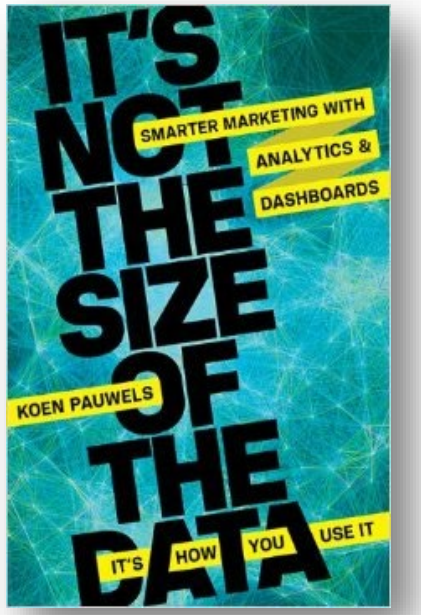
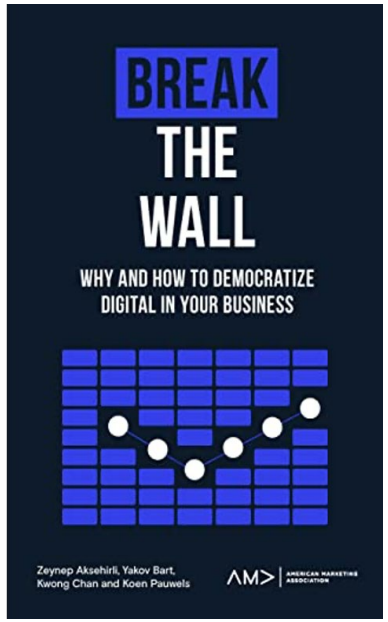
4.23.24

Privacy shown in consumer attitudes vs their actions

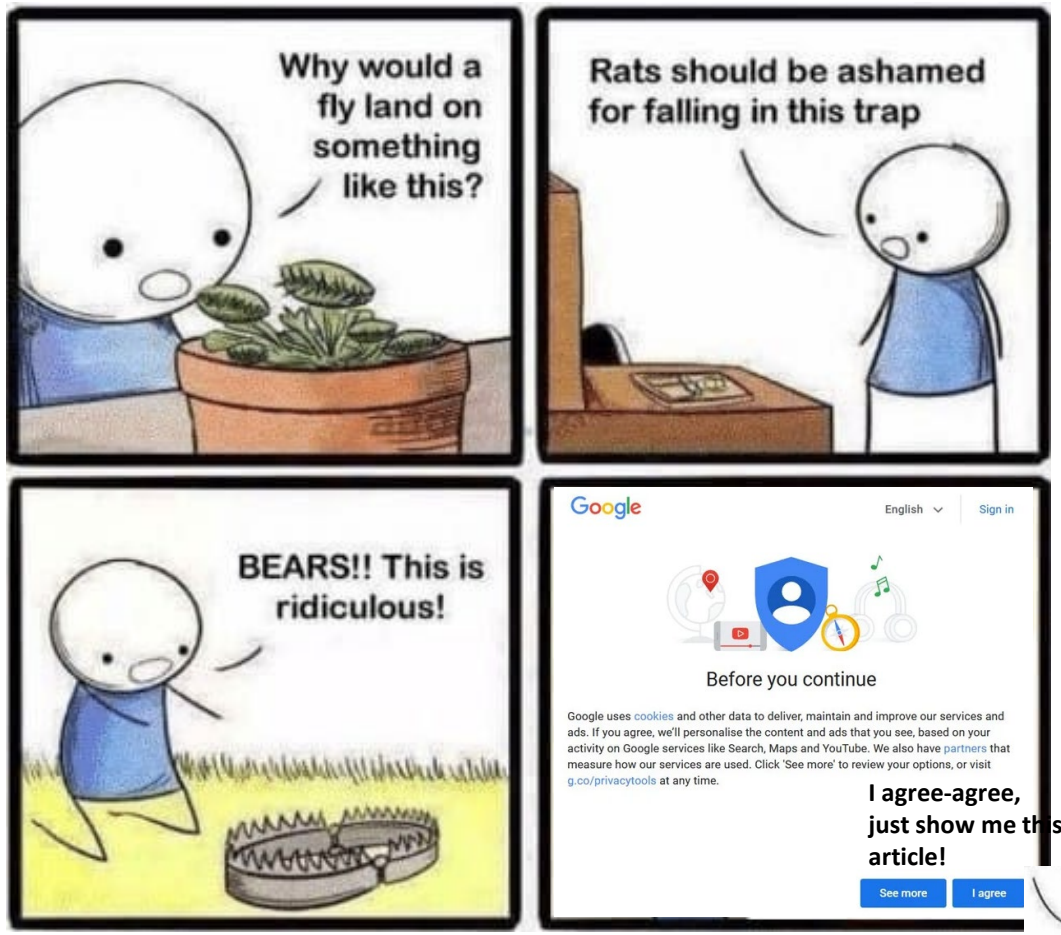
Northeastern University
D'Amore-McKim School of Business





IT'S NOT THE SIZE OF THE DATA
SMARTER MARKETING WITH ANALYTICS & DASHBOARDS
KOEN PAUWELS
IT'S HOW YOU USE IT


BREAK THE WALL
WHY AND HOW TO DEMOCRATIZE DIGITAL IN YOUR BUSINESS
Zeynep Aksehirli, Yakov Bart, Kwong Chan and Koen Pauwels
AMA

Consumers have limited ability to detect privacy threats online



Among highly privacy concerned users almost half in fact reveal sensitive information on social media (Acquisti et al., 2015).

Privacy paradox: attitudes vs behavior not understood (Aguirre et al., 2015, Shariff et al., 2021).

Most subjects provide their monthly income for a price discount of 1 Euro. Even without it, only half of subjects shopped with the more privacy-friendly branch of the DVD retailer (Beresford et al 2013)

Cookie artist of 2014

- To get a cookie, people had to turn over personal data that could include address, driver's license number, phone number and mother's maiden name.
- Just under half gave what they said were the last four digits of their Social Security numbers. About one-third allowed her to take their fingerprints.

Stated privacy preferences suffer from several biases

Characteristics of customer privacy preferences: (Acquisti et al. 2022, 21)

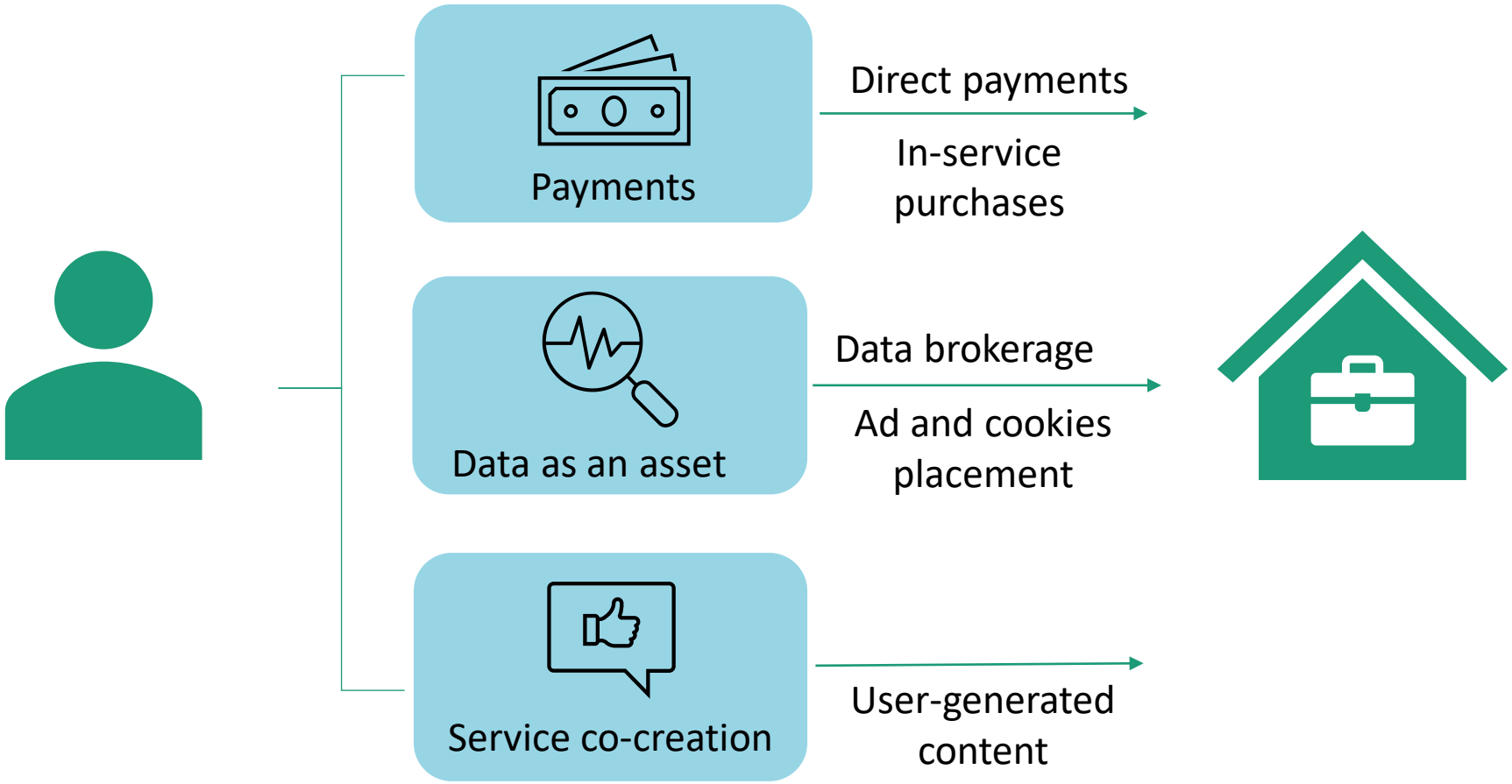
Uncertain

Context-dependent

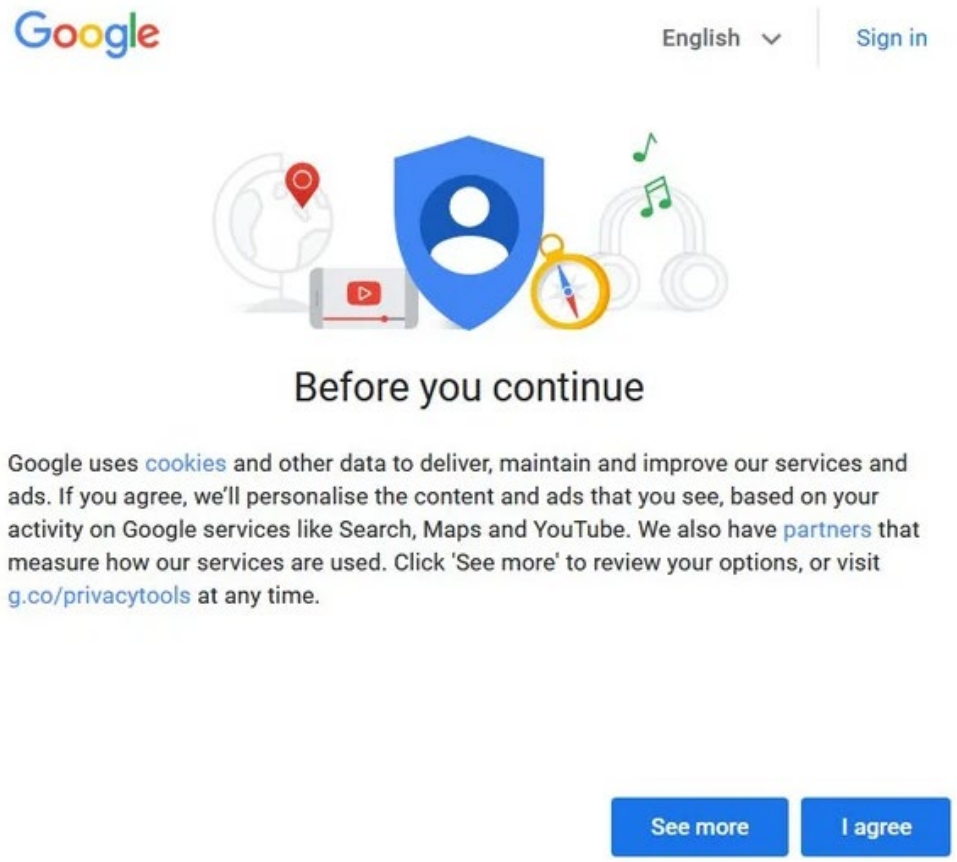
Prone to manipulations

Consumers may well care for privacy and try to regulate the extent to which they may have to reveal personal information, but psychological and economic hurdles may make the **desired privacy unattainable in absence of clear regulatory guidelines**, which can then create **dark patterns in technology designs** which affect consumers (Acqusti et al., 2021; Mullighan et al., 2021).

Firms can (mis)use these biases to create benefits in multiple ways



The **G**eneral **D**ata **P**rotection **R**egulations & **C**alifornia **C**onsumer **P**rotection **A**ct



Privacy consent fallacies:

- "Customer responsibilization" approach is not viable as it relies on rational decision-making (Acquisti, 2021).
- Privacy policies and consent notice increase trust, in fact provoking customers to give up privacy rights (Hoofnagle & Urban, 2014).
- Consumers not required to understand or even read the policies they agreed on (Salazar, 2020).
- Regulations don't address harms consequent to data protection failures

Consumers DIFFER in how much they value privacy

- In a) **how much money** they would accept to disclose otherwise private information, or how much they would pay to protect otherwise public information; and b) the **order** in which they consider different offers for that data (Acquisti, John & Loewenstein 2013)
- Super endowment effect: in a survey of 2,416 Americans, the median consumer is willing to pay just **$5 per month** to maintain data privacy, but would **demand $80** to allow access to personal data. Much higher than the 1:2 ratio often found between **willingness to pay and willingness to accept** (Winegar & Sunstein 2019)
- While consumers claim that personally identifiable information (PII) was more valuable than non-PII in the **interview**, they did not demand a higher WTA price when monetizing PII in two **experiments**. However, consumers became more cautious and provided fewer data items when dealing with PII, compared to non-PII (Liu et al. 2023)

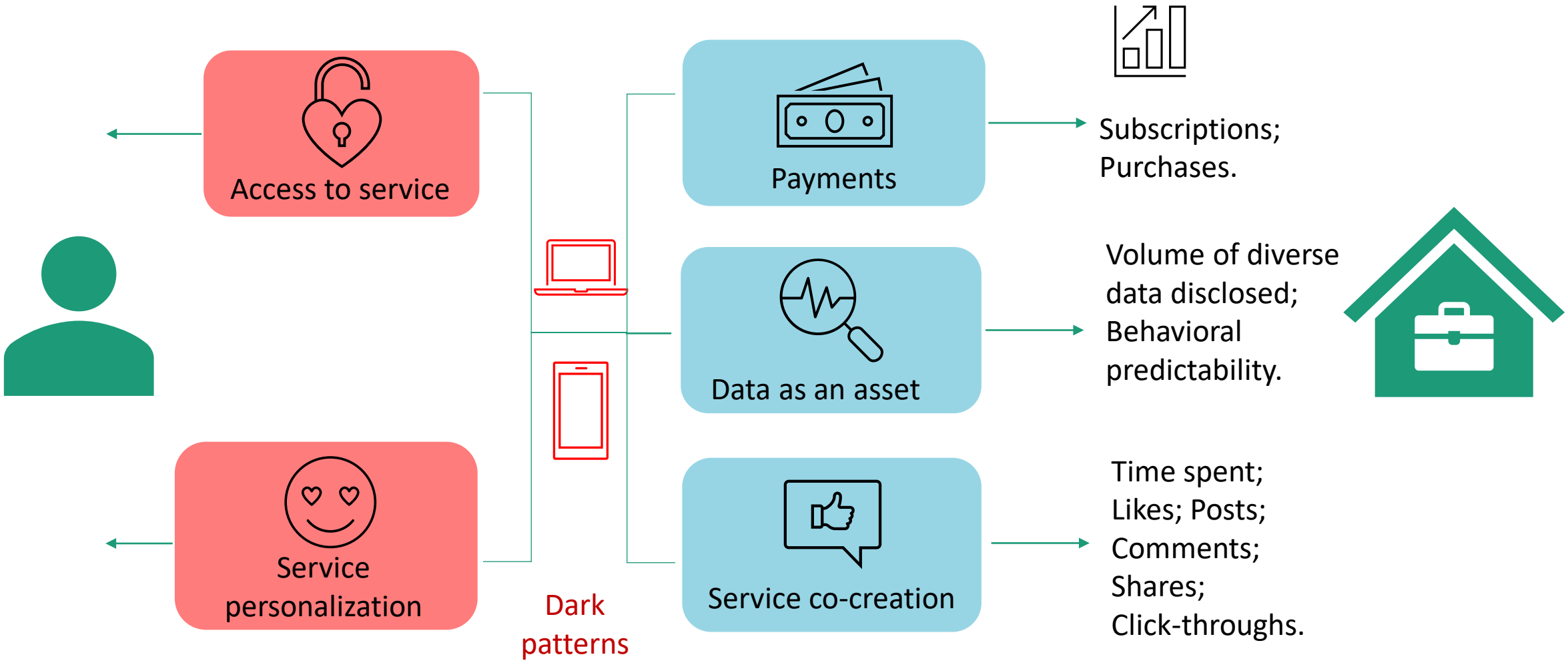
Customer experience, risk aversion, nationality, and setting matter:

- Valuations for concealing contact lists and text messages for more **experienced** consumers are larger than those for less experienced consumers (Savage & Waldman 2013)
- Consumers willingness to incur a privacy risk is driven by **risk aversion**, self-reported value for private information and general attitudes to privacy (Frik & Gaudeul 2020)
- **Germans** value privacy more than do people in the **US and Latin America**. People most value privacy for financial (bank balance) and biometric (fingerprint) information. People had to be paid the least for permission to receive ads (Prince and Wallsten 2022)
- Lin (2022) separates two components in a consumer's privacy preference. The intrinsic component is a **"taste" for privacy**, a utility primitive. The instrumental component comes from the consumer's **anticipated economic loss** from revealing his private information to the firm and arises endogenously from a firm's usage of consumer data. They are highly heterogeneous across consumers and categories of data.

How consumer segments tradeoff privacy for other benefits

- Consumers consider their privacy as a form of “currency” that they can use in marketing exchanges. The higher the benefits they receive, the higher their willingness to give up their privacy (Schumann et al. 2014)
- Many customers willingly share their personal information in exchange for **benefits, such as personalized online offers, increased convenience, and location-relevant mobile content** (Aguirre et al. 2015; Rainie and Duggan 2016).
- Our Northeastern Tier 1 project estimates **consumer segments** that care most about privacy, price, convenience, personalization and location-relevant advice, and how these differ across regulatory environments

Firms provide personalization benefits and chose user interface design to drive customer engagement and information disclosure



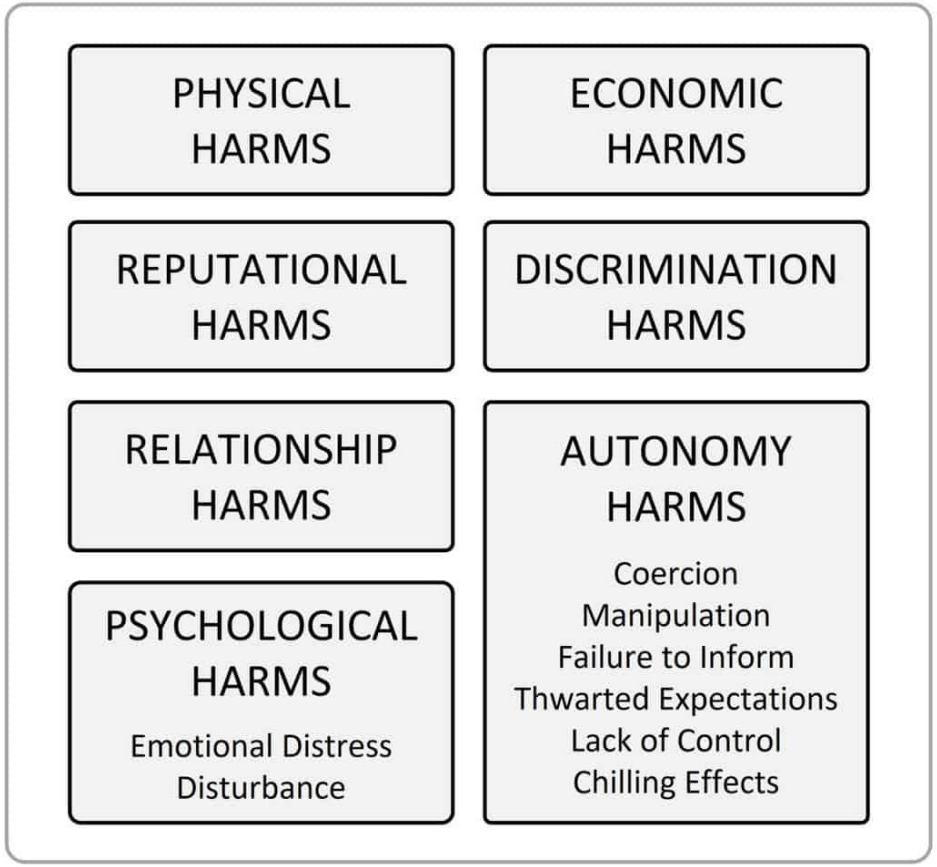
Thank you.

Appendix 1. Biases affecting privacy decision-making by Acquisti et al. (2021)

Some Psychological Factors Affecting Privacy Decision Making

Psychological factor	Description	Representative consequence	Firms' response
Information asymmetries	Consumers are unaware of the diverse ways firms collect and use their data	Consumers cannot respond to risks they are unaware of	Increases firms' ability to collect and use consumer information
Bounded rationality	Consumers lack the processing capacity to make sense of the complexities of the information environment	Few read, or even could make sense of, privacy policies	Writing policies using sophisticated, legalistic terms that obscure the central issues
Present bias	Overemphasizing immediate, and under-weighing delayed, costs and benefits	Consumers will incur long-term costs —for example, intrusive profiling and advertising—in exchange for small immediate benefits—for example, online discounts	Offering small benefits in exchange for consumer data sharing
Intangibility	Putting little weight on outcomes that are intangible—difficult to isolate or quantify	Consequences of privacy violations are often diffuse and difficult to connect with specific actions	Making it difficult for consumers to draw connections between specific acts of data sharing and specific privacy violations (e.g., price discrimination)
Constructed preferences	Uncertainty about one's preferences leads people to rely on crude decision heuristics that often run counter to considerations of objective costs and benefits	Sticking with default privacy settings	Setting defaults that are advantageous to the firm rather than to the consumer
Illusory control	The feeling (often illusory) that one is in control of a situation leads to increased risk-taking	Consumers share more when given more granular control over privacy settings	Provide consumers with more granular privacy controls to encourage disclosure
Herding	The tendency to imitate the behavior of other people	Consumers share more when they see others sharing more on social media	Provide social media feeds that convey a maximal sense of others' sharing
Adaptation	The tendency to get used to risks that are unchanged over time or that increase gradually	Despite ever-increasing violations of privacy, consumers adapt to them and accept them	Change data usage practices gradually
The drive to share	The powerful drive to share information, including personal information	Sharing of highly private, or even incriminating, information (e.g., on social media)	Working behavioral levers that elicit the motive to share (e.g., recommending photographs to share)

Appendix 2. Customer privacy harms by Citron & Solove (2022)



- **Physical harms** - harms that result in bodily injury or death. Physical harms are well recognized as cognizable under the law.
- **Economic** harms involve monetary losses or a loss in the value of something. Privacy violations can result in financial losses that the law has long understood as cognizable harm.
- **Reputational** harms involve injuries to an individual's reputation and standing in the community. Reputational harms impair a person's ability to maintain "personal esteem in the eyes of others" and can taint a person's image.

- **Discrimination** harms involve entrenching inequality and disadvantaging people based on gender, race, national origin, sexual orientation, age, group membership, or other characteristics or affiliations.

- **Autonomy** harms involve restricting, undermining, inhibiting, or unduly influencing people's choices. People are prevented from making choices that advance their preferences. People are either directly denied the freedom to decide or are tricked into thinking that they are freely making choices when they are not.

- **Psychological** harms - Psychological harms involve a range of negative mental responses, such as anxiety, anguish, concern, irritation, disruption, or aggravation. Although there is a wide array of feelings are categorized into one of two general types—emotional distress or disturbance. Emotional distress involves painful or unpleasant feelings. Disturbance involves disruption to tranquility and peace of mind.

- **Relationship** harms involve the damage to relationships that are important for one's health, well-being, life activities, and functioning in society.