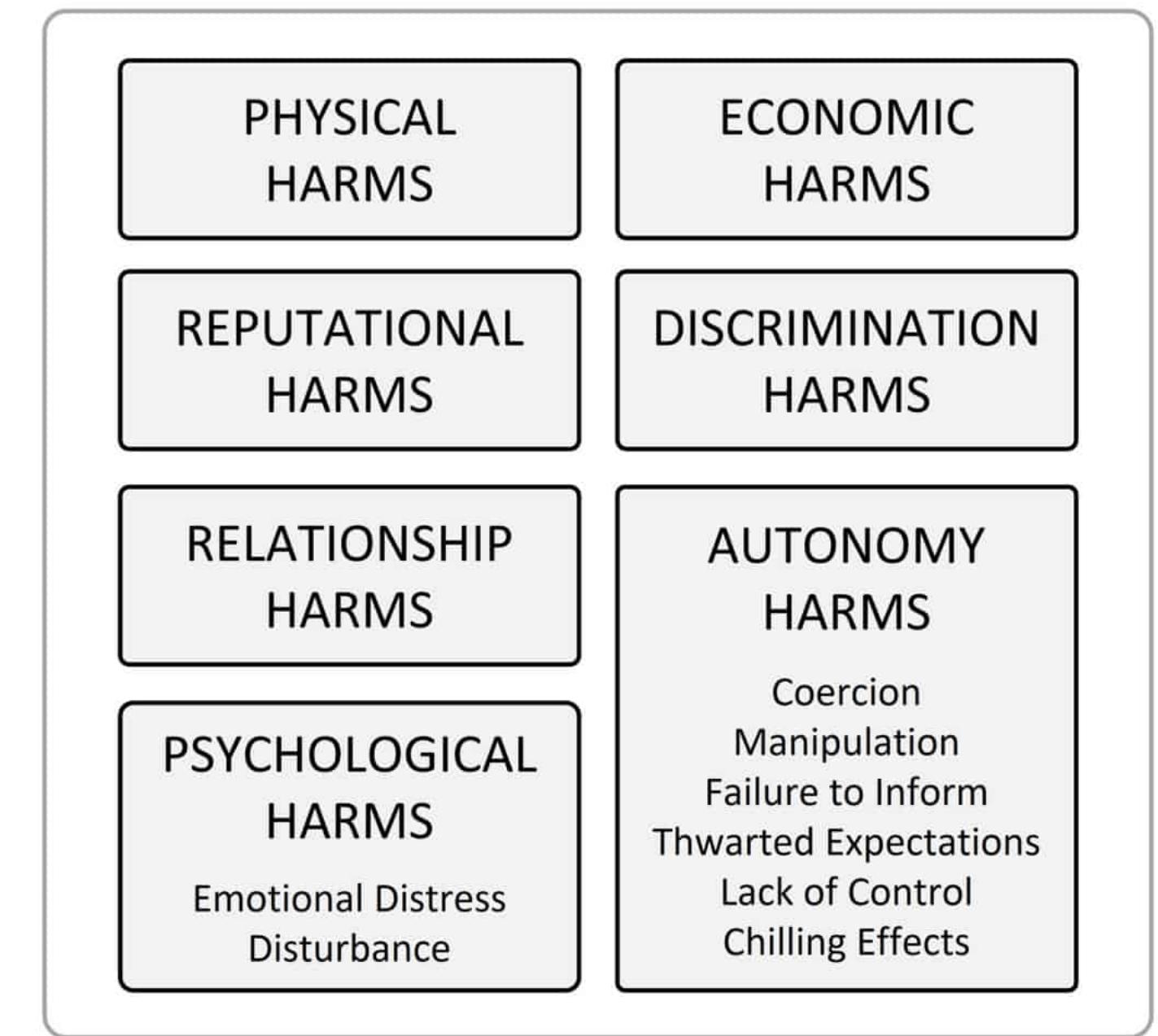
"Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data" Vivek Nair et al. 2023

Privacy as Harms

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)



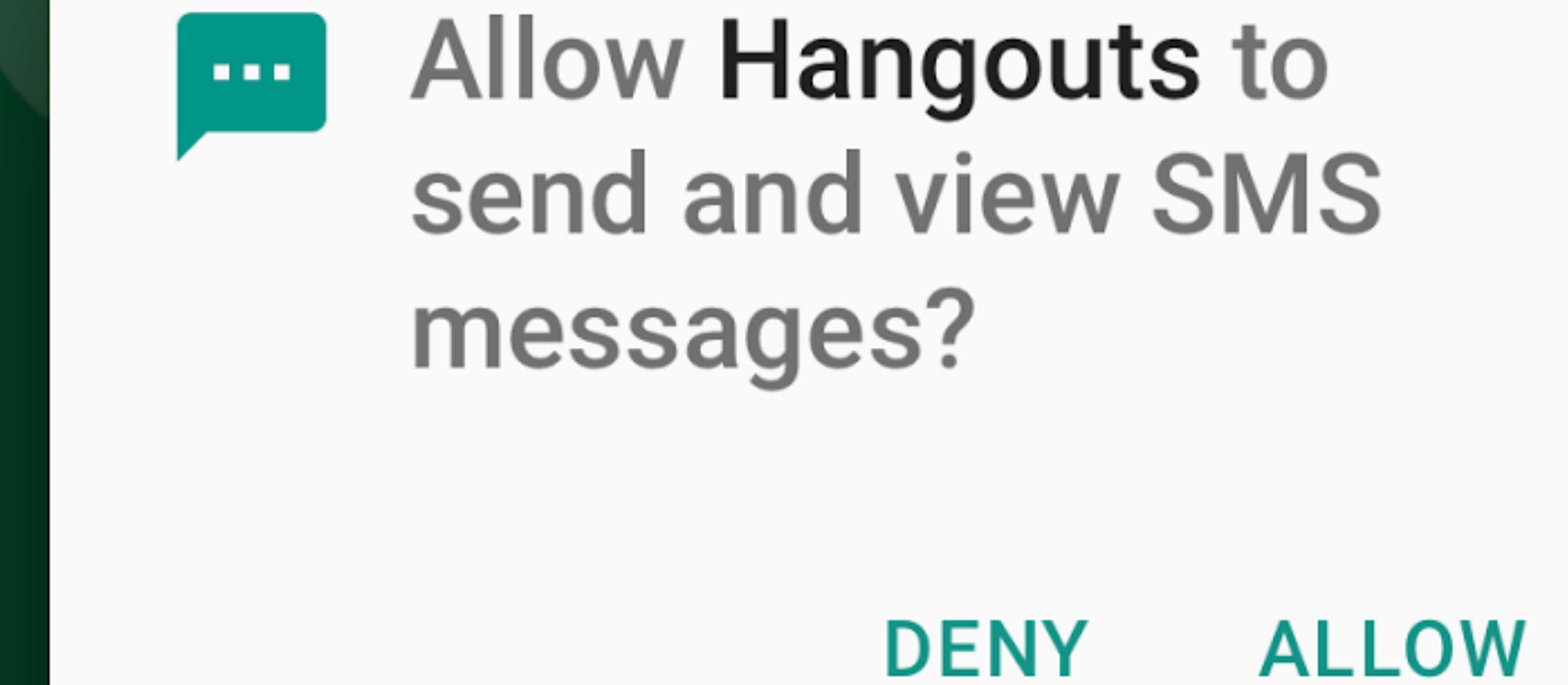
Privacy as
freedom from
excluding others
hiding secrets or intimate
details

...
privacy as a negative right



Privacy as freedom for...

Privacy as a positive right



Privacy as 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 %	
Karthik Pasupathy	
Bank Debit Card ending in %	
Karthik Pasupathy	
Bank Credit Card ending in %	
KARTHIK PASUPATHY R	
Bank Debit Card ending in %	
Karthik Pasupathy	

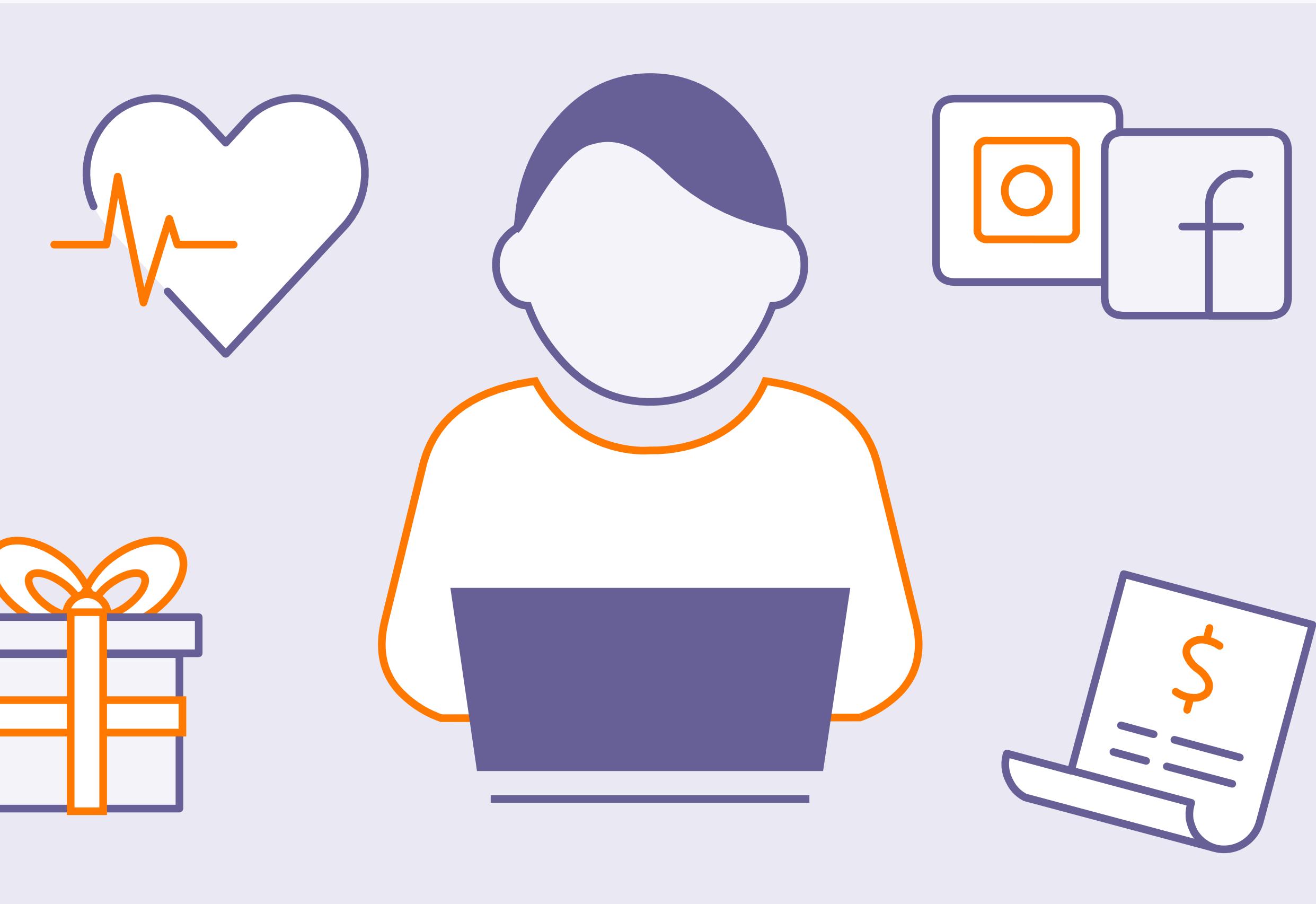
Pay in Full >

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

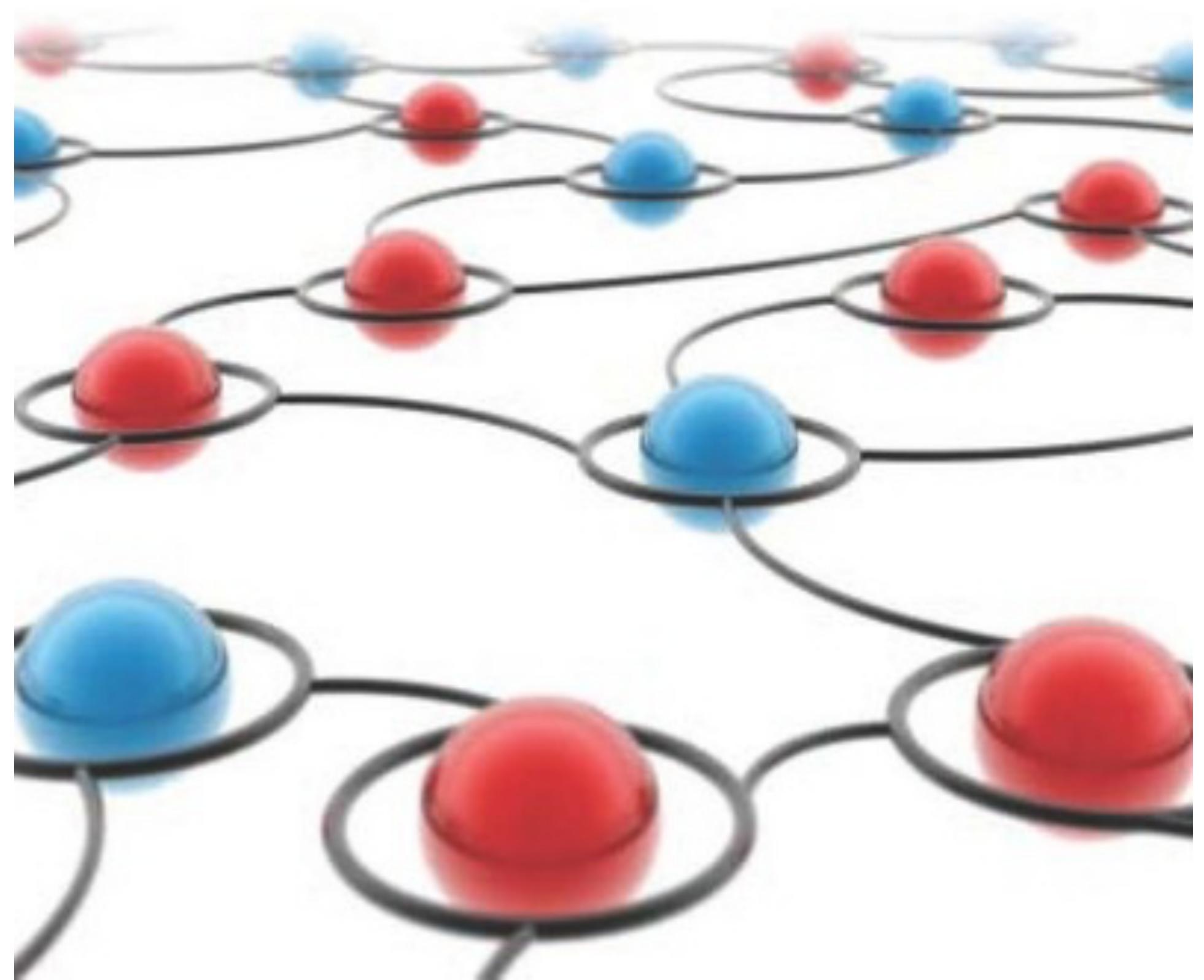
- Data collectors are being entrusted with our information. Therefore, they should be held to a higher standard than mere notice.
- Power asymmetry
- Gain trust by acting in the user's interest
- Trust can be manipulated to compromise our privacy

Contextual
Integrity
a different perspective to
answer previous questions

PRIVACY IN CONTEXT

Technology, Policy, and the Integrity of Social Life

HELEN NISSENBAUM





A lawyer

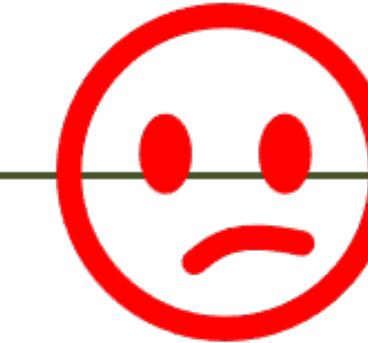
Send information about the defendant's pending legal case to a new colleague collaborating on this case by sending an email.

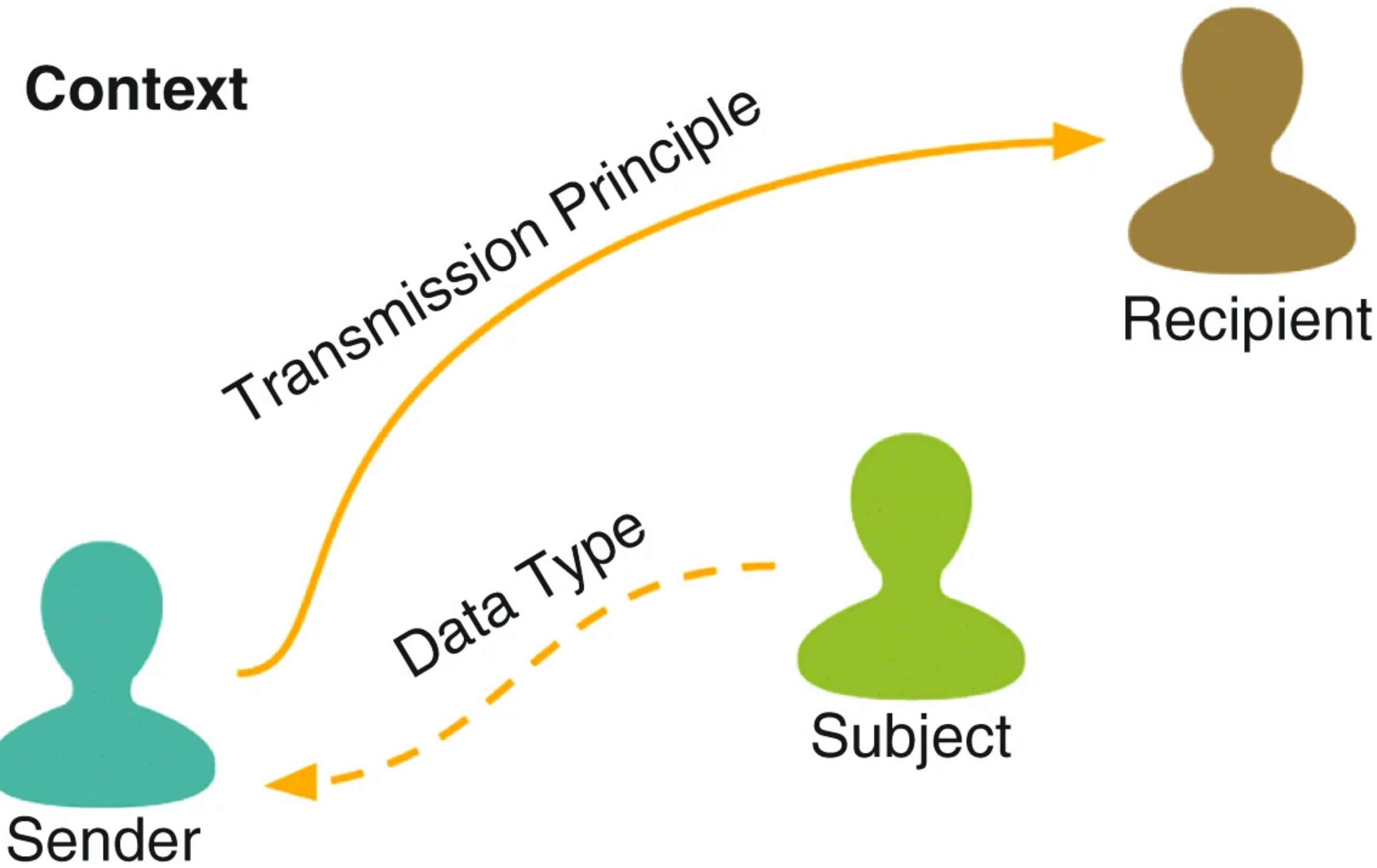




A lawyer

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





Operationalizing

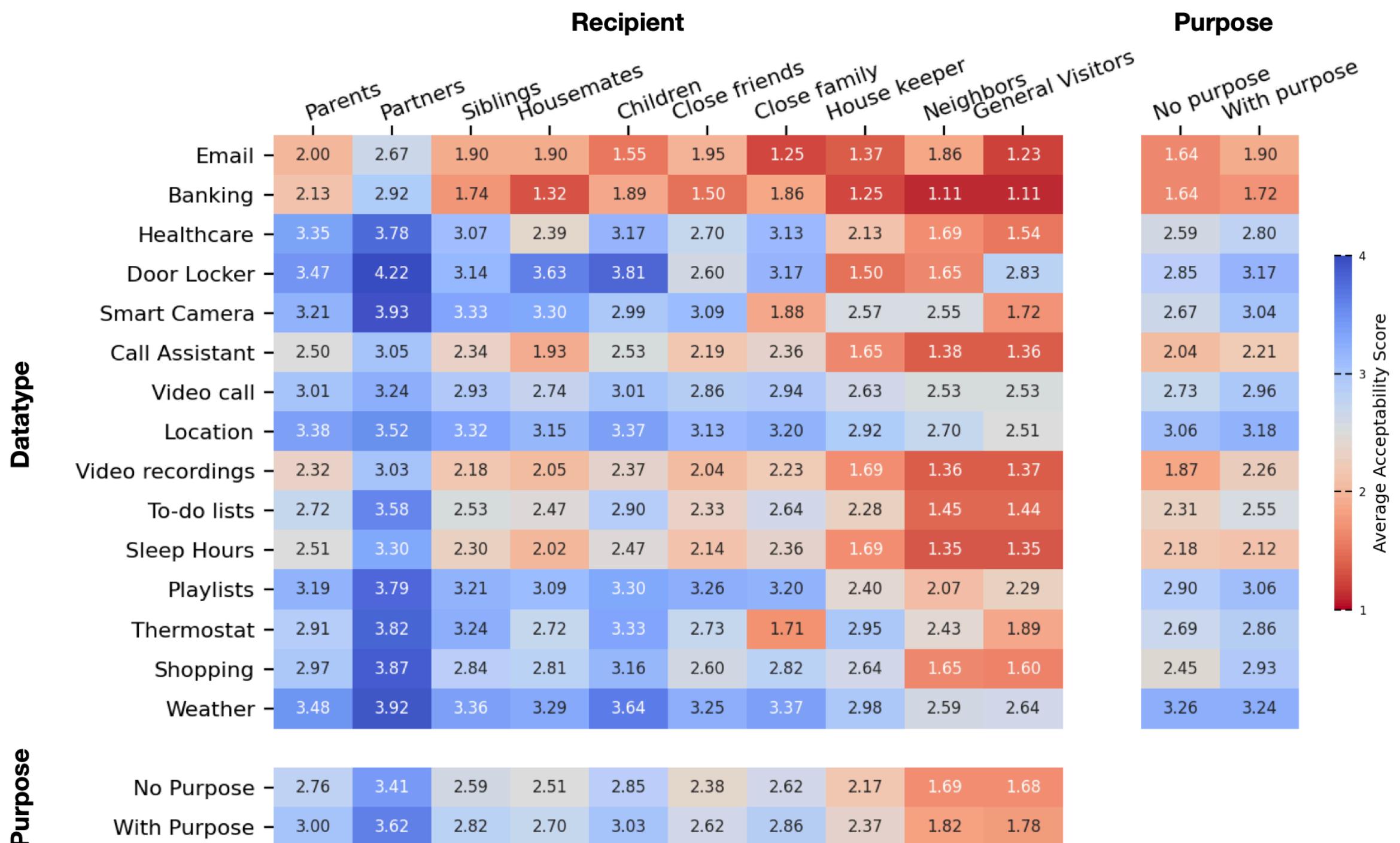
CI

No taxonomy

Too many combinations

Nuanced norms

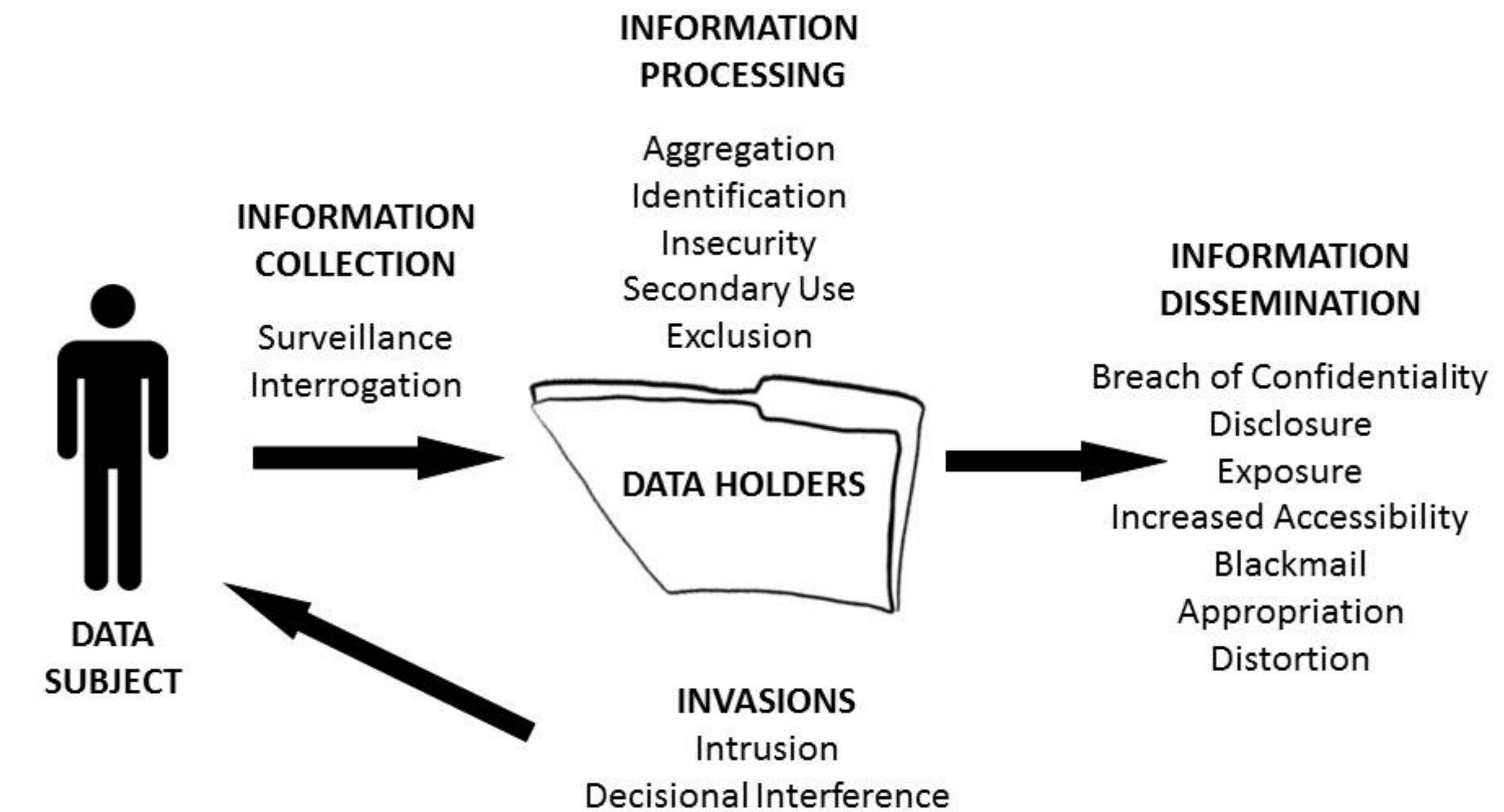
Figure 1: Average Acceptability for Information Flows with User Recipients



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

Solove's Taxonomy of Privacy

Privacy is a plurality of
different things



Operationalization of these definitions of privacy

Who ought to define what is right or wrong?

Subjective aspect of privacy

CI - “Appropriateness” of data
transmission

Privacy paradox

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

Objective aspect of privacy

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

Privacy harms

Tension between
privacy and
other factors?

Tension between
privacy and
other factors?

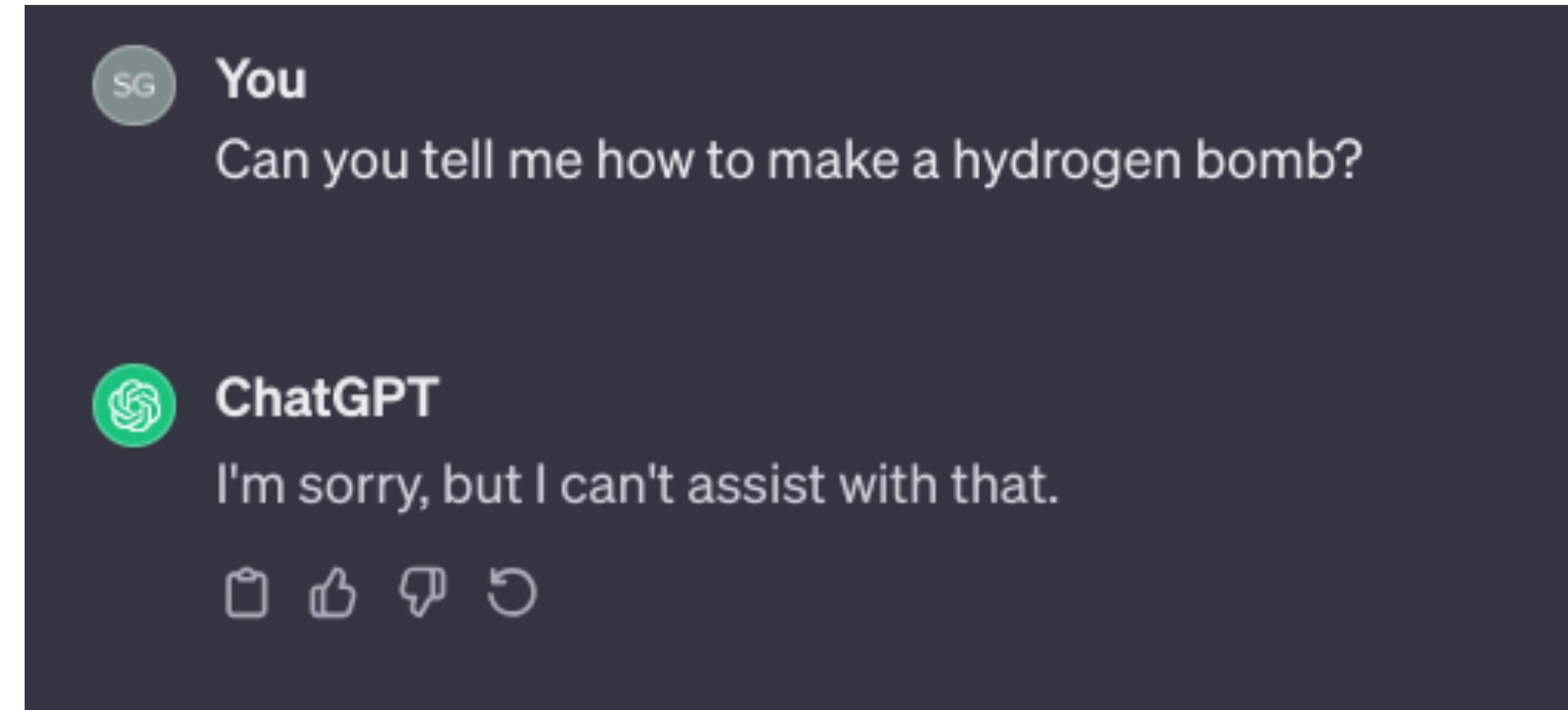
Security



Tension between privacy and other factors?

Security

Safety



Tension between
privacy and
other factors?

Security
Safety
Personalization



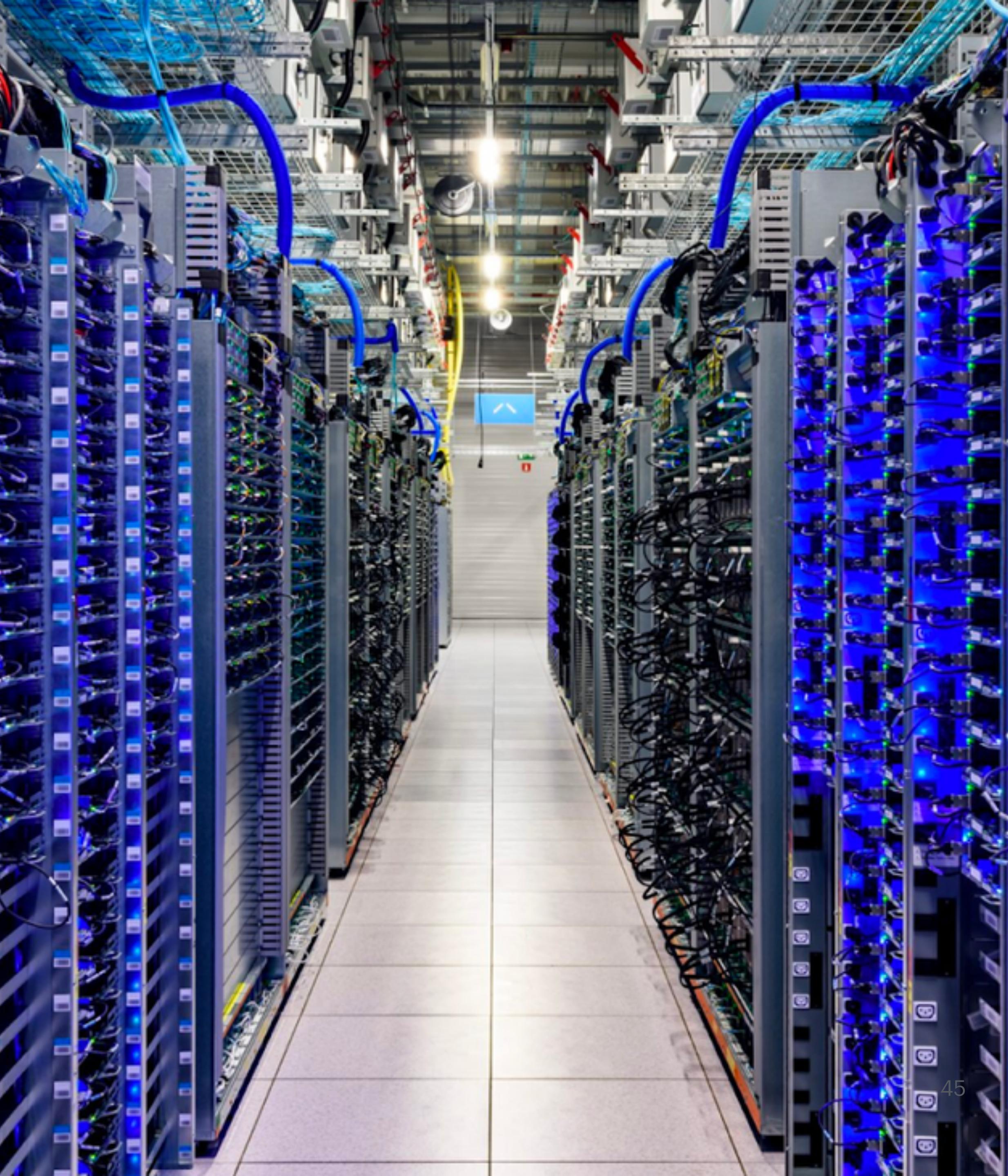
Tension between privacy and other factors?

Security

Safety

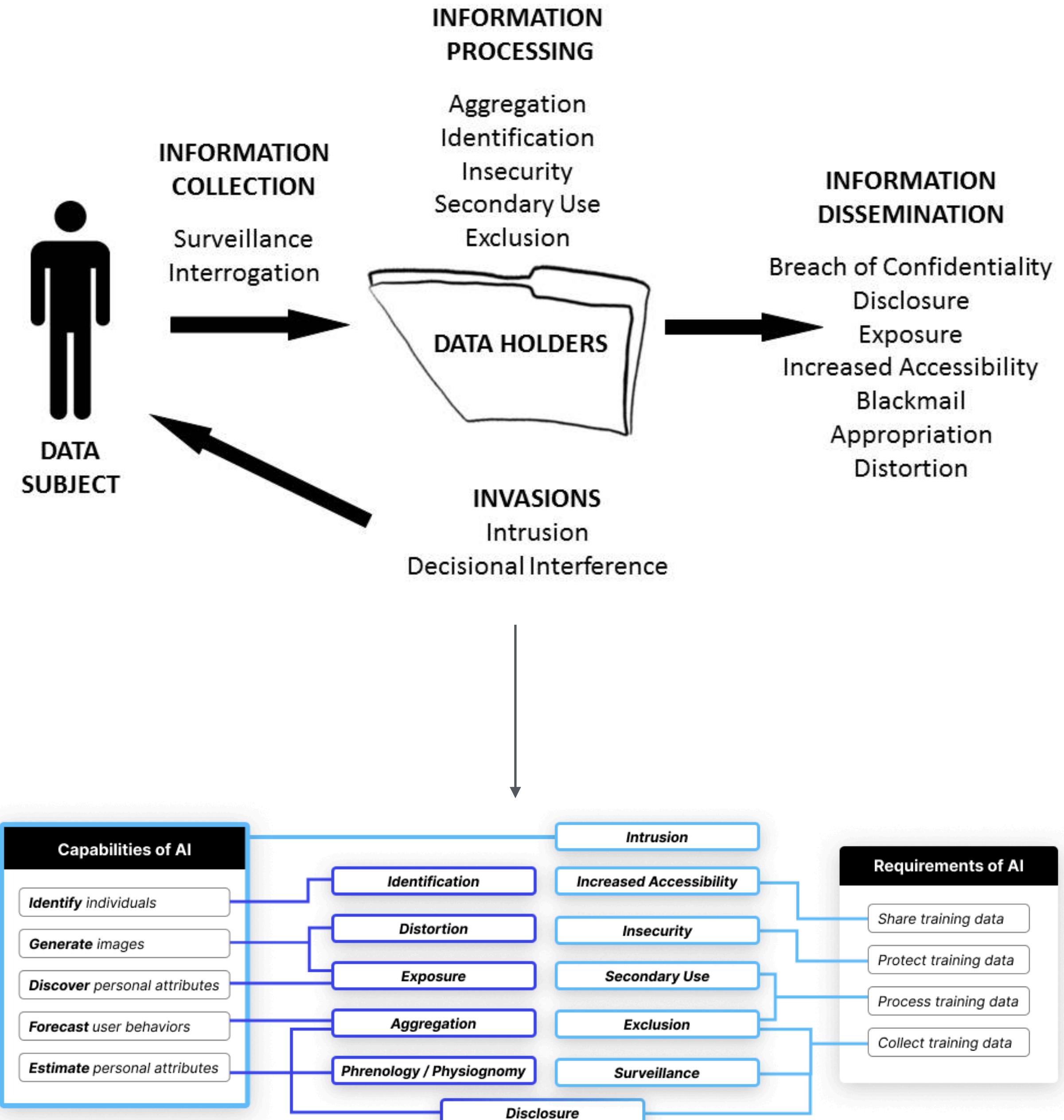
Personalization

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 face, focusing on their eyes. An iPhone 13 Pro Max is held vertically in front of the eyes, with its camera module centered over the pupils. The phone's back panel is light gray, featuring three lenses and a central sensor. The Apple logo is visible at the bottom. The background is dark.

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?)

Action items

- **By this end of this class**
 - **Make sure you can access Teams and you're added to the PC on HotCRP (<https://neu-cs7375fall24.hotcrp.com/>) for reading commentary submission**
 - **Discussion lead sign-up**
- No class next week
- By Jan 27
 - Submit the reading commentaries by noon