



Institut
Mines-Télécom

Economics of privacy

Grazia Cecere

Telecom Ecole de Management

Chercheuse associée au RITM





Outline of the presentation

1. Introduction to economics of privacy
2. Market of personal data
3. Giving up your privacy for free services in post-Snowden era: Are you still comfortable with it?
Natural field experiment

○

Economics of privacy: Long history...

- The role of **personal information** in economics has been exacerbated by the digitalization of the economy. Individuals' concealing of personal information was first supposed to lead to **information asymmetry** between employee/employer, insured/insurer generating **market inefficiencies** (see Hirshleifer, 1980; Stigler, 1980; Posner, 1981).
- Privacy is difficult to define: Protection of someone personal space and the right to be left alone (Warreïn and Brandeïns, 1890); the safeguard of personal information (Westin, 1967).
- It involves different disciplines economics, marketing, behavioral economics, information system, innovation, law.....and different methods in particular *field experiment*



Economics of privacy

1. Motivations and conditions that lead individuals to disclose or not personal information
2. How firms exploit personal data: Innovation, market structure and firms strategies
3. Role of regulation: the realm of “open data and government surveillance” and the impact for commercial outcomes

1. Privacy behaviour of individuals

Motivations and conditions that lead individuals to disclose (or not) personal information

- Trade off disclosure of personal data for immediate gratification (John et al. 2011)
- Privacy concerns and cultural differences (Cecere et al. 2015)
- Privacy paradox (Norbert et al. 2007) and asymmetry of information
- Demand for privacy (Tsai et al. 2011)
- Adoption of new technologies in the health sector (Miller and Tucker, 2011)

Open research questions:

- Assess the demand for privacy once asymmetry of information changes;
- More field experiments to estimate the demand for privacy;
- Demand for privacy enhancing technologies.

2. How firms exploit personal data

Innovation, market structure and firms strategies

- Price discrimination (Taylor, 2004; Belleflamme and Vergote, 2016) and other forms of discrimination (Acquisti and Fong, 2015; Manant et al. 2015)
- Personalized ad is effective once consumers control over their data (Tucker, 2015)
- Market for privacy (Acquisti et al. 2016); New firms and businesses are emerging with a complex market structure (Le Guel, 2016)

Open research questions:

- Monetization strategies of free services focusing on personal data ;
- Industry structure of the innovative firms operating in the market of personal data;
- Identification of new business models for existing and new companies

3. Regulation and policy intervention

Role of regulation: the realm of “open data and government surveillance” and the impact for commercial outcomes

- Self-regulation vs. regulation (Swire, 1999; Cecere et al. 2015);
- Policy can reduce the effectiveness of ad (Tucker and Goldfarb, 2011), Massive government surveillance program affects individuals and businesses (Marthew and Tucker, 2015; Preibusch, 2015)
- Soft paternalisms (Acquisti et al. 2016)

Open research questions:

- Better understanding of the effect of big scandal in the privacy behaviour of individuals and potential outcomes for companies
- More field experiment to adress soft paternalism;
- Keep the balance between innovation and privacy



**Giving up your privacy for free in post
Snowden area:
Are you still comfortable with it?**

Cecere, G.^o, Le Guel, F.* , Manant. M*.
Telecom Ecole de Management^o
Université Paris Sud*

Surveillance

Look who's listening

America's National Security Agency collects more information than most people thought. Will scrutiny spur change?

Jun 15th 2013 | LONDON AND WASHINGTON, DC | From the print edition

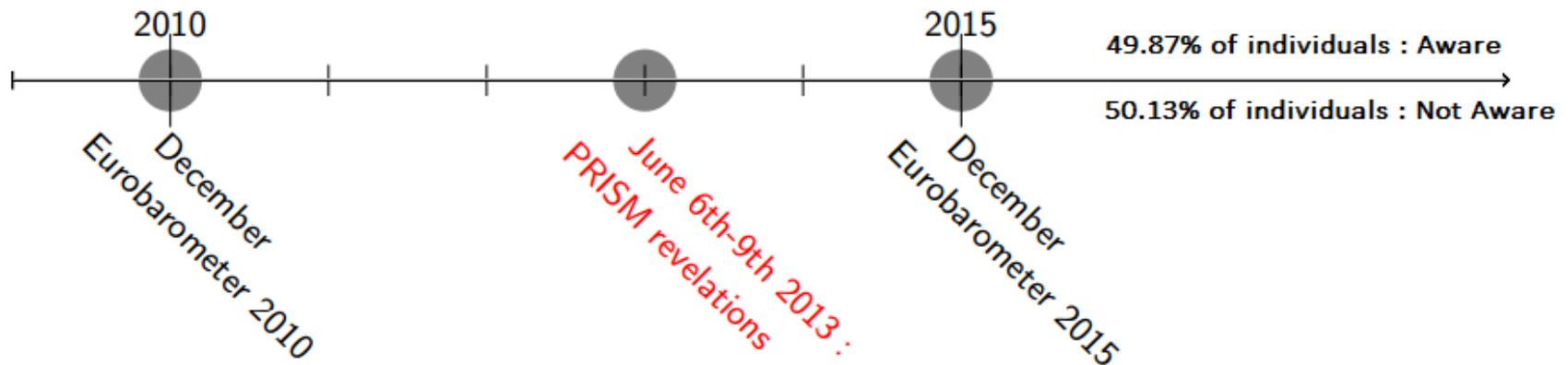
THICK and fast they came at last, and more and more and more. On June 5th the *Guardian*, a British newspaper, reported that America's National Security Agency (NSA) was collecting the telephone records of millions of Americans not suspected of crimes. A day later, the *Washington Post* reported the existence of a programme code-named

PRISM, under which the NSA collects an unknown quantity of e-mails, internet phone-calls, photos, videos, file transfers and social-networking data from big internet companies, including Google, Facebook, Apple, YouTube, Skype, Microsoft and PalTalk—a video-chat service popular in the Middle East and among Muslims.



Natural field experiment

After Snowden's revelations, the business model of the Internet firms based on the trust in the web companies may be challenged as individuals often disclose their personal data in order to access to free services available on the Internet.

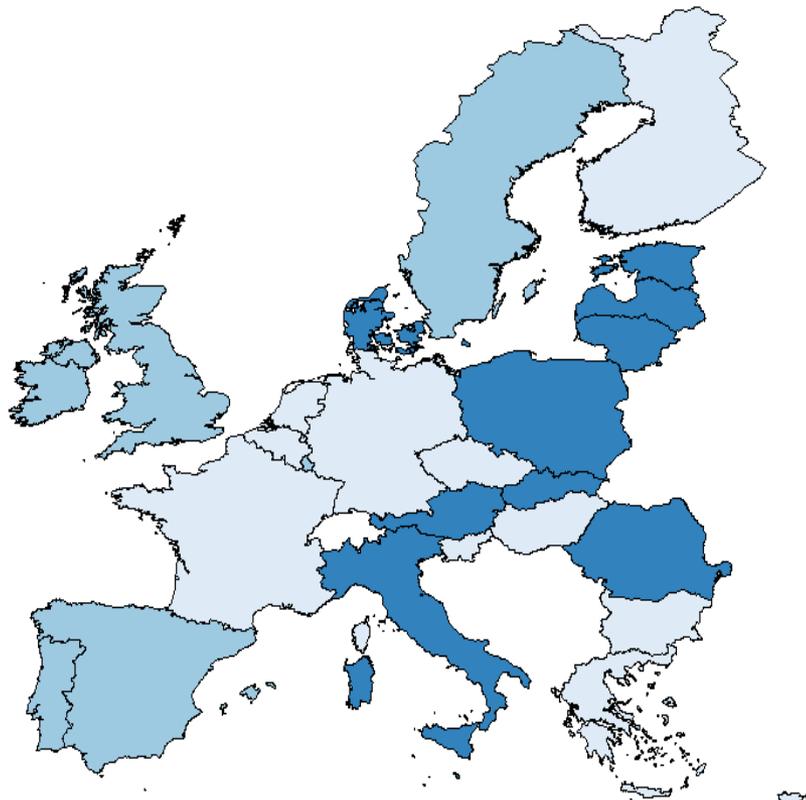


Research question and methodology

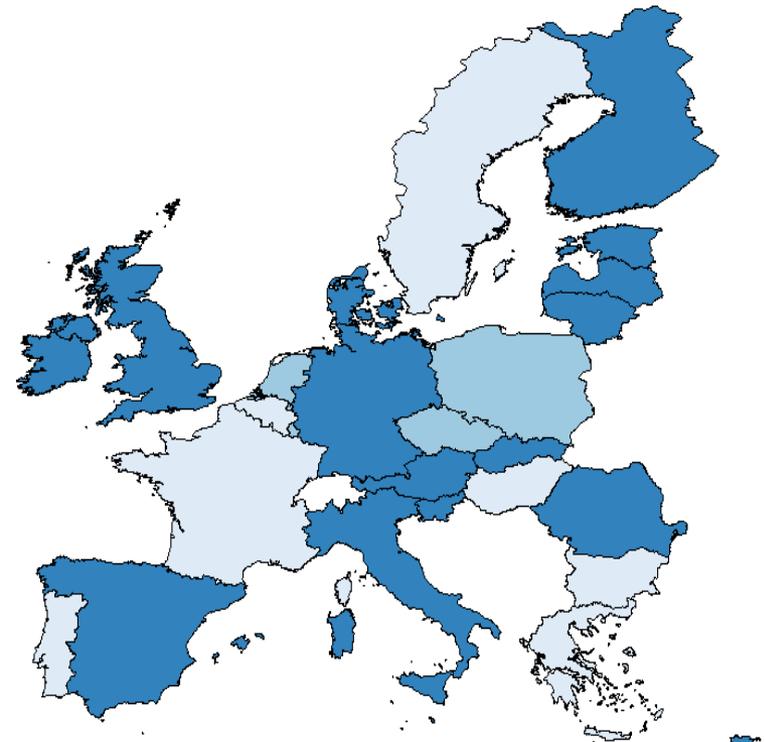
- **Intuition** : Individuals are the owners of the data and the **acceptance** of the disclosure of data is essential for the business models of many internet companies. *Is Snowden affair challenging this model?*
- Study the evolution of users' acceptance of personal data disclosure against the access to free services between 2010 and 2015 using pooled cross section (about 40000 individuals)
- **Estimation**: Econometric model on a *pooled cross section* of two European surveys and the *propensity score matching* to estimate the net effect of being informed about this scandal

Percentage of individuals accepting the model before and after the PRISM program

2010



2015



Empirical section

Econometric models

- Ordered logit: Dependent variable NotMINDFREE : degree of acceptance of the exchange of free services against personal data
- Regressors measures privacy concerns, asymetry of information, time varying variables.

Propensity score matching

- As we can disentangle the net effect of being informed, as we can match informed with non informed individuals.

Results

- The econometrics estimations on the pooled cross section show that individuals have decreased the acceptance of the model
- We show a counter-intuitive result: to be informed about privacy issues increases the probability to accept the actual model.
- Propensity score matching on informed individuals corroborate the previous results
- Policy implications: Government behaviour might affect individual privacy which affect internet companies.