TESTIMONY

Professor Alessandro Acquisti
Heinz College, Carnegie Mellon University

Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing and
Trade, U.S. House of Representatives

Understanding Consumer Attitudes About Privacy

October 13, 2011

Chairman Bono Mack, Ranking Member Butterfield, and Members of the Subcommittee:
I was honored to receive the invitation to appear before you today to discuss the topic of 'Understanding Consumer Attitudes About Privacy.'

My name is Alessandro Acquisti. I am an associate professor at the Heinz College, Carnegie Mellon University (CMU), and the co-director of CMU's Center for Behavioral Decision Research (CBDR).[1] I am an economist by training, and I have been studying the economics and behavioral economics of privacy for about 10 years. My research combines economics, experimental behavioral decision research, and information technology to investigate the trade-offs associated with the protection and disclosure of personal information, and how consumers calculate, and make decisions about, those trade-offs.

Some of my work focuses on quantifying the value of personal data, the costs of privacy invasions, and the benefits of information disclosure.[2] My remarks in this testimony, however, will concern research that I and others have carried out into the field of consumer privacy attitudes and behavior. I will discuss how consumers perceive, and make decisions about, the values, costs, and benefits associated with the disclosure of their personal information.

In my testimony, I will highlight three findings:

First, consumers want more than one thing when it comes to privacy and disclosure. Consumers enjoy disclosing information online to friends, and enjoy receiving personalized and free services as a result of the information they disclose. However, they also want the information they reveal to others to be protected, and they are concerned about misuses of their personal data.

Second, consumers face major hurdles in properly trading-off privacy and disclosure in the marketplace. Problems of asymmetric information, bounded rationality, and cognitive and behavior biases make it difficult for consumers to choose optimally between protecting privacy and sharing data.

Third, industry and academic research on privacy enhancing technologies suggests that consumers and firms can simultaneously achieve information sharing and privacy protection. In fact, research in this area shows that it is possible for companies to make innovative uses of personal data, and tap information as an economic resource, in ways that do not sacrifice consumer privacy. Therefore, a critical question for Congress is how to create incentives that will foster the deployment of these innovative technologies.

1. Consumers Attitudes: Consumers Want Privacy, Like Sharing

Over the years, surveys have found repeated evidence of significant privacy concerns among US consumers.[3] Most Americans believe that their right to privacy is "under serious threat" and express concerns over the way businesses collect their personal data.[4] According to some studies, a majority of individuals believe that privacy is a right, and that being asked to pay for it is "extortion."[5] Many individuals favor governmental intervention and legislation over self-regulation as a means for privacy protection.[6] Other surveys report that privacy concerns negatively affect consumers' willingness to purchase online or register on websites.[7]

Consumers seem especially troubled by tracking technologies. In a survey of 587 US adults about attitudes towards location-tracking techniques, Tsai et al. found widespread and elevated concerns about the control over data about individuals' location; generally, "respondents [felt that] the risks of using location-sharing technologies outweigh[ed] the benefits."[8] In a nationally representative survey about online behavioral targeting by marketers, Turow et al. found that 66% of US consumers did not want marketers to tailor advertisements to their interests, and that the majority "mistakenly believe[d] that current government laws restrict companies from selling wide-ranging data about them."[9] Very similar findings were reported in a different study by CMU researchers about targeted advertising.[10]

Recently, empirical experimental research has provided behavioral support for the view that consumers care for privacy: when decision-making hurdles are mitigated, consumers make deliberate decisions to protect their data, at the cost of foregoing monetary advantages.[11]

However, other market-based evidence, surveys,[12] and experiments[13] have highlighted apparent discrepancies between privacy attitudes (what consumers claim in surveys) and actual behavior. Individuals seem willing to trade privacy for convenience and bargain the release of personal information in exchange for relatively small rewards. The success of many social media services indicates that consumers like sharing information online with their friends, and enjoy the free services or personalized experiences that are made possible by sharing personal information with online providers.

2. Privacy Behavior: Hurdles In Decision Making

Consumers' willingness to share personal information is not in contradiction with their desire for privacy.[14] In economic terms, both the protection and the disclosure of personal information carry tangible and intangible trade-offs for data subjects and data holders alike. In an information economy, personal information is a currency that both consumers and firms can try to use strategically, to optimize those trade-offs.

Research, however, suggests that consumers face significant challenges in navigating those complex trade-offs in ways that reflect their self-interests. Due to those challenges, actual privacy behavior may differ from stated attitudes and, more importantly, consumers' decisions to reveal or protect personal information may be suboptimal. Roughly speaking, research has uncovered three types of hurdles that can impair privacy decision making:

a) *Asymmetric information*. Research has suggested that US consumers are often ill-informed about the collection and usage of their personal information, and the consequences of those usages. This puts them in a position of asymmetric information, and sometimes disadvantage, relative to the data holders that collect and use that information. For instance, studies have shown that websites have used tracking technologies such as "flash cookies" without disclosing their presence to consumers, and sometimes even in ways that stand directly in contrast to consumers' revealed preferences.[15] Other studies have shown that a majority of consumers mistakenly interpret the presence of a privacy policy on a website as implying privacy

protection,[16] and that members of social network sites hold erroneous beliefs about the actual visibility of their online profiles and the way social media companies handle their data.[17]

b) *Bounded rationality*. As consumers, we are limited in our ability to process information available to us and formulate rational plans for solving complex problems.[18] In the field of privacy, research has shown that 54% of privacy policies are written in ways that render them beyond the grasp of 57% of the Internet population (requiring the equivalent of more than fourteen years of education).[19] Furthermore, if US consumers were to read online privacy policies word–for–word, the opportunity costs to the economy of the time lost reading would be about $652 billion annually.[20] The problem of bounded rationality is exacerbated by the fact that the proliferation of consumer data tracking and progresses in data mining have made it possible to re-identify seemingly anonymous data and infer sensitive information from non-sensitive data. In experiments at Carnegie Mellon University, my co-authors and I were able to predict individuals' SSNs using simple demographic data made available by the individuals themselves through their social media profiles.[21] We were also able to identify (and infer personal information about) individuals in public spaces using face recognition technologies and photos made publicly available by the targets on social networking sites.[22] Consumers are unlikely to predict how the non-sensitive information they reveal today will be aggregated and analyzed tomorrow to produce such sensitive inferences.

c) *Cognitive and behavioral biases*. Even if consumers had access to complete and perfect information about all usages of their personal information, and all trade-offs associated with those usages, a host of cognitive and behavioral biases (that is, systematic deviations from theoretically rational decision making) may impact their marketplace behavior, leading to suboptimal disclosure decisions. Such biases have been analyzed by behavioral economists and decision researchers for several years. Some examples applicable to the field of privacy include:

- *Instant gratification bias.* Human beings tend to value the present more than the future, which may lead consumers to underappreciate future negative

consequences of current actions.[23] In previous research, I have shown that while the benefits of information disclosure are often immediate, the costs associated with those disclosures are not just uncertain, but appear as distant in the future. As a consequence, even when the benefits of disclosure may be small compared to its possible risks (for instance, identity theft), consumers may give in to immediate gratification, disclosing information that may put them at risk in the future.[24]

- *The paradox of control in privacy decision making*. In a series of experiments at Carnegie Mellon University, we have found that increasing the feeling of control over the release of private information can decrease individuals' concern about privacy, and paradoxically increase their propensity to disclose sensitive information - even when the objective risks associated with such disclosures do not change or, in fact, *worsen*. Our findings highlight how technologies that make individuals feel more in control over the release of personal information may have the consequence of eliciting greater disclosure of sensitive information and more elevated privacy risks.[25]
- Numerous additional experiments we ran at Carnegie Mellon University (online, in the lab, or in natural conditions) suggest that the disclosure of personal and even sensitive information by individuals can be manipulated merely by subtly altering the interface of Internet services – for instance, by showing that other individuals have made sensitive disclosures,[26] by asking questions covertly so that the act of disclosing is not salient,[27] or by altering the order in which questions of varying sensitivity are asked.[28]

The results in this area suggest that consumers often lack the information, resources, foresight or self-insight to make optimal decisions about privacy protection and information disclosure. In fact, the decision-making challenges that consumers face in the marketplace can be, and sometimes have been, exploited by firms to nudge consumers towards more disclosures.[29]

On the other hand, research suggests that, *if and when* both informational and behavioral gaps are addressed, consumers make conscious decisions to protect their privacy.

In an experiment with actual cash incentives and real privacy/monetary trade-offs, my co-authors and I investigated whether more prominent, salient, and straightforward information comparing the data handling strategies of different merchants will cause consumers to incorporate privacy considerations into their online purchasing decisions. We designed an experiment in which a shopping search engine interface clearly and compactly compared privacy policy information for different merchants. When such information was made available, consumers tended to purchase from online retailers who better protected their privacy. In fact, our experiment indicated that when comparative privacy information was made more salient and accessible, consumers were willing to pay a *premium* to purchase from more privacy protective websites.[30]

In another series of experiments, we examined the power of framing on consumers' valuations of their personal data. In one of those experiments, subjects were asked to choose between a $10 gift card with privacy protection and a $12 gift card with no such protection. In a first condition, subjects were first endowed with the card with more protection, and then asked whether they were wanted to swap that card for the more valuable, but less protected, card. In a second condition, subjects were presented with exactly the same two alternatives – but the order in which they received the cards was inverted. Our subjects were five times more likely to choose privacy protection (and reject the additional cash provided by the $12 card) in the first condition, in which they had been primed to think that their privacy would be, by default, protected. The results suggest that consumers who start from positions of greater privacy protection are much more likely to forego monetary offers and preserve that protection than consumers who feel that their data is not protected. As a consequence, repeated claims that consumers do not have privacy protection may be self-fulfilling: if consumers are told not to expect privacy, then their expectations may be altered, and they may end up valuing privacy less.[31]

3. Privacy Enhancing Technologies: Sharing Data While Protecting Privacy

While self-regulatory solutions based on notice and choice do offer consumers some degree of transparency and control, they are unlikely to solve consumers' hurdles in privacy decision

making, and sometimes fail to create sufficient incentives for firms to comply. For instance, recent Carnegie Mellon research on behavioral targeting and opt-out technologies reported numerous instances of non-compliance with the Network Advertising Initiative (NAI) and Digital Advertising Alliance (DAA) behavioral ads opt-out mechanisms among 100 leading websites.[32] Related research also indicated that consumers do not understand what they are opting out of, have difficulty opting out, and are not able to distinguish among the hundreds of tracking companies to make informed opt-out decisions.[33]

However, industry and academic labs across the United States have also developed other technologies that may address the problem of consumers' decision making hurdles, without sacrificing firms' ability to access data and innovate. "Privacy Enhancing Technologies" (or PETs) can be used to protect, aggregate, and anonymize those data in ways that are both effective (in the sense that re-identifying individual information becomes so costly to discourage the attempt) and efficient (in the sense that the desired transaction can be completed with no or minor additional costs for the parties involved). In other words, privacy-enhancing principles can be utilized without limiting the main purpose of an application or a transaction.

A vast body of research in privacy enhancing technologies suggests, in fact, that cryptographic protocols can be leveraged to satisfy both needs for data sharing and needs for data privacy. Not only is it already possible to complete verifiable and yet privacy enhanced transactions in areas as diverse as electronic payments,[34] online communications,[35] Internet browsing,[36] or electronic voting;[37] but it is also possible to have credential systems that provide authentication without identification,[38] share personal preferences while protecting privacy,[39] leverage the power of recommender systems and collaborative filtering without exposing individual identities,[40] or even execute calculations while keeping data encrypted and confidential,[41] opening the doors for novel scenarios of privacy preserving data gathering and analysis, and even privacy-preserving behavioural targeting.[42]

In other words, privacy enhancing technologies may make it possible to reach equilibria where data holders can still analyse and act upon vast amounts of micro-data, while individual information stays protected. Hence, results in this area suggest that there are ways to protect privacy without causing inefficiencies in the marketplace. Arguably, the transition to these new

equilibria would not be costless; but it could be welfare-enhancing for consumers and society as a whole.[43] Such transition could also provide the right conditions for new business models, and – as consumers develop greater trust in the way their information is protected - for more truthful sharing of consumers' data.

4. Conclusion

Consumers' attitudes towards privacy and disclosure are nuanced. Consumers enjoy exchanging information online with friends and receiving personalized services through the information they disclose. But they also want the information they reveal to be protected, and remain concerned about abuses of their personal information. Consumers thus face significant decision making hurdles when navigating the complex privacy trade-offs that emerge in the marketplace. Research suggests that self-regulatory solutions do not address those hurdles. Giving consumers knowledge of and control over the usage of their data may be *necessary* conditions for privacy protection; but empirical evidence supported by behavioral economics and decision research suggests that they are not *sufficient* conditions. As Loewenstein and Haisley write, "[i]nformational interventions are only effective against one of the two broad categories of mistakes that people make – those that result from incorrect information – and not against the other: self-control problems."[44]

However, both industry and academic labs in the United States have developed tools that can help both consumers and companies find a more desirable balance between information disclosure and information protection, and achieve better trade-offs. Research in the area of privacy enhancing technologies shows that it is possible for companies to make innovative uses of personal data, and tap information as an economic resource, in ways that do not sacrifice privacy. Policy makers should consider how to create mechanisms that will incentivize the deployment of these innovative technologies.

Thank you for inviting me to testify today. I look forward to answering your questions.

---

[1] Http://www.heinz.cmu.edu/~acquisti/

[2] A. Acquisti, 2010. “The Economics Of Personal Data and The Economics Of Privacy.” Commissioned By The OECD, For The OECD Roundtable On The Economics Of Privacy and Personal Data, Paris, December 2010. http://www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-OECD-22-11-10.pdf.

[3] Early Works In This Area Include: A.F. Westin, 1991. “Harris-Equifax Consumer Privacy Survey.”; M. Ackerman, L. Cranor, and J. Reagle, 1999. “Privacy In Ecommerce: Examining User Scenarios and Privacy Preferences.” ACM Electronic Commerce Conference (EC), 1-8. More Recent Studies Include: Harris Interactive, 2001. “Privacy On and Off The Internet: What Consumers Want.”; CBS News, 2005. “Poll: Privacy Rights Under Attack.” http://www.cbsnews.com/stories/2005/09/30/opinion/polls/main89473.shtml; J. Turow, L. Feldman, K. Meltzer, 2005. “Open To Exploitation: American Shoppers Online and Offline.” A Report From The Annenberg Public Policy Center Of The University Of Pennsylvania; Burst Media, 2009. “Online Privacy Still A Consumer Concern.” http://www.burstmedia.com/assets/newsletter/items/2009_02_01.pdf.

[4] CBS News, 2005. “Poll: Privacy Rights Under Attack.” http://www.cbsnews.com/stories/2005/09/30/opinion/polls/main89473.shtml.

[5] A.M. McDonald, and L.F. Cranor, 2010. “Americans’ Attitudes About Internet Behavioral Advertising Practices.” Workshop On Privacy In The Electronic Society (WPES).

[6] A. Acquisti, and J. Grossklags, 2005. “Privacy and Rationality In Decision Making.” IEEE Security and Privacy 3(1) 26–33. http://www.heinz.cmu.edu/~acquisti/papers/acquisti.pdf.

[7] Privacy & American Business (P&Ab). 2005. “New Survey Reports An Increase In Id Theft and Decrease In Consumer Confidence.” Conducted By Harris Interactive. http://www.pandab.org/deloitteidsurveypr.html.

[8] J. Tsai, P. Kelley, L. Cranor, and N. Sadeh, 2009. “Location-Sharing Technologies: Privacy Risks and Controls." Telecommunications Policy Research Conference (TPRC).

[9] J. Turow, J. King, C. Hoofnagle, A. Bleakley, and M. Hennessy, 2009. “Americans Reject Tailored Advertising and Three Activities That Enable It.” Available At SSRN: http://ssrn.com/abstract=1478214.

[10] A.M. McDonald, and L.F. Cranor, 2010. “Americans’ Attitudes About Internet Behavioral Advertising Practices.” Workshop On Privacy In The Electronic Society (WPES).

[11] J. Tsai, S. Egelman, L. Cranor, and A. Acquisti, 2011. “The Effect Of Online Privacy Information On Purchasing Behavior: An Experimental Study.” Information Systems Research, 22, 254-268. http://www.heinz.cmu.edu/~acquisti/papers/acquisti-onlinepurchasing-privacy.pdf. A. Acquisti, L. John, and G. Loewenstein, 2010. “What Is Privacy Worth?” In Workshop On The Economics of Information Security (WISE). (Leading Paper, 2010 Future Of Privacy Forum's Best “Privacy Papers For Policy Makers” Competition.) http://www.heinz.cmu.edu/~acquisti/papers/acquisti-ISR-worth.pdf.

[12] Harris Interactive, 2003. "Most People Are 'Privacy Pragmatists' Who, While Concerned About Privacy, Will Sometimes Trade It Off For Other Benefits." www.harrisinteractive.com/harris_poll/index.asp?pid=365.

[13] S. Spiekermann, J. Grossklags, and B. Berendt, 2001. "E-Privacy In Second Generation E-Commerce: Privacy Preferences Versus Actual Behavior," ACM Electronic Commerce Conference (EC), 38–47.

[14] Attitudes framed in broad scenarios are not accurate predictors of context-specific behavior. See M. Fishbein and I. Ajzen, 1975. *Belief, Attitude, Intention and Behavior: An Introduction To Theory and Research*, Addison-Wesley.

[15] Websites Have Used Flash Cookies To Surreptitiously Re-Instantiate cookies deleted by users. See A. Soltani, S. Canty, Q. Mayo, L. Thomas, and C. Hoofnagle, 2009. "Flash Cookies and Privacy." Available At SSRN: http://ssrn.com/abstract=1446862.

[16] J. Turow, C. Hoofnagle, D. Mulligan, N. Good, and J. Grossklags, 2006. "Consumers & Privacy In The Coming Decade." Session On Communicating With Consumers In The Next Tech-Ade - The Impact Of Demographics and Shifting Consumer Attitudes, Public Hearings On Protecting Consumers In The Next Tech-Age, Federal Trade Commission (FTC), Washington D.C., November 6 - 8, 2006.

[17] Acquisti, A. and J. Grossklags, 2005. "Privacy and Rationality In Individual Decision Making." IEEE Security and Privacy 3 (1), 24-30. The study was contacted in 2005. As consumers get more informed about the privacy trade-offs associated with an existing technology (for instance, online social networks), new tracking technologies often arise that leave the consumer uninformed (for instance, flash cookies and behavioral tracking).

[18] H. Simon, 1957. "A Behavioral Model Of Rational Choice." In *Models Of Man, Social and Rational: Mathematical Essays On Rational Human Behavior In A Social Setting*. New York: Wiley. H. Simon, Herbert, 1991. "Bounded Rationality and Organizational Learning." Organization Science, 2 (1): 125-134.

[19] C. Jensen and C. Potts, 2003. "Privacy Policies Examined: Fair Warning Or Fair Game?" GVU Technical Report 03-04, ftp://ftp.cc.gatech.edu/pub/gvu/tr/2003/03-04.pdf.

[20] A. McDonald, and L. Cranor, 2008. "The Cost Of Reading Privacy Policies." I/S: A Journal Of Law and Policy For The Information Society.

[21] A. Acquisti and R. Gross, 2009. "Predicting Social Security Numbers From Public Data." Proceedings Of The National Academy Of Science, 106(27), 10975-10980. http://www.pnas.org/content/106/27/10975.full.pdf+html.

[22] A. Acquisti, R. Gross, and F. Stutzman, 2011. "Faces Of Facebook: Privacy In The Age Of Augmented Reality." Blackhat USA. http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/.

[23] T. O'Donoghue and M. Rabin, 2000. "The Economics Of Immediate Gratification," Journal Behavioral Decision Making, 13, 233–250.

[24] A. Acquisti, 2004. "Privacy In Electronic Commerce and The Economics Of Immediate Gratification." ACM Electronic Commerce Conference (EC), 21-29. http://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf. Also see: A. Acquisti, and J. Grossklags, 2005. "Privacy and Rationality In Decision Making." IEEE Security and Privacy 3(1) 26–33.

[25] L. Brandimarte, A. Acquisti, and G. Loewenstein, 2010. "Misplaced Confidences: Privacy and The Control Paradox." CIST. (Winner, Best Doctoral Student Paper Award, Cist 2010; Runner-Up, Best Paper Award, Cist 2010; Leading Paper, 2010 Future Of Privacy Forum's Best "Privacy Papers For Policy Makers" Competition.) http://www.heinz.cmu.edu/~acquisti/papers/acquisti-SPPS.pdf.

[26] A. Acquisti, L. John, and G. Loewenstein, 2011. "The Impact Of Relative Judgments On Concern About Privacy." Journal Of Marketing Research, Forthcoming 2011. http://www.heinz.cmu.edu/~acquisti/papers/acquisti-JMR.pdf.

[27] L. John, A. Acquisti, and G. Loewenstein, 2011. "Strangers On A Plane: Context-Dependent Willingness To Divulge Personal Information." Journal Of Consumer Research, 37(5), 858-873. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1430482.

[28] A. Acquisti, L. John, and G. Loewenstein, 2011. "The Impact Of Relative Judgments On Concern About Privacy." Journal Of Marketing Research, Forthcoming 2011. http://www.heinz.cmu.edu/~acquisti/papers/acquisti-JMR.pdf.

[29] R. Balebako, P. G. Leon, H. Almuhimed, P.G. Kelley, J. Mugan, A. Acquisti, L. Cranor and N. Sadeh, 2011. "Nudging Users Towards Privacy On Mobile Devices," Proceedings Of The Workshop On Persuasion, Nudge, Influence and Coercion, Computer-Human Interaction Conference (CHI).

[30] J. Tsai, S. Egelman, L. Cranor, and A. Acquisti, 2011. "The Effect Of Online Privacy Information On Purchasing Behavior: An Experimental Study." Information Systems Research, 22, 254-268.

[31] A. Acquisti, L. John, and G. Loewenstein, 2010. "What Is Privacy Worth?" In Workshop On The Economics of Information Security (WISE). (Leading Paper, 2010 Future Of Privacy Forum's Best "Privacy Papers For Policy Makers" Competition.) http://www.heinz.cmu.edu/~acquisti/papers/acquisti-ISR-worth.pdf.

[32] S. Komanduri, R. Shay, G. Norcie, B. Ur, L. Cranor, 2011. "Adchoices? Compliance With Online Behavioral Advertising Notice and Choice Requirements." Carnegie Mellon CyLab Technical Report CMU-Cylab-11-005. http://www.cylab.cmu.edu/research/techreports/2011/tr_cylab11005.html.

[33] P. Leon, B. Ur, R. Balebako, L. Cranor, R. Shay, and Y. Wang, 2011. "Why Johnny Can't Opt Out: A Usability Evaluation Of Tools To Limit Online Behavioral Advertising." Under Review. [Draft Available From The Authors].

[34] D. Chaum, 1983. “Blind Signatures For Untraceable Payments.” Advances In Cryptology, 199-203. Plenum Press.

[35] D. Chaum 1985. “Security Without Identification: Transaction Systems To Make Big Brother Obsolete.” Communications Of The ACM 28 (10), 1030-1044.

[36] R. Dingledine, N. Mathewson, and P. Syverson, 2004. “Tor: The Second-Generation Onion Router.” Usenix Security Symposium, 13, 21.

[37] J.C. Benaloh, 1987. *Verifiable Secret-Ballot Elections*. Ph. D. Thesis, Yale University.

[38] J. Camenisch, J. and A. Lysyanskaya, 2001. “An Efficient System For Non-Transferable Anonymous Credentials With Optional Anonymity Revocation.” Advances In Cryptology - Eurocrypt, 93-118. Springer-Verlag, Lncs 2045.

[39] E. Adar and B. Huberamn, 2001. “A Market For Secrets.” First Monday 6, 200-209.

[40] J. Canny, 2002. “Collaborative Filtering With Privacy.” IEEE Symposium On Security and Privacy, 45-57.

[41] C. Gentry, 2009. “Fully Homomorphic Encryption Using Ideal Lattices. ACM Symposium On Theory Of Computing, 169-178.

[42] V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum, S. Barocas, 2010. “Adnostic: Privacy Preserving Targeted Advertising.” NDSS 2010.

[43] A. Acquisti, 2008. Identity Management, Privacy, and Price Discrimination. IEEE Security & Privacy, 46-50.

[44] G. Loewenstein and E. Haisley, 2008. “The Economist As Therapist: Methodological Ramifications Of ‘Light’ Paternalism.” *Perspectives On The Future Of Economics: Positive and Normative Foundations*, A. Schotter & A. Caplin (Eds.).