22 June 2012 – Politecnico di Milano

Privacy in the Age of Augmented Reality

Prof. Alessandro Acquisti

The lecture of Prof. Alessandro Acquisti – Carnegie Mellon University - served to present highlights from his research field that relates to the behavioral economics of privacy and the study of privacy and disclosure behavior in online social networks[1]

Content: I. Introduction; II. Behavioral economics of privacy and the study of privacy and disclosure behavior in online social networks[2]

I. Introduction

According to the theory of economics of privacy, protection and revelation of personal data flows involve tangible and intangible trade-offs for the data subject as well as the potential data holder. Over the years we have known different attitudes towards privacy:

- Early 2000's: ostensibly, privacy concerns cost merchants billions in lost e-tail sales (Jupiter research [3]), significant reason for internet users to avoid e-commerce (P&AB 2005).
- Nowadays: self-professed privacy attitudes do not predict privacy behavior (Spiekermann 2001, Acquisti & Gross 2006[4]).

This new trend (and the incredible amount of on-line data uploaded by users), leads naturally to ask whether people really care about privacy.

[1] For more information please see: "The Economics of Privacy," Alessandro Acquisti and Laura Brandimarte. In Martin Peitz and Joel Waldfogel (eds), The Oxford Handbook of the Digital Economy, Oxford University Press, forthcoming 2011;"Faces of Facebook: Privacy in the Age of Augmented Reality" Alessandro Acquisti, Ralph Gross and Fred Stutzman; BlackHat USA, 2011; "The Impact of Relative Judgments on Concern about Privacy" Alessandro Acquisti, Leslie John and George Loewenstein. Journal of Marketing Research, forthcoming 2011; and "Strangers on a Plane: Context-dependent Willingness to Divulge Personal Information" Alessandro Acquisti, Leslie John and George Loewenstein. Journal of Consumer Research, 37(5), 858-873, 2011.

[2] Conference participants: Stefano Zanero (Politecnico di Milano), Giuseppe Vaciago (Università dell'Insubria), Andrea Rossetti (Università degli Studi di Milano), Luca Luparia (Università degli Studi di Milano), Pietro Meda (Studio Legale Meda), Davide Gabrini (Polizia Postale), Pasquale Stirparo JRC (Joint Research Centre) – European Commission, Daniele Mazzocchi (Fondazione Boella – Torino), Alessandro Mantelero (Università di Torino), Francesca Bosco (Tech and Law Center), Andrea Barili (Università di Pavia), Stefano Ricci (Università degli Studi di Milano), Monica Togliato (Studio Legale Rossotto & Partners, Federico Maggi (Politecnico di Milano), Giulia Franzoso (Università degli Studi di Milano-Bicocca), Brikena Memaj (Università degli Studi Milano-Bicocca.

[3] Jupiter Research. Seventy percent of US consumers worry about online privacy, but few take protective action, 2002. http://www.prnewswire.com/news-releases/70-of-us-consumers-worry-about-online-privacy-but-few-take-protective-action-reports-jupiter-media-metrix-77697202.html.

[4] "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook" Alessandro Acquisti and Ralph Gross. Proceedings of Privacy Enhancing Technologies Workshop (PET), Lecture Notes in Computer Science 4258, Springer, 36-58, 2006.

So we have to move from the “economics of privacy” to the “behavioral economics of privacy”.
Therefore we need to take into account other factors, such as privacy decision making hurdles:

- Asymmetric/incomplete information;
- Bounded rationality;
- Cognitive and behavioral biases.

In this new field of study it is of great importance the power of frame on the privacy evaluations: framing can change the valuation of personal data.
Test on behavioral economics shows how individual privacy valuations are strongly influenced by order and endowment effects (valuations can be affected by contextual effects) and valuations are non-normally distributed (deep gap between subjects' willingness to pay to protect the privacy of their data and their willingness to accept money in order to give up privacy protection).
People’s concerns for privacy depend on framing: individuals assign different values to the privacy of their data, depending on whether they consider the amount of money they would accept to disclose private information, or the amount of money they would pay to protect public information; but it depends also on the order in which they consider different offers for that data (priming).
In conclusion we can deduce the strong dependence of privacy evaluations on the concrete situation and - consequently - the general inconsistency of privacy evaluations.

II. Behavioral economics of privacy and the study of privacy and disclosure behavior in online social networks.

Analysis of competing Frames in the privacy debate:

A) Privacy as control & transparency Vs. Privacy as protection from control;
B) Big data increases aggregate welfare Vs. Big data extracts consumer surplus;
C) Data is the price for free services Vs. “There’s no free lunch”.

The first couple of compared frames, privacy as control and transparency versus privacy as protection from control, is the one on which Prof. Acquisti focused his talk.
First of all he explained the relation between privacy and control and showed the “paradox of control”.
There is a discrepancy between control over the publication and control over the access and usage of personal data: generally, since an individual has the control over publication of private/sensitive information, she/he gives less importance to control over the accessibility and use of that information by others. This is the paradox of control on personal data: control over publication makes the lack of control over usage less important.
Consequently people subjected to higher control increase self-disclosure (decreased privacy concern), while people with less control over the publication of their private information are less willingness to publish sensitive information (increased privacy concern).
People privacy concerns also depend on the type of detection system of the information used: a system where the information is available but it has to be searched (pull model), is generally considered less privacy-invasive than a system where the same information is provided by default, without the need to ask for it or put any effort in searching for it (push model).
The implications are:
i) is not just the publication of personal information that disturbs people but the fact that someone else will publish it for them;
ii) people care about the final use of their data, so granting individuals control on how their personal information is widespread and used is an important condition for privacy protection.
Consequently, self-regulatory approach to privacy protection, which only rely upon providing “more control” and “more transparency” to users, would be the best way forward.
In conclusion, privacy is protection from control and is not an issue of transparency; to confirm this, there are

some statistical researches discovering that only 3% of consumers read the privacy treatment, and the 75% of users think that privacy is protection from control. In particular privacy is protection from (biased) judgments.

Prof. Acquisti, with Laura Brandimarte and Joachim Vosgerau, conducted a series of experiments on field to find answers to questions like "How does information about a person's past, retrieved today, get discounted?" and – specifically - "Does information about a person's past with negative valence receive more weight on impression formation than information with positive valence?".
The hypothesis was that the impact of negative information lasts longer than the impact of positive information, not only because of asymmetric effects of valence or memory, but also because of different weights (discount rates) applied to the two types of information; and this may be due to:
i) mobilization effects[5] and evolutionary theory (Baumeister et al. 2001);
ii) negativity bias[6];
iii) negative information is more attention grabbing (Pratto & John 1991[7]).
From these experiments they understood that negative information are not just stronger than positive ones, but are also discounted differently than positive ones.
An important implication is that in the "age of augmented reality", new ICT technologies (Internet in particular) could imply the end of the forgetting thanks to their capacity to conserve data for a long time. It could be a problem when negative information revealed today will play a discrimination role in the future of individuals.
Unwanted inferences (see infra "face-recognition and privacy": getting sensitive information from an anonymous photo using social networks such as Facebook or Linked-in).

Face-recognition and privacy (online social network and data mining)

New technologies are challenging and they are changing our concept of privacy and our expectation of anonymity.
The combination of publicly available Web 2.0 data and off-the-shelf face recognition software may allow large-scale, automated, end-user individual re-identification.
Professors Acquisti, Ralph Gross and Fred Stutzman investigated the implications of face-recognition on privacy.
First of all, they started analyzing the phenomenon of face-recognition in general and found out that "though face-recognition of everyone, everywhere, all the time is not yet feasible, current technological trends suggest that most current limitations will keep fading over time"- as Prof. Acquisti said.
In confirmation of this we can see how automatic face-recognition has consistently improved and has started being used in production applications, for examples in security and web 2.0.
Secondly they conducted several specific experiments in order to draw the implications of face-recognition on privacy in the "Age of Augmented Reality", i.e. in the context of converging technologies[8]
They identified strangers online across different online services (Experiment 1), offline, in the physical world (Experiment 2), and then inferred additional, sensitive information about them, combining face

[5] Taylor, Shelley, Asymmetrical effects of positive and negative events: The mobilization-minimization hypothesis.
http://psycnet.apa.org/index.cfm?fa=search.displayRecord&uid=1991-32481-001
http://www.ncbi.nlm.nih.gov/pubmed/1891519
[6] Journal of Experimental Psychology, Seligman & Maier, 1967.
http://psych.hanover.edu/classes/learning/papers/seligman%20maier%201967.pdf
http://www.andrew.cmu.edu/user/morewedg/personal/papers/NegativeAgencyBias.pdf
[7] Pratto, F. & John, O.P., Automatic vigilance: The attention-grabbing power of negative social information., JPSP, 1991, 61, 380-391. http://psycnet.apa.org/index.cfm?fa=search.displayRecord&uid=2000-07798-002

[8] Converging technologies: (I) Increasing public self-disclosures through online social network (especially photos); (II) Continuing improvements in face recognizers' accuracy; (III) Cloud computing; (IV) Ubiquitous computing; (V) Statistical re-identification thanks to a sensitive inferences from public data.

recognition and data mining, thus blending together online and offline data (Experiment 3).

Finally, they developed a mobile phone application to demonstrate the ability to recognize and then predict someone's sensitive personal data (sexual orientation, credit score, etc…) directly from their face in real time.

"The study – Prof. Acquisti said - is less about face-recognition and more about privacy concerns raised by the convergence of various technologies. There is no obvious answer and solution to the privacy concerns raised by widely available face recognition and identified (or identifiable) facial images".

Prof. Acquisti, remembering the Google's Eric Schmidt observation "in the future, young individuals may be entitled to change their names to disown youthful improprieties", said that it could be too much optimistic; with a face-recognition highly developed system, in fact, disclaiming past improprieties would be impossible unless change someone's face.

Prof. Acquisti also said "Other than adapting to a world where every stranger in the street could predict quite accurately sensitive information about you, we need to think about policy solutions that can balance the benefits and risks of peer-based face recognition" but he does not see the solution in the self-regulation, or opt-in mechanisms (since his results are based on publicly available information).