Comment

Federal Trade Commission
Informational Injury Workshop
P175413

The Program on Economics & Privacy (PEP) at George Mason University's Antonin Scalia Law School welcomes this opportunity to submit a Comment for the Federal Trade Commission's (FTC) Informational Injury Workshop. PEP's mission is to foster the use of rigorous economic analysis in public policy discussions surrounding the digital economy. The Informational Injury Workshop will explore an issue that is central to effective privacy and data security policy.

The principal point this Comment makes is that the FTC should be guided by empirical evidence when assessing whether certain informational practices harm consumers. Toward that end, this Comment makes four suggestions:

- Avoid basing privacy policy solely on stated preference, as it provides no information on tradeoffs.
- Rely on revealed preference data to the extent feasible, including engaging in research to better understand the role that asymmetric information and behavioral biases play in interpreting revealed preference data.
- Distinguish between harms due to (a) disparate treatment based on accurate information versus unwanted observation, and (b) human versus machine observation.
- Incorporate empirical evidence on the benefits of data sharing and the costs of privacy regulation.

It is important to note at the outset that because privacy is subjective and there is no ready market for privacy, it is highly unlikely that privacy tradeoffs will ever be measured with the precision of those for normally traded goods and

services. Nonetheless, it is important for the FTC to lay an empirical foundation for its actions in this area. In this regard, the FTC should apply lessons learned from the development of antitrust law to its privacy and data security policy. Over the past forty years antitrust enforcement has enjoyed wide bi-partisan legitimacy because it has evolved into a largely evidenced-based endeavor; legal presumptions reflect economic learning that identifies harmful practices, not enforcement officials' or judges' subjective views of what is harmful.[1] Indeed, the FTC was instrumental in laying much of the empirical groundwork for the legal analysis of restrictions on information flows.[2]

Although informational injuries necessarily involve subjective values, the FTC should not rely on subjective views when forming privacy and data security policy. A privacy and data security policy grounded in empirical evidence will enjoy legitimacy and durability because it is much more likely to benefit consumers than one left to policy makers' subjective preferences.[3]

1. Avoid Reliance on Stated Preferences

A key to assessing informational injury is determining how much people value the ability to control certain types of information that may be revealed as a result of a privacy or data security incident. It is relatively easy to quantify financial harm from identity theft in terms of fraudulent charges or time and hassle costs. It is more difficult to measure pure privacy harms—harms that arise when one loses control of personal information that does not result in direct monetary damages, but nonetheless compromises one's dignity or reduces one's scope of autonomy. For example, although web browsing histories, TV viewing habits, and geolocation data can be monetized, their collection does not result in direct monetary harm to consumers.[4]

Clearly, measuring the subjective values associated with informational injuries is difficult, but the FTC should avoid relying on stated preference—data from surveys or other instruments asking consumers if, or how intensely, they value something. Value is measured by the amount of one thing a person is willing to trade for another. For example, if a consumer is willing to pay $1 for a pound of apples and $2 for a pound of oranges, we can say that she would be willing to trade two pounds of apples for a pound of oranges. A survey asking a consumer if they like apples, or how much on a scale of 1-10 they like apples, tells us nothing about how much they value apples relative to oranges, or anything else for that matter. Only when we observe actual tradeoffs, can we truly measure value.

Stated preference results from surveys of consumer attitudes toward privacy tell us only that privacy has value.[5] They provide no information on how consumers value privacy relative to other things, such as time, convenience, or money. Yet this is the key question for policy makers who are trying to evaluate informational

injuries. For example, concepts like "privacy by design" and "data minimization" imply tradeoffs between privacy and other values. Similarly, opt-in consent requirements (*e.g.*, for certain types of data[6] or when firms merge datasets as part of an acquisition[7]) implicitly presume that a data practice is harmful to most people. The extent to which such policies actually benefit consumers cannot be known without understanding how consumers trade privacy for other things of value. Accordingly, as discussed in more detail below, the FTC should lay the empirical foundation for its privacy and data security policy to the fullest extent possible on revealed preference data that comes from measuring consumers' responses to changes in privacy conditions in the real world, or from experimental settings that sufficiently replicate the real world.

2. Reconcile Rational Actor and Behavioral Models of Revealed Preference Data

There is a growing literature that attempts to measure consumers' value of privacy, typically in an experimental setting. The results generally suggest that consumers are willing to trade personal information for small amounts of money.[8] Similarly, real-world tradeoffs suggest that consumers generally are comfortable with the typical information collection scenarios found in our digital life. For example, there are over 200 million Facebook users in the U.S.,[9] 150 million people use Snapchat daily,[10] health tracking apps and wearables continue to grow apace,[11] and 64 percent of U.S. households have an Amazon Prime account.[12] Further, consumer uptake of privacy protective tools has been meager.[13]

Despite this real-world behavior, survey data suggest that consumers place a high value on privacy.[14] This mismatch between revealed preference and stated preference has been dubbed "the privacy paradox," and has led some to suggest that revealed preference does not accurately reflect consumer demand for privacy. For example, there is a burgeoning literature examining privacy tradeoffs from a behavioral perspective. Several studies find some evidence of an "endowment" effect in privacy, where the value placed on revealing personal information fluctuates depending on whether one is buying or selling privacy.[15] Further, other studies find privacy to be context dependent, with consumer choices subject to change based on ordering and salience.[16] Together, this behavioral understanding of privacy choices casts doubt on the meaningfulness of revealed preference data.

Importantly, however, the gap between revealed and stated preferences does not necessarily imply observed choices are false measures of actual preferences. For example, as discussed above, there is no *a priori* reason to expect stated preferences and revealed preferences to match, as they measure different things. Further, although it is likely that privacy choices (*e.g.*, setting privacy preferences in an app) are made with less than full information—consumers do not comprehend (or even read) privacy policies, and the future impact of data sharing decisions made now is fraught with uncertainty—this fact alone is insufficient to discount

revealed preference. Choices are made every day without full information (*e.g.*, restaurants, plumbers, automobiles), but we do not discount the choices and prices formed in these markets. Moreover, the desire to become less than fully informed about privacy choices before making them can be entirely rational if the benefits (in terms of expected future informational injury) are less than the costs. Indeed, research suggests that even when information about exceedingly intrusive data practices is made highly salient, few consumers still bother to alter their willingness to share personal data.[17]

Another empirical regularity that is conducive both to rational choice and market failure arguments is that we see little evidence that firms compete on privacy. A central tenant in the economics of information is that parties with private positive information have an incentive to report it as long as they credibly can do so in a cost-effective manner. This result flows from the fact that parties rationally assume the worst from a failure to report because anyone with good information would willingly reveal it.[18] Thus, firms with strong privacy protections would find it in their interest to make clear and credible privacy promises.

There are two equally plausible explanations for why we tend not to observe this reality. First, we may not see competition over privacy because firms are unable to make credible commitments with respect to their collection and use of personal data, perhaps because data is durable beyond its initial collection and uncertainty surrounds potential future uses.[19] In this manner, the lack of competition on privacy could be evidence of a "lemons" equilibrium, with only low quality providers of privacy surviving. Similarly, behavioral economics suggests that consumers may be irrationally impatient or unable to fully appreciate the future consequences of choices they make now, so that even if consumers were to believe firms' privacy promises, they irrationally discount the potential of future informational injuries, rendering current promises valueless.[20] However, an equally plausible explanation for lack of competition over privacy is that consumers' willingness to pay for privacy is relatively small, so that competition over this dimension makes little economic sense.[21]

As the discussion above illustrates, empirical observations regarding consumers' value for privacy are subject to both rational choice and market failure interpretations. Importantly, however, the data have yet to speak to which interpretation is more accurate. Before discounting revealed preference data, the FTC should engage in research to understand more fully the role that asymmetric information and consumer biases play in forming observed behavior.[22] As part of this inquiry, the FTC should investigate the extent to which market mechanisms, such as reputation, work to ameliorate asymmetric information problems surrounding privacy. Further, the FTC additionally should consider the extent to which laboratory experiments can be generalized to the real world, where factors like experience and increased stakes can ameliorate or eliminate the effects of behavioral biases.[23]

3. BE PRECISE ABOUT THE SOURCE OF THE PRIVACY HARM

When identifying conduct that gives rise to informational injury, the FTC should precisely identify the source of harm because it is likely to be germane to the level of harm. First, the FTC should distinguish between harm caused solely by less favorable marketplace outcomes (*e.g.*, higher interest rates or prices, or lower wages) that arise when accurate information (*e.g.*, poor credit history, high willingness to pay, poor work habits) is discovered, and harm caused solely by the discovery or sharing of private information.[24] Only the latter scenario should be treated as an informational injury.[25]

Second, when identifying informational injury, who's watching matters. For example, surreptitious viewing of intimate activities by strangers[26] raises very different privacy concerns than the collection and analysis of aggregated de-identified television viewing habits[27] or shopping patterns[28] on a remote server. Research suggests that informational injury is more likely to result from proximate observation by individuals than distant observation by computers. For example, Wittes and Liu find evidence from Google Autocomplete that people often search for information on topics such as HIV and sexual identification, suggesting that the ability to search anonymously online for information about these topics provides an important privacy benefit and probably spurs increased information generation.[29] In follow-up work, Wittes and Kohse survey consumers and find a general preference for dealing with remote faceless entities over actual humans when it comes to certain sensitive purchases.[30]

4. INCORPORATE EVIDENCE ON THE BENEFITS FROM INFORMATION SHARING AND THE COSTS OF PRIVACY REGULATION

Lack of information can severely impact the abilities of markets to generate welfare for consumers. For example, markets with asymmetric information often suffer from adverse selection, which occurs when a firm's offerings attract a disproportionate amount of risky borrowers, unproductive workers, bad drivers, those with unhealthy lifestyles, and the like. In addition to adverse selection, markets characterized by asymmetric information are often subject to moral hazard, which concerns hidden actions—actions that impact the value of the relationship—that occur *after* the parties enter into a contract. A vast empirical literature documents adverse selection and moral hazard in a variety of markets, and both of these market failures impose serious costs on society by limiting the incentives of firms and consumers to participate in some markets.[31] To the extent that privacy regulation limits the ability to discover beneficial private information, it has the potential to exacerbate these problems, which will negatively impact consumers.[32]

Relatedly, there is an empirical literature that documents some of the direct consequences from privacy regulation that retards information flows. For example,

Kim and Wagman present empirical evidence that opt-in requirements for selling consumers' financial information reduces the marketability of these data, and hence firms' incentives to assure its accuracy.[33] They find that counties with opt-in requirements had lower loan-denial rates and concomitantly higher foreclosure rates. Similarly, Miller and Tucker find that increased consent requirements for sharing health care data reduces incentives to adopt health information technology (HIT). Their results show that the lower HIT adoption rates are associated with worse health outcomes, especially for minority babies.[34]

It is important to note that merely identifying costs associated with restrictions on data collection and use doesn't mean that the FTC's actions are necessarily welfare-reducing. To the contrary; these costs may be justified if the informational injuries are sufficiently high. But the FTC should take this highly germane body of knowledge into account—and potentially develop its own—when developing policy in this area.

CONCLUSION

Relying on empirical evidence to identify informational injuries will help assure that the FTC's actions more closely match consumer preferences. For this reason, laying an empirical foundation for its privacy and data security policy will provide legitimacy and durability to the FTC's work in this important area.

---

[1] *See*, *e.g.*, *Leegin Creative Leather Prods., Inc. v. PSKS, Inc.*, 551 U.S. 887 (2007) (describing evolution of antitrust treatment of vertical restraints in light of economic learning); *Cal. Dental Ass'n v. FTC*, 526 U.S. 756 (1999) (describing evolution of presumptions under rule of reason in context of professional advertising based on economic studies). The Horizontal Merger Guidelines, moreover, have been revised several times since their advent to reflect growing economic sophistication of merger analysis. *See* U.S. DEP'T OF JUSTICE AND FTC, HORIZONTAL MERGER GUIDELINES (Aug. 2010), at https://www.ftc.gov/sites/default/files/attachments/merger-review/100819hmg.pdf. On the benefits of antitrust law's adoption of the consumer welfare standard, *see generally* Joshua D. Wright & Douglas A. Ginsburg, *The Goals of Antitrust: Welfare Trumps Choice*, 81 FORDHAM L. REV. 2405, 2406 (2013).

[2] *See* Timothy J. Muris, California Dental Association v. Federal Trade Commission: *The Revenge of Footnote 17*, 8 S.CT. ECON. REV. 265(2000); William MacLeod *et al.*, *Three Rules and a Constitution*, 72 ANTITRUST L.J. 943 (2005).

[3] Policy making based on subjective standards is likely to cause uncertainty and to attract dissipative expenditures on rent seeking. *See* James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, The First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129 (2013).

[4] *See*, *e.g.*, *In re Jet Blue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299 (E.D.N.Y. 2005) (denying value of personal information as economic damages in a contract claim because an individual passenger's information does not have "any compensable value in the economy at large").

[5] *See*, *e.g.*, Pew Research Center, *Privacy and Information Sharing* (Jan. 14, 2016), *at* http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf.

[6] *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICY MAKERS at vii (Mar. 2012) (requiring "affirmative express consent" when companies collect "sensitive data for certain purposes").

[7] Letter from Jessica L Rich to Erin Egan & Anne Hoge (Apr. 10, 2014), *available at* https://www.ftc.gov/public-statements/2014/04/letter-jessica-l-rich-director-federal-trade-commission-bureau-consumer. The letter called for "affirmative express consent" for changes, and a

blog posting from a BCP staffer later clarified that merging parties needed to obtain "express opt-in consent" for material changes to data practices. *See Mergers and Privacy Policies* (Mar. 25, 2015), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2015/03/mergers-privacy-promises.

[8] For a full review of the results from various experiments designed to elicit consumers' value of privacy, *see* Alessandro Acquisti *et al*., *The Economics of Privacy*, 54 J. ECON. LIT. 442, 478 (2016). *See also* Lior Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers ?*, 45 J. LEG. STUD. 69 (2016) (among a panel of Gmail users who find privacy concerns with Gmail scanning, 85% of consumers would not pay anything to avoid scanning); James C. Cooper, *Anonymity, Autonomy, and the Collection of Personal Data: Measuring the Privacy Impact Google's 2012 Privacy Policy Change* (Apr. 2017) (finding a small and transient reduction in sensitive Google search after Google's 2012 privacy policy change), *at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2909148.

[9] *See Number of Facebook Users by Age in the U.S. as of January 2017, at* https://www.statista.com/statistics/398136/us-facebook-user-age-groups.

[10] Sarah Frier, *Snapchat Passes Twitter in Daily Usage*, Bloomberg News, June 2, 2016, *available at* https://www.bloomberg.com/news/articles/2016-06-02/snapchat-passes-twitter-in-daily-usage.

[11] Stephen McInerney, *Can You Diagnose Me Now? A Proposal to Modify the FDA's Regulation of Smartphone Mobile Health Applications with A Pre-Market Notification and Application Database Program*, 48 U. MICH. J.L. REFORM 1073 (2015) (*citing* Kevin Pho, *Health App Users Beware*, USA Today (Apr. 2, 2014), *available at* http://www.usatoday.com/story/opinion/2014/04/02/medical-app-fitness-health-fda-technology-column/7224837/). Andrew Meola, *Wearables and Mobile Health App Usage has Surged by 50% Since 2014*, BUSINESS INSIDER (Mar. 7, 2016) (health tracker use increased from 16% in 2014 to 33% in 2015), *at* http://www.businessinsider.com/fitbit-mobile-health-app-adoption-doubles-in-two-years-2016-3. *See also* Susannah Fox, *The Self-Tracking Data Explosion*, PEW RESEARCH CENTER (June 4, 2013), *available at* http://www.pewinternet.org/2013/06/04/the-self-tracking-data-explosion/.

[12] *See* Shep Hyken, *Sixty-Four Percent of U.S. Household Have Amazon Prime*, Forbes (Jun. 17, 2017), at https://www.forbes.com/sites/shephyken/2017/06/17/sixty-four-percent-of-u-s-households-have-amazon-prime/#647807654586.

[13] *See* Alessandro Acquisti *et al*., *The Economics of Privacy*, 54 J. ECON. LIT. 442, 476 (2016) (noting that that the adoption of privacy enhancing technologies has lagged substantially behind the use of information sharing technologies).

[14] *See*, *e.g*., *id*.; Pew Research Center, *Privacy and Information Sharing* (Jan. 14, 2016), *at* http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf.

[15] *See, e.g.,* Alessandro Acquisti *et al*., *What's Privacy Worth?,* 42 J. LEG. STUD. 249 (2013).

[16] *See*, *e.g*., Alessandro Acquisti *et al*., *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509 (2015).

[17] *See* Omri Ben-Shahar & Adam S. Chilton, *Simplification of Privacy Disclosures: An Experimental Test*, 45 J. LEG. STUD. 41 (2016). *See also* Jane R. Bambauer *et al*., *A Bad Education*, 2017 IL. L. REV. 109 (2017)(finding evidence that privacy disclosures are usually wasteful and may cause consumers to overreact).

[18] For example, consumers rationally would assume a used car had been in an accident if the car dealer refused to show a Carfax report. *See* Paul R. Milgrom, *Good News and Bad News: Representation Theorems and Applications*, 12 BELL J. ECON. 380 (1981).

[19] *See* Ginger Zhe Jin & Andrew Stivers, *Protecting Consumers in Privacy and Data Security: A Perspetive of Information Economics*, at 19-20 (2017), *at* https://www.ftc.gov/system/files/attachments/press-releases/ftc-announces-workshop-informational-injury/public_notice_injury_workshop.pdf.

[20] *Cf.* Xavier Gabaix & David Laibson, *Shrouded Attributes, Consumer Myopia, and Information Suppression in Competitive Markets*, 121 Q.J. ECON. 505 (2006). If firms compete by providing free content and services to take advantage of consumer myopia with respect to data sharing, the full price that consumers pay—in terms of shared data and free content and services—could be similar to that in a competitive market with full information, except that we share too much data and enjoy

too much free content. *See* Carl Shapiro, *Aftermarkets and Consumer Welfare: Making Sense of* Kodak, 63: ANTITRUST L.J. 483 (1995).

[21] More technically, the elasticity of demand with respect to enhanced privacy protection may be small.

[22] Some work has been to explore the relative explanatory power of rational choice and behavioral theories of privacy decision making. *See, e.g.,* Idris Adjerid *et al*., *A Query-Theory Perspective of Privacy Decision Making*, 45 J. LEG. STUD. 597 (2016).

[23] *See*, *e.g*., John A. List, *Does Market Experience Eliminate Market Anomalies: The Case of Exogenous Market Experience*, 101 AM. ECON. REV. 313 (2011); Steven D. Levitt & John A. List, *What Do Laboratory Experiments Measuring Social Preferences Reveal About the Real World?,* 21 J. ECON. PERSPECTIVES 153 (2007); John A. List, *Neoclassical Theory Versus Prospect Theory: Evidence from the Marketplace*, 72 ECONOMETRICA 615 (2004); John A. List, *Does Market Experience Eliminate Market Anomalies*?, 118 Q. J. ECON. 41 (2003). *See also* Jennifer Arlen & Stephan Tontrup, *Does the Endowment Effect Justify Legal Interventions? The Debiasing Effect of Institutions*, 44 J. LEG. STUD. 143 (2015) (showing that joint decision-making can eliminate the endowment effect, and suggesting that parties intentionally employ such institutions to debias).

[24] *See*, *e.g*., FEDERAL TRADE COMMISSION, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION, at 9-10 (2015), *at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf. (Cautioning against the use of big data resulting in "individuals being denied opportunities" and "higher-priced goods and services for lower income communities," as well as the possibility of "creating or reinforcing existing disparities").

[25] *See* James C. Cooper, *Separation Anxiety*, 20 VA. J.L. TECH. __ (*forthcoming* 2017); Lior Jacob Strahilevitz, *Privacy vs. Antidiscrimination*, 75 U. CHI. L. REV. 363, 376 (2008).

[26] *See DesignerWare, LLC* (Apr. 15, 2012), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3151/designerware-llc-matter.

[27] *See Vizio, Inc. and Vizio Inscape Svs., LLC* (Feb. 3, 2017), *at* https://www.ftc.gov/enforcement/cases-proceedings/162-3024/vizio-inc-vizio-inscape-services-llc.

[28] *See Nomi Tech., Inc.* (Sept. 3, 2015), *at* https://www.ftc.gov/enforcement/cases-proceedings/132-3251/nomi-technologies-inc-matter.

[29] Benjamin Wittes & Jodie Liu, *The Privacy Paradox: The Privacy Benefits of Privacy Threats*, CENTER FOR TECHNOLOGY INNOVATION AT BROOKINGS (May 2015), *at* http://www.brookings.edu/~/media/research/files/papers/2015/05/21-privacy-paradox-wittes-liu/wittes-and-liu_privacy-paradox_v10.pdf. Similar research finds that self-checkout in libraries has increased the number of LGBT books checked out by students, again suggesting that privacy concerns are reduced when human interaction is removed from the situation. *See* Stephanie Mathson & Jeffry Hancks, *Privacy Please? A Comparison Between Self-Checkout and Book Checkout Desk for LGBT and Other Books*, 4 J. ACCESS SERVS. 27, 28 (2007).

[30] Benjamin Wittes & Emma Kohse, T*he Privacy Paradox II: Measuring the Privacy Benefits of Privacy Threats*, CENTER FOR TECHNOLOGY INNOVATION AT BROOKINGS (Jan. 2017), *at* https://www.brookings.edu/wp-content/uploads/2017/01/privacy-paper.pdf.

[31] *See, e.g.,* Amy Finkelstein & James Poterba, *Testing for Asymmetric Information Using 'Unused Observables' in Insurance Markets: Evidence from the U.K. Annuity Market*, 81 J. RISK & INS. 709 (2014); Liran Einav *et al*. *The Impact of Credit Scoring on Consumer Lending*, 44 RAND J. ECON. 249 (2013) (subprime auto loan market); Sumit Agarwal *et al*., *The Importance of Adverse Selection in the Credit Card Market: Evidence from Randomized Trials of Credit Card Solicitations*, 42 J. MONEY, CREDIT, & BANKING 743 (2010);Dean Karlan & Jonathan Zinman, *Expanding Credit Access: Using Randomized Supply Decisions to Estimate the Impacts*, 23 REV. FIN. STUD. 433 (2010) (South African subprime lender); William Adams *et al*., *Liquidity Contraints and Imperfect Information in Subprime Lending*, 99 AM. ECON. REV. 49 (2009) (subprime auto loan market); Wendy Edelburg, *Risk-Based Pricing of Interest Rates for Consumer Loans,* 53 J. MONETARY ECON. 2283 (2006) (consumer loan market); Bev Dahlby, *Testing for Asymmetric Information in Canadian Automobile Insurance* (1992) (auto insurance); Lawrence M. Ausbel *Adverse Selection in the Credit Card Market*, (1999) (credit card markets); Daniel Altman, David M. Cutler & Richard Zeckhauser, *Adverse Selection and Adverse Retention*, 88 AM.ECON. REV. 122 (1998) (health insurance); Robery Puelz & Arthur Snow, *Evidence on*

Adverse Selection: Equilibrium Signaling and Cross-Subsidization n the Insurance Market, 102 J. POL. ECON. 236 (1994).

[32] *See* James C. Cooper, *Separation Anxiety*, 20 VA. J.L. TECH. __ (*forthcoming* 2017).

[33] Jin-Hyuk Kim & Liad Wagman, *Screening incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis*, 46 RAND J. Econ. 1 (2015).

[34] Amalia R. Miller & Catherine E. Tucker, *Can Health Care Information Technology Save Babies? ,* 119 J. POL. ECON. 289 (2011); Amalia R. Miller & Catherine E. Tucker, *Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records*, 55 MGM'T SCI. 1077 (2009).