

***Of Frogs and Herds:
The economics (and behavioral
economics) of privacy***

Alessandro Acquisti

Heinz College & CyLab
Carnegie Mellon University

*ICEB 2010
4-5 January 2010, Hong Kong*

The economics of privacy

- *Protection & revelation of personal data flows involve **tangible and intangible** trade-offs for the **data subject** as well as the potential **data holder***
- Some of our studies
 - Conditioning prices on purchase histories (*Marketing Science 2005*)...
 - Impact of breaches on stock market valuation (*ICIS 2006*)...
 - Impact of data breach notification laws on identity theft (*WEIS 2008*)...
 - Impact of gun owners DB publication on crime rates (*work in progress*)...

However...

- Attitudes about privacy
 - Ostensibly...
 - Top reason for not going online... (Harris Interactive)
 - Billions in lost e-tail sales... (Jupiter Research)
 - Significant reason for Internet users to avoid Ecommerce... (P&AB)
- Actual behavior
 - Dichotomy between privacy attitudes and privacy behavior
 - *Spiekermann et al. 2001, Acquisti & Gross PET 2006*

*Do people really care for privacy?
If they do, can they act on their concerns?
If they don't (or can't), should policy-makers do so on their behalf?*

A rational model of privacy decision making



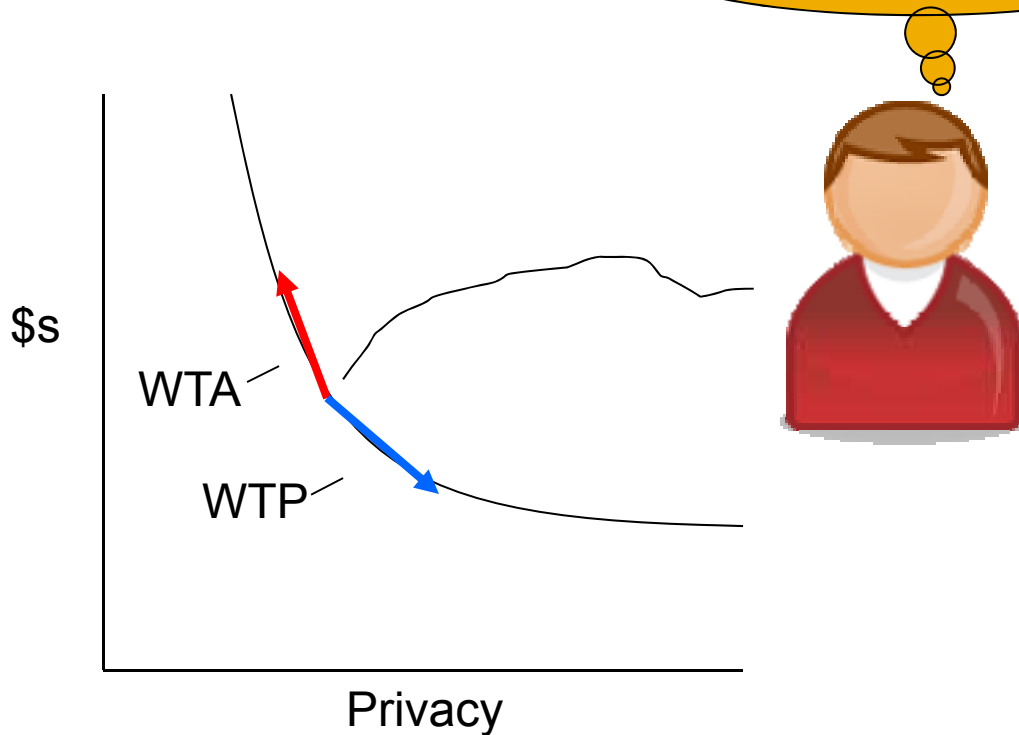
A rational model of privacy decision making

Maybe I'll find a lover... But what about my future job prospects? And what if my parents happen to log on...



A rational model of privacy decision making

$$\sum p_i \sum \frac{1}{(1+d)^t} u(\text{benefits}_{it}) - \sum q_i \sum \frac{1}{(1+d)^t} u(\text{costs}_{it})$$



Hurdles that hamper (privacy) decision making

1. Incomplete information
 - E.g.: download DOB/hometown from social network >> predict member's SSN (*PNAS 2009*)
 2. Bounded rationality
 3. Cognitive/behavioral biases, investigated by behavioral economics & decision research
 - E.g., optimism bias, hyperbolic discounting, ambiguity aversion, ...
- *Hence: the need for a behavioral, experimental economics of privacy (and information security)*

The behavioral economics of privacy

- Some of our previous and ongoing results (2004-2009)
 - Hyperbolic discounting in privacy valuations (*ACM EC 2004*)...
 - Over-confidence, optimism bias in online social networks (*WPES 2005, PET 2006*)...
 - Confidentiality assurances inhibit information disclosure (*SJDM 2007*)...
 - Individuals more likely to disclose sensitive information to unprofessional sites than professional sites (*SJDM 2007*)...
 - Herding behavior in information revelation (*SJDM 2009*)
 - Illusion of control in online social networks (*iConference 2009*)...

Can non-normative factors determine inconsistencies in privacy concerns/valuations?

- **Privacy valuations** may be not only **context-dependent**, but also
 - Malleable to non-normative factors
 - In fact, possibly internally inconsistent
- Hence, personal disclosures likely to be influenced by subtle framing, which can
 - Downplay privacy concerns
 - Act like 'alarm bells' – triggering concern for privacy that is often latent
- *Joint work with Leslie John and George Loewenstein*

Specifically: How framing impacts valuations of personal data

- Willingness to accept (WTA) money to give away information
- *vs.*
- Willingness to pay (WTP) money to protect information
- Hypothesis:
 - People assign different values to their personal information depending on whether they are focusing on **protecting it** or **revealing it**

WTA/WTP in the privacy realm

- Valuation of private information likely to change depending on whether trade-off between privacy and money is framed as
 - A problem of protection (WTP)
 - *Firewalls, anonymous browsing, (signing up for do-not-call list)*
 - A problem of disclosure (WTA)
 - *Grocery loyalty cards, sweepstakes, Internet searches*

Experimental design

- Experimental subjects asked to choose between 2 gift cards
 - We manipulated trade-offs between privacy protection and value of cards
- Subjects endowed with either:
 - **\$10 Anonymous gift card.** *"Your name will not be linked to the transactions completed with the card, and its usage will not be tracked by the researchers."*
 - **\$12 Trackable gift card.** *"Your name will be linked to the transactions completed with the card, and its usage will be tracked by the researchers."*
- Subjects asked whether they'd like to switch cards
 - From \$10 Anonymous to \$12 Trackable (WTA)
 - From \$12 Trackable to \$10 Anonymous (WTP)

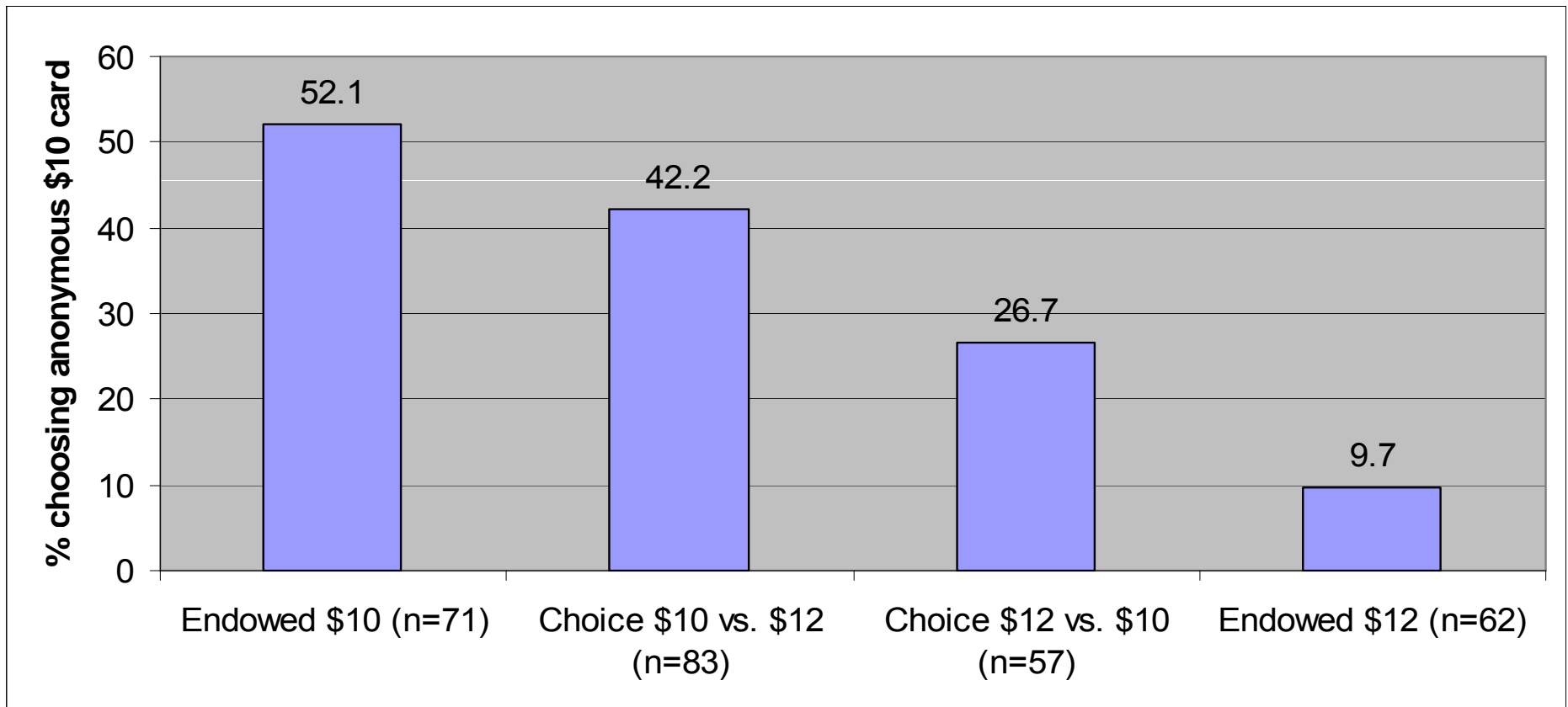
Two versions of the experiment

1. Hypothetical questionnaire
2. Actual field experiment with VISA gift cards
 - Mall patrons stopped at mall, asked to participate in (unrelated) study, offered real gift card for participation in study
 - 349 participants

Design

- 2x2 conditions between-subjects design
- Endowment conditions (2):
 - Endowed with \$10 anonymous card
 - Endowed with \$12 identified card
- Choice conditions (2):
 - \$10 anonymous card listed first
 - \$10 anonymous card listed second

Results



$\chi^2 (3) = 30.61, p < 0.0005$

Implications

- People's concerns for privacy (and security) depend, in part, on priming and framing
 - This does *not* necessarily mean that people don't care for privacy, or are "irrational," or make wrong decisions about privacy
- Rather, it implies that reliance on "revealed preferences" argument for privacy may lead to sub-optimal outcomes if privacy valuations are inconsistent...
 - People may make disclosure decisions that they stand to later regret
 - Risks greatly magnified in online information revelation
- Therefore, implications for policy-making & the debate on privacy regulation
 - E.g., Chicago School approach vs. privacy advocates
 - A problem of incentives

Hence... soft paternalism

- “Soft” or asymmetric paternalism: design systems so that they enhance (and sometimes influence) individual choice in order to increase individual and societal welfare
 - **Nudging privacy:** *using soft paternalism to address and improve security and privacy decisions through policy and technology design that anticipates and/or exploits behavioral/cognitive biases (IEEE S&P 2009)*

Soft vs. strong paternalism vs. usability

- Consider online social networks users who post dates of birth online
- Imagine that a study shows some risks associated with revealing DOBs (e.g., SSN predictions)
 - Strong paternalistic solution: ban public provision of dates of birth in online profiles
 - “Usability” solution : design a system to make it intuitive/ easy to change DOB visibility settings
 - Soft paternalistic solution?

Nudging privacy

- Saliency of information
 - Provide context to aid the user's decision - such as visually representing how many other users (or types of users) may be able to access that information
- Default settings
 - By default, DOBs not visible, unless settings are modified by user
- Hyperbolic discounting
 - Predict and show immediately SSN based on information provided
- ... and so forth

For more info

- Google: [economics privacy](#)
- Visit: <http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm>
- Email: acquisti@andrew.cmu.edu