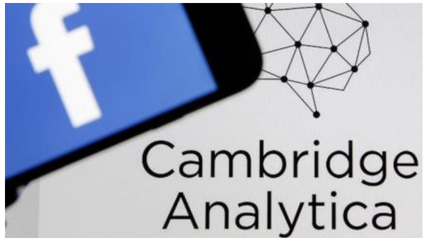
Privacy, data and competition

Professor Tommaso Valletti
Imperial College London

Autoridade da Concorrência
June 1 Junho

Two cases



- Network effects
- Data and privacy
- Competition
- Externalities
- Business model

Some economics of data (I). The positive side?

- **Jones and Tonetti** (AER, 2020) “Nonrivalry and the Economics of Data”
- Data are non-rival (infinitely usable) but excludable
- Representative consumers and firms that produce different varieties
- Consumption generates data: Data improve own and other varieties (spillover)
- Contrasting effects: Social gains if many firms use data, but also privacy concerns
- Who should own the data?
  - Firms. Overuse and do not adequately respect consumer privacy
  - Consumers. Better balance concerns for privacy against the gains from selling data
  - Assigning data property rights to consumers typically generates higher welfare
- Total ban on data very inefficient
- Less obvious effect. If selling data increases the rate of creative destruction, firms may hoard data

Policy implications

- Increasing returns to scale associated with data: there exist incentives for merging
- Data is a barrier to entry. As incumbent firms accumulate data, this makes it harder for other firms to enter
- Government shall **jointly** implement antitrust and data policies

Some economics of data (II). The negative side?

- **Acemoglu et al.** (AEJ: Micro, forth.) “Too much data: Prices and Inefficiencies in Data Markets”
- Privacy paradox?

- Work of Acquisti et al.:
- “Even subtle changes in the way privacy trade-offs are presented to individuals can cause radical changes in people’s valuations of their data or the importance of keeping their data protected. One of the conclusions of my research is that it’s probably fruitless to try to pinpoint with a single number the value of privacy.”

Simple example

- One platform and two users i, j
- Platform wants to acquire users’ leaked data
- Assume:
  - Valuation of the platform for the users’ leaked information = 1
  - Values that users attach to their privacy are vi = ½ and vj = v
  - Correlation of valuations ≈ 1
- Then:
  - User i will always sell her data, because vi= ½ < 1. Hence, the platform will know almost everything about user j
  - User j will be willing to sell her data for approx. 0, leaking information about user i
  - But then user i can only charge a very low price for her data
  - ⇒ The platform **acquires both users’ data at approx. 0 price!**

Implications

- Data externalities: when a user shares her data with a platform, she typically reveals relevant information about other users ⇒ “excessive” data sharing
- Individual-level data underpriced and the market generates “too much data” (no privacy paradox)

- Given this: rethink Google-Fitbit and typical antitrust approach (“small” installed base of Fitbit), or the WhatsApp new terms of service (“they don’t apply to EU”)

- Policies:
  - Tax on data transactions
  - De-correlation via a mediator (remove correlation with the information of other users and only share transformed data of those who are willing to sell their data.)

- Competition does not work (more on this later)

Selling data

- Think of impact on “downstream” markets
- Data provide information: better customization but also price discrimination
- **Montes, Sand-Zantman and Valletti** (Management Science, 2019)
- Data provider sells info to downstream competing firms & consumers can protect their privacy
  - If data is sold to all -> intense price competition, no reason to protect privacy
  - However at equilibrium, all data sold exclusively (= auction with negative externality)
- Re-focus on allocation of data (exclusivity contracts)

Attention bottlenecks and mergers

- **Prat and Valletti** (AEJ: Micro, forth.)
- Look at platforms as “attention brokers” who sell hyper-targeted ads
- Follow the money: ads are ultimately paid by producers of products
- This impacts downstream competition (“incumbents vs entrants”)
- Different platforms -> different ways to get attention
- With concentrated platforms, ads become more expensive because foreclosure strategies of “incumbents” become profitable
- Mergers even in so-called “zero price” markets cause consumer harm: more expensive final products
- Need to have the right metric: “attention overlaps” not “usage shares”

Incorporate Privacy into Antitrust

- It’s not currently done, TBH: push the agency hierarchy to be bold and visionary! (Even if supporting case law has to be built.)
- Privacy as a “quality” characteristic? Not so sure
- Rather **(lack of) privacy is a price**: deals that allow more collection/combination/use of data raise prices for those services
- Often these prices are unobservable: obfuscation by design
- Unobserved prices high also **because** consumers have few ways to say no

Incorporate Privacy into Antitrust

- **(Lack of) privacy can facilitate exploitation and foreclosure**
- Offensive leveraging/data envelopment (at odds with **purpose limitation**)
- Can reframe classic concerns around personal data as the relevant asset
- E.g., “Privacy-policy tying” to deter entry and lower consumer surplus (Condorelli and Padilla, 2021, on “platform envelopment”, adapting dynamic leveraging of Carlton and Waldman, 2002)
- E.g., Google’s “Privacy Sandbox”
  - Is it self-preferencing?
  - Do we then want to preserve “external data free to all”? No

Challenges to the economics/antitrust orthodoxy

- Challenge 1: “more information is always good”
  - Lack of privacy is an (unobservable) price of using platforms which facilitates mainstream antitrust harms such as exploitation and foreclosure
- Challenge 2: “more data generate more surplus”
  - Data combinations by a dominant firm allow a discriminating monopolist to extract the majority of the rents from “good” customers and jack up prices to “bad” ones -> Google/Fitbit (Chen et al., 2021)
- Challenge 3: it’s not the “intersection” between privacy and antitrust, but the “integration”

Muito Obrigado!

https://www.imperial.ac.uk/people/t.valletti

https://twitter.com/TomValletti