Endogenous Privacy in Games

a.k.a. “Privacy Can Arise Endogenously in an Economic System with Learning Agents”

Nivasini Ananthakrishnan, Tiffany Ding, Mariel Werner, Sai Praneeth Karimireddy, Michael I. Jordan

UC Berkeley

What kind of data privacy do people care about?

The New York Times

Florida Man Sues G.M. and LexisNexis Over Sale of His Cadillac Data

Romeo Chicco's auto insurance rate doubled because of information about his speeding, braking and acceleration, according to his complaint.

Sharing data = 😠

npr

PRIVACY & SECURITY

Weighing Privacy Vs. Rewards Of Letting Insurers Track Your Fitness

"John Hancock, a U.S.-based insurer, hopes that fit and active people will **exchange activity data** for **lower life insurance premiums** and other perks"

Sharing data = 😊

Motivating Question

What kinds of privacy arise from utility-maximizing behavior (“endogenous privacy”)?

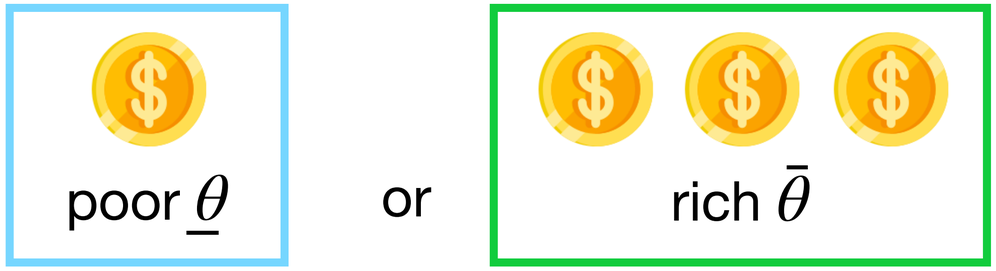
We answer this by formulating a **game** and analyzing the **optimal behavior** for each player.

Price Discrimination (PD) Game

The Players

Buyer

Seller



w.p. μ

w.p. $1-\mu$

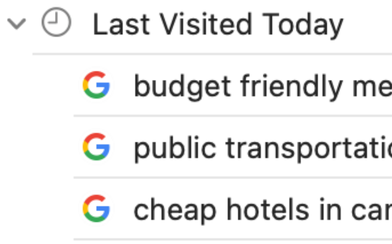
Price Discrimination (PD) Game

Stage 1

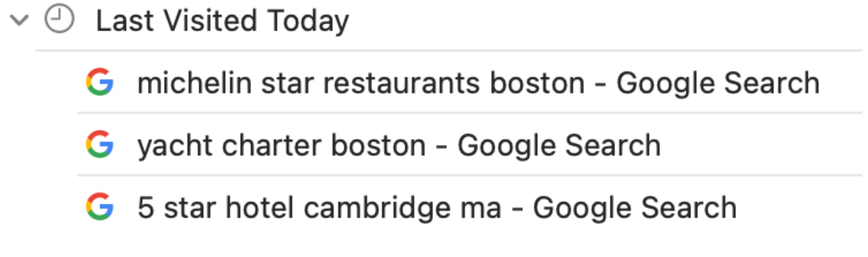
Buyer sends a signal s

No cost to send "true" signal

But if the buyer "evades," they incur cost c_B (and the seller incurs cost c_S)



poor signal $\underline{s}$

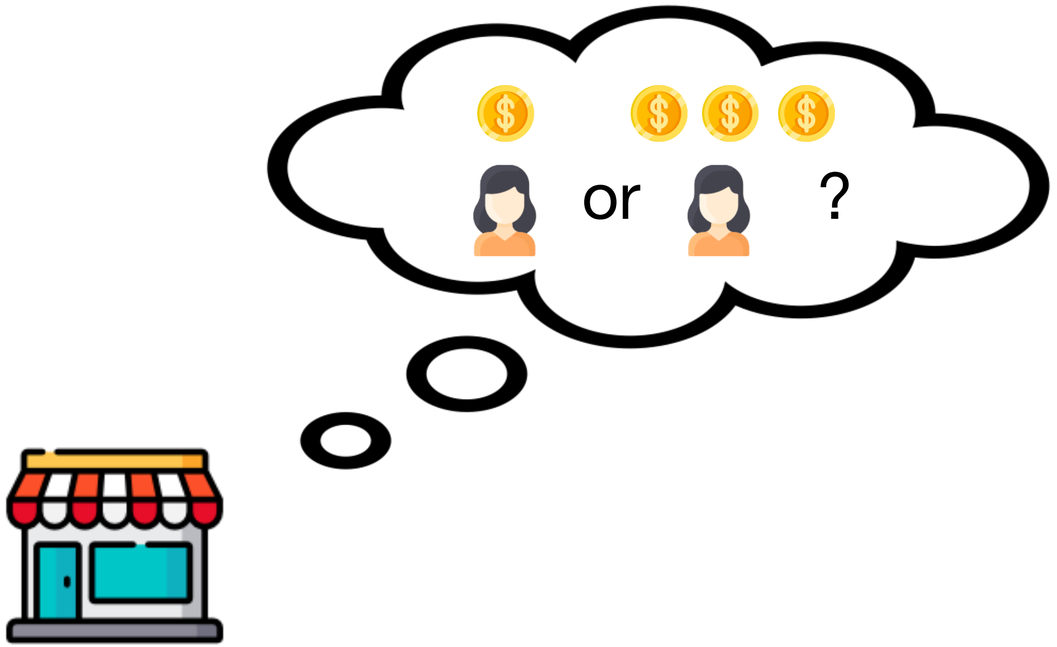


rich signal $\underline{s}$

Price Discrimination (PD) Game

Stage 2

Seller sets price $p \in \{\underline{\theta}, \bar{\theta}\}$ after seeing s



Buyer buys good if the price does not exceed their valuation

Equilibrium of PD game

Theorem 1: At the perfect Bayes Nash equilibrium,

(a) $\underline{\theta}$-buyers always tell the truth

(b) $\bar{\theta}$-buyers lie w.p. $q^* = \min\left\{1, \frac{(1-\mu)\underline{\theta}}{\mu\Delta\theta}\right\}$ ← Buyer-induced privacy

$\Delta\theta := \bar{\theta} - \underline{\theta}$

(c) Seller sets price

$$p = \begin{cases} \underline{\theta} & \text{if } s = \underline{s} \\ \bar{\theta} & \text{if } s = \bar{s} \end{cases}$$

Where does q^* come from?

High-level idea:

Rich buyer wants to lie as much as possible,
but not so much that seller associates $\underline{s}$ with "rich"

Lying probability q induces posterior $f_q(\theta) := \Pr(\theta \mid \underline{s}, q)$

q^* is the highest probability q such that

$$\mathbb{E}_{\theta \sim f_q(\theta)}[\text{utility for } p = \bar{\theta}] \leq \mathbb{E}_{\theta \sim f_q(\theta)}[\text{utility for } p = \underline{\theta}]$$

Is price discrimination actually good for the seller?

If the seller price discriminates (and the buyer believes they are price discriminating),

$$\text{Seller's PD utility} = \mu\bar{\theta} - \frac{(1-\mu)c_S}{\Delta\theta}$$

If the seller does *not* price discriminate (and the buyer believes they are *not* price discriminating),

$$\text{Seller's no PD utility} = \max\{\underline{\theta}, \mu\bar{\theta}\}$$

Observe: we always have

$$\text{Seller's PD utility} \leq \text{Seller's no PD utility}$$

and if $c_S > 0$,

$$\text{Seller's PD utility} < \text{Seller's no PD utility}$$

Price discrimination does not help the seller!

What if the seller can **credibly commit** to providing some level of privacy?

Can they achieve a higher utility?

Seller with commitment ability

If seller could commit to α level of privacy i.e. disregarding signals with $1 - \alpha$ probability

Seller would commit to an $\alpha^* = c_B / \Delta\theta$ level of privacy to maximize their utility

Seller-induced privacy (= disregarding signals)

Buyer's response to seller's commitment

α-PD game: Seller commits to α privacy level

Buyer's response: $\begin{cases} \text{truthful signaling if } \alpha \leq \alpha^* = c_B/\Delta\theta \\ \text{PD PBNE response if } \alpha > \alpha^* \text{ .} \end{cases}$

$\left(\Pr(\underline{s}\,|\,\underline{\theta}) = 1, \Pr(\underline{s}\,|\,\overline{\theta}) = q^*\right)$

Q: Can seller-induced privacy arise even without seller commitment power?

A: Yes, when buyers interact with the seller over multiple rounds and acts according to the *reputation* of the seller.

Reputation from past pricing

- Repeated interaction between same seller and different buyers
- Buyers share information with each other to build estimates $(\hat{\alpha}_t)_{t=1}^{T}$ of degree of price discrimination
- Buyer model: Buyer chooses $\hat{\alpha}_t$-PD PBNE response

Under buyer model, if the sequence $(\hat{\alpha}_t)$ is *consistent*, then

Under buyer model, if the sequence $(\hat{\alpha}_t)$ is *consistent*, then

- the optimal commitment strategy (using signals with probability α^* in every round) is a *weakly dominant strategy* for the seller.

Under buyer model, if the sequence $(\hat{\alpha}_t)$ is *consistent*, then

- the optimal commitment strategy (using signals with probability α^* in every round) is a *weakly dominant strategy* for the seller.
- Always price-discriminating is a *strictly dominated strategy.*

Consistent $(\hat{\alpha}_t)_{t=1}^{T}$

α_t = probability that the seller sets different price for $\underline{s}, \overline{s}$ at time t.

Definition: A sequence of buyer beliefs $\left(\hat{\alpha}_t\right)_{t=1}^{T}$ is a *consistent sequence* if

$$\lim_{T\to\infty} \left| \mathbb{E}[\hat{\alpha}_T] - \frac{1}{T}\sum_{t\leq T} \alpha_t \right| .$$

Consistent $(\hat{\alpha}_t)$

$$\hat{\alpha}_t = \frac{1}{t} \sum_{r=1}^{t-1} \frac{X_r I_r}{\mathbb{E}[I_r]}$$

X_r: $1\{$Different prices for different signals at round $r\}$

I_r: $1\{$Data for different signals available at round $r\}$

	One-shot, no commitment	One-shot, with commitment	Repeated, without commitment
Solution concept	PBNE	PBNE	Buyer: Equilibrium-response to consistent sequence of PD beliefs Seller: Cumulative utility maximizing
Buyer's privacy response	Randomly flip signals	No buyer-side privacy	No buyer-side privacy
Seller's privacy response	No seller-side privacy	Commit to disregard signals with some probability	Commit to disregard signals with some probability

Thank you!

{nivasini, tiffany_ding, mariel_werner, sp.karimireddy, michael_jordan}@berkeley.edu