Editor: Angela Sasse, A.Sasse@cs.ucl.ac.uk

# Complementary Perspectives on Privacy and Security: Economics

**Alessandro Acquisti** | Carnegie Mellon University

Economics and behavioral economics offer different but complementary approaches to understanding privacy and security. For this inaugural contribution to the new In Our Orbit department, I was asked to explain briefly their methodological differences and similarities, and why they matter in our thinking about security and privacy.

## A Brief Background

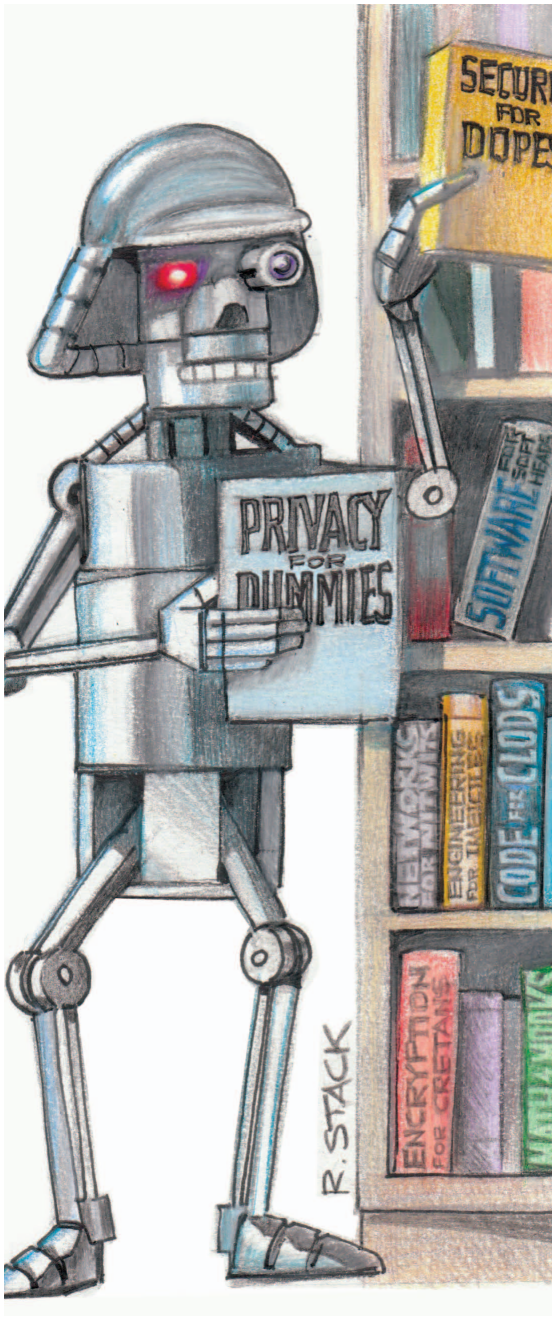
In the past decade, those of us working in privacy and security have become more active in exploring fields beyond computer science, seeking to understand how multidisciplinary results might inform cybersecurity theory and practice. Some of our forays outside of computer science have involved economics—specifically, computer scientists have become interested in the role of incentives and trade-offs in explaining security failures,[1] and economists have started applying their toolkits to calculate the optimal amount of security investment.[2] This led to the development of venues such as the Workshop on the Economics of Information Security (WEIS). As far as privacy goes, economists had been interested in the subject since the late 1970s.[3]

A second field approached by security and privacy researchers is psychology. Human factors[4,5] and usability[6,7] researchers were already influencing privacy and security scholars by the time economists entered the arena. Similarly, social scientists from psychology to sociology had been studying privacy and disclosure for decades.[8,9] The combination of economics, psychology, and computer science led to the development of what could be called the behavioral economics of privacy[10] and information security,[11] and to gatherings such as the Security and Human Behavior (SHB) workshop.

## Two Streams

At a high level, traditional neoclassical economics—the type of economics taught in most North American undergraduate and graduate programs—focuses on agents (consumers or firms) that attempt to maximize an objective function (utility or profits) under certain constraints (budgets). Neoclassical economics assumes that those economic agents are rational, in the sense that they engage in forward-looking maximization of said objective function, and in applying Bayesian updating (correctly using all available information and updating beliefs based on new knowledge).

Behavioral economics, on the other hand, studies systematic—and therefore predictable—deviations from such rational maximization behavior. Behavioral economics does not suggest that people are "irrational" in the sense of being erratic, naïve, or faulty. Rather, it critiques the assumptions underlying the economic interpretation of rationality. Behavioral




1540-7993/13/$31.00 © 2013 IEEE

This issue introduces a new department to *IEEE Security & Privacy*: In Our Orbit. Over the past 15 years, many security and privacy researchers, practitioners, and policymakers have begun to realize that results and perspectives from other disciplines can help us think about and solve security, privacy, and dependability problems. In Our Orbit will provide insights from experts on advances in their disciplines. By bringing these insights into your orbit, we hope to stimulate your thinking and eventually make your research, practice, or policy more effective. —Shari Lawrence Pfleeger, editor in chief, and Angela Sasse, department editor

economists see economic agents as bounded in their rationality; biases and emotions can play as important a role in affecting decision making as the attempt to maximize utility.

Applying neoclassical economics to security trade-offs can be enlightening in many regards. For example, Cormac Herley points out that a user's rejection of security advice might be economically rational in a neoclassical view of the world.[12] Herley considers microeconomic trade-offs to point out that the cost of acting on security suggestions might actually be higher than the expected benefits. A similar argument is proposed by Adam Shostack and Paul Syverson in the case of privacy: perhaps it is rational to exchange private information for tiny rewards if the expected cost associated with doing so is even smaller.[13]

Behavioral economics takes a different approach and offers different insights—and sometimes alternative explanations. It shows how lack of information (or asymmetric information), inability to process all available information (or bounded rationality), and cognitive or behavioral biases can interfere with and affect the analysis of security and privacy's microeconomic trade-offs, and therefore the conclusions of traditional economic models. For instance, hyperbolic discounting—an alternative model of how humans discount costs and benefits over time, compared to the exponential model common in economics—can impact privacy and security decision making. Models of privacy behavior that include hyperbolic discounting (and its associated immediate gratification bias) offer one explanation—although by no means the only one—for why individuals genuinely interested in protecting their privacy might not do so, due to the intertemporal nature of privacy costs and benefits. The benefits of disclosing data are often immediate, while the potential associated costs usually happen—if at all—later in time.[10]

## Positive and Normative Arguments

Another way in which economics and behavioral economics can complement each other in their contribution to cybersecurity research is in the nature of their arguments. Economists often distinguish between positive and normative arguments: positive economics describe the world as it is, and normative economics describe the world as it should be. In principle, both neoclassical and behavioral economics can be used to make either type of claim. For instance, a positive, neoclassical economic statement about privacy could consist of observing that data breach notification laws appear to have decreased identity theft in the US by 6 percent.[14] A normative statement could be that litigation should be preferred to regulation (or regulation to litigation) to achieve a desirable balance between personal information protection and IT innovation.

Although both economic and behavioral economic models can be used for either normative or positive claims, it is not always the case that they are. For instance, economists more often use structural models, which are then applied to make predictions and policy recommendations (a normative focus), whereas behavioral economists more often use reduced form models to describe a phenomenon (such as a cognitive bias) and its causes (its underlying psychological processes)—a positive focus.

Much of the current behavioral experimental research in privacy and security decision making should be interpreted first and foremost as a positive, not normative, endeavor. It attempts to understand how people make decisions that involve privacy and security trade-offs, and how those decisions can be affected by heuristic and biases. In doing so, behavioral privacy or security research could raise questions about the conclusions of economic models based on empirically suspect assumptions about individual behavior (such as access to complete information or unbounded cognitive powers), without necessarily attempting to say how individuals should act instead (for instance, whether they should increase or decrease security, or protect their privacy more or less). That extra step would require the ability to precisely calculate and compare the costs and benefits associated with information protection and information sharing—a notoriously difficult, if not impossible, task in the case of privacy. In other words, uncovering a bias in privacy decision making does not imply, per se, that individuals should protect their information more or less. But it does signal that, *if* the individual's or policymaker's goal is to protect privacy, then one should consider the impact of said bias on the probability of achieving the goal.

However, it is also true that once a certain decision-making bias is uncovered (such as hyperbolic discounting), behavioral economists can start researching ways to address that bias (for instance, by investigating nudging interventions aimed at countering the effect that hyperbolic discounting can have on people's wellness and satisfaction). Whether such interventions will succeed or fail in de-biasing decision making is neither a victory nor a loss of behavioral economic research itself—no more than an astronomer is responsible for an asteroid hitting the Earth after accurately calculating it will. Indeed, behavioral economics could well predict that certain types of interventions (such as just-in-time warnings) will work, while other interventions (such as health warnings on packs of cigarettes) will not.

This type of experimental behavioral research, which tends to be quantitative, can be supplemented by methodologies and investigations from other disciplines—structured and unstructured interviews, qualitative focus groups, user testing, and so forth. As privacy and security research becomes more interdisciplinary, researchers have an opportunity to develop a richer understanding of how people perceive threats, risks, and privacy and security controls—and how their perceptions influence their actions. I am hopeful that in future contributions to In Our Orbit, research techniques and findings from diverse disciplines will continue to be highlighted, demonstrating how they can enrich our methods, policies, and outcomes. ■


## Acknowledgments

I thank Shari Lawrence Pfleeger and Angela Sasse for proposing the topic of this article and for their useful suggestions. I also thank Idris Adjerid, Ross Anderson, Laura Brandimarte, Bruce Schneier, and Cormac Herley for many helpful comments.


## References


1. R. Anderson, "Why Information Security Is Hard: An Economic Perspective," *Proc. 17th Ann. Computer Security Applications Conf.* (ACSAC 01), IEEE, 2001.
2. L.A. Gordon and M.P. Loeb, "The Economics of Information Security Investment," *ACM Trans. Information and System Security*, vol. 5, no. 4, 2002, pp. 438–457.
3. R. Posner, "An Economic Theory of Privacy," *Regulation*, 1978, pp. 19–26.
4. A. Adams and M.A. Sasse, "Users Are Not the Enemy," *Comm. ACM*, vol. 42, no. 12, 1999, pp. 40–46.
5. L.J. Camp, *Trust and Risk in Internet Commerce*, MIT Press, 2001.
6. A. Whitten and J.D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," *Proc. 8th Usenix Security Symp.*, McGraw-Hill, 1999.
7. L. Cranor and S. Garfinkel, *Security and Usability: Designing Secure Systems that People Can Use*, O'Reilly Media, 2005.
8. I. Altman, *The Environment and Social Behavior*, Brooks/Cole, 1975.
9. V.J. Derlega and A.L. Chaikin, "Privacy and Self-Disclosure in Social Relationships," *J. Social Issues*, vol. 33, no. 3, 1977, pp. 102–115.
10. A. Acquisti, "Privacy in Electronic Commerce and the Economics of Immediate Gratification," *Proc. 5th ACM Conf. Electronic Commerce*, ACM, 2004.
11. B. Schneier, "The Psychology of Security," *Comm. ACM*, vol. 50, no. 5, 2007, p. 128.
12. C. Herley, "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users," *Proc. New Security Paradigms Workshop*, 2009.
13. A. Shostack and P. Syverson, "What Price Privacy?" *Economics of Information Security*, 2004, pp. 129–142.
14. S. Romanosky, R. Telang, and A. Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft?" *J. Policy Analysis and Management*, vol. 30, no. 2, 2011, pp. 256–286.



**Alessandro Acquisti** is an associate professor at the Heinz College, Carnegie Mellon University. His research interests include the economics and behavioral economics of privacy. Acquisti has a PhD in information systems from the University of California, Berkeley. Contact him at acquisti@andrew.cmu.edu.