TECHNOLOGY POLICY INSTITUTE
Studying the Global Information Economy

# Applications Want to be Free: Privacy Against Information

**March 2011**

Michael R. Hammock
Paul H. Rubin

# Applications Want to be Free: Privacy Against Information

**Michael R. Hammock**

**Paul H. Rubin**

*Forthcoming, Competition Policy International*

Michael R. Hammock is an Adjunct Professor of Economics at Middle Tennessee State University; Paul Rubin is the Samuel Candler Dobbs Professor of Economics at Emory University and a Senior Fellow at the Technology Policy Institute

**Abstract**

The debate over online privacy pays too little attention to the costs and benefits of the current systems of privacy protection and advertising-supported online applications. The costs of online privacy-related harm (such as identity theft) and of protective activities are small relative to the benefits from applications that are supported by online advertising, which depends on the collection of personal information. Advocates of increased privacy focus too much on increased privacy as a solution, and not enough on alternative forms of information security. Surveys show that consumers do not like targeted advertising, or the information collection that allows it, but this may be a form of rational irrationality. That is, it may not pay for consumers to understand the costs and benefits of reduced information use.

## I. Introduction

Both Europe[1] and the United States[2] are considering regulation that would increase consumer privacy and make the collection of personal information more difficult. Therefore it is worth examining whether these regulatory changes make economic sense.

Privacy advocates have pointed to identity theft as a reason to increase online privacy. They propose to make it illegal to collect information about consumers, by mandating opt-in as a default rule, or by other regulatory changes. These suggested policy changes seem not to be based on economic theory or on evidence beyond anecdotes. In this paper, we propose and defend the following assertions:

1. Proponents of increased privacy have not made a case based in economic theory or evidence, are vague regarding harm caused to consumers by lost privacy, and sometimes demonstrate fundamental misunderstandings of basic economics and the relevance of information security.

2. The total benefits of the current "opt-out" default rule (which requires consumers to take action to prevent the collection of their personal information) exceed the total costs, although it is not possible to tell if the marginal benefit of increased privacy equals the marginal costs. While some alternative approaches (such as a complete prohibition on information collection) to protecting personal information are undoubtedly inefficient, for some others (such as "quid pro quo") the data and theory do not allow us to make a prediction as to their efficiency. Nonetheless the fact that the collection of personal information has generated such a huge surplus of benefits in excess of costs suggests that we should be reluctant to impose fundamental changes.

3. Surveys of consumers suggest that consumers dislike both targeted advertising and the information collection that allows it. We contend that these surveys may have problems and that, even if the surveys are correct, consumers may be displaying "rational irrationality." Their opinions on privacy regulation may be no more reasonable than their opinions on international trade. If consumers do have valid privacy concerns, markets can and do respond to them.

[1] *See* A. Diana, *European Union to Update Privacy Laws*, INFORMATION WEEK (Nov. 4, 2010)*, available at* http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=228200181&cid=RSSfeed_IWK_All.

[2] *See* R. Singel, *FTC Backs 'Do Not Track' Browser Setting* (Dec. 1, 2010), WIRED, *available at* http://www.wired.com/epicenter/2010/12/ftc-do-not-track/.

## II. The Arguments of the Privacy Advocates

We have not been able to find any privacy advocates making sensible economic arguments for increased privacy. As far as we can tell, arguments for increased online privacy are based on rights (rather than efficiency) and anecdotes (rather than data). Walker[3] also complained of a lack of cost-benefit analysis in discussions of privacy rights, and Szoka & Thierer[4] point out that the harm privacy advocates worry about is conjectural or speculative, rather than concrete. Lenard & Rubin[5] provide an overview of how information collection and targeted advertising work, and argue that the benefits of more relevant ads are large, while the costs are small.

Hahn & Layne-Farrar[6] divided the participants in the online privacy debate into four positions. The distinctions between some of these categories are fuzzy; we simplify them into two: The "Increased Privacy" camp and the "Status Quo" camp. The Increased Privacy camp wants to make opt-in the default rule and wants to limit the use of data to the task for which it was originally collected. This would mean that consumer information cannot be collected without the consumer explicitly choosing to allow it. Also data could not be used for any task other than the task immediately at hand, and could not be resold or reused without explicit permission from the person described by that personal information. We will call the other side of this argument the "Status Quo" camp. The Status Quo camp argues that the benefits of information collection under the current system exceed the costs, and that market responses will take care of any problems.

When members of the Increased Privacy camp argue for restrictions on the re-use of personal information, or for a switch to "opt-in" as a default rule, their arguments are generally based on an implicit right on the part of consumers not to have any information collected about them without their knowledge and consent. This is reflected in the European view of privacy regulation as well. As *The Economist* put it, "European regulations are inspired by the conviction that data privacy is a fundamental human right and that individuals should be in control of how their data are used." Regarding U.S. regulation, when Marc Rotenberg of the Electronic Privacy Information Center ("EPIC") testified on December 2, 2010 to the Committee on Energy and Commerce, his argument seemed to be that firms collect a *lot* of information, and consumers don't know this.[7] In 2008 he argued that "the detailed profiling of Internet users violates the

---

[3] *See* K. Walker, *The Costs of Privacy*, 25 HARV. J.L. & PUB. POL'Y 87, 89 (2001).

[4] *See* B. Szoka & A. Thierer, *Targeted Online Advertising: What's the Harm & Where Are We Heading?*, 16 PROGRESS ON POINT 1, 3 (June 2009). *Available at* http://pff.org/issues-pubs/pops/2009/pop16.2targetonlinead.pdf.

[5] *See* T. Lenard & P. Rubin, *In Defense of Data: Information and the Costs of Privacy*, 2 POL'Y & INTERNET 149-183 (2010).

[6] *See* R. Hahn & A. Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, AEI-Brookings Joint Center Working Paper No. 01-14, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=292649.

[7] *See* M. Rotenberg, *Statement for the Record of The Electronic Privacy Information Center (EPIC)*, Hearing on "Do Not Track Legislation: Is Now the Right Time?" *available at* http://epic.org/privacy/consumer/EPIC_Do_Not_Track_Statement_120910.pdf.

fundamental rights of individuals, diminishes the accountability of large corporations, and threatens the operation of democratic governments."[8] There is no discussion of benefits and costs—are consumers genuinely being harmed? Do they benefit in any way?

At a Federal Trade Commission ("FTC") roundtable discussion, a panelist from the Privacy Rights Clearinghouse shared a few examples of horrifying cases in which information collected online was used for criminal means, including stalking and rape.[9] As terrible as these cases may be, however, anecdotes are less persuasive than data. Basing policy on anecdotes will result in a bias toward regulating; millions of people uneventfully going about their business online do not make for interesting counter-anecdotes. Furthermore, the data suggest that online identity fraud is rare. We will return to the costs of identity fraud shortly.

Gellman[10] argued that consumers have revealed their preference for privacy through their willingness to pay for it, in the form of unlisted numbers, caller ID, spam filters, and sorting through junk mail. Some of these costs are dated now, with do-not-call lists to stop telemarketers, the ubiquity of cell phones (with caller ID built in), and very effective automatic spam filters for free email accounts such as Gmail—technology and policy have already caught up with many of these problems. Gellman then adds up the costs of pursuing extreme privacy—anonymization service, identity theft protection, reports from all three credit bureaus, credit monitoring, and so on. The total annual costs for a single consumer are nearly $300, but what are we to make of this? The costs of pursuing such extreme privacy are very high, but this is like arguing that the roads are not safe enough by citing the high cost of an armored car. Consumers who do not incur these costs face an extremely small chance of identity theft occurring, as we discuss later. Consumers are wise to forego all these expenses unless they put an extremely high value on safety.

Privacy advocates are not always so explicit about the costs of lost privacy. In the Center for Digital Democracy's comments submitted to the FTC regarding privacy regulation,[11],the word "cost" appears six times, yet in none of those cases are the costs of lost privacy described or explained. Rather, it is asserted that researchers who attempt to determine the costs and benefits of behavioral advertising (which depends on the collection of personal information) "misunderstand" the costs for consumers—without explaining how they have erred. The authors

[8] *See* M. Rotenberg, *Data Protection and Search Engines on the Internet: Google-Doubleclick and other case Studies*, *available at* http://epic.org/privacy/ftc/google/EPIC_LIBE_Submission.pdf.

[9] *See* B. Givens, *Online Information Brokers: Where is the Balance*, presentation at Computers Freedom and Privacy Conference, San Jose, CA, San Jose State University (Jun. 15, 2010), *available at* http://www.privacyrights.org/node/3438.

[10] R. Gellman, *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete* (2002), *available at* http://epic.org/reports/dmfprivacy.html.

[11] *See* J. Chester & E. Mierzwinski, *Comments of The Center for Digital Democracy and U.S. PIRG before the Federal Trade Commission*, (Feb. 18, 2011), *available at* http://www.democraticmedia.org/files/2011-02-17-FTC-Comments.pdf.

seem to suggest that the fact that targeted ads can now be targeted accurately and delivered very quickly is itself cause for action.

What of the costs to consumers of information breaches? In 2009 Mark Rotenberg of EPIC testified to the House Commerce Committee[12] regarding legislation that would regulate notification of data security breaches. Rather than focusing on information security, however, Professor Rotenberg also talked about making it more difficult for corporations to collect and use personal information in the first place. It is true that preventing corporations from collecting personal information (or preventing it from being in their interests to collect personal information) would reduce the damage from data security breaches. This is like arguing that doing away with privately owned cars would be a means to reduce automobile accidents—the cure would be worse than the disease. Whether data security should be regulated differently is a good question, and one that EPIC has addressed in the past (as with the case of TJX).[13]

A growing body of economic literature examines information security. Anderson & Moore[14] provide a good overview of the fundamental economic issues. The core problem is that people with the responsibility to protect data may not face the full costs of failing to do so—there may be a negative externality, resulting in inefficiently lax security. It is not clear that this is the case; Lenard and Rubin[15] argue that the costs of breach fall almost entirely on firms that store information. This could mean that investment in security is slightly suboptimal, unless the externality is inframarginal, in which case it need not be suboptimal at all. Even if there is a market failure, it seems more reasonable to address this market failure than to shrink the market for personal information. To put it succinctly, if members of the Increased Privacy camp are concerned about data breach, the lowest cost way to address this is to improve the incentives to provide security rather than to limit the collection and use of information. How could this be accomplished?

There are several possible regulatory tools available to improve information security. For example, altered breach disclosure laws could allow both consumers and firms to be both more proactive as well as react more quickly, although Romanosky et al.[16] find that state-level variation in breach disclosure laws have only a small effect on identity theft. Anderson et al.[17]

---

[12] *See* M. Rotenberg, *Testimony and Statement for the Record of Marc Rotenberg, Executive Director, EPIC*, Legislative Hearing on "H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act," (May 5, 2009), *available at* http://epic.org/linkedfiles/rotenberg_house_ctcp2221_1319.pdf.

[13] *See* M. Rotenberg and J Verdi, *Comments of the Electronic Privacy Information Center*, (Apr. 28, 2008), *available at* http://epic.org/privacy/idtheft/042808_ftc.pdf.

[14] *See* R. Anderson & R. Moore, *The Economics of Information Security*, 314 SCIENCE 610, 610-613 (2006).

[15] T. Lenard & P. Rubin, *Much Ado About Notification*, 29 REGULATION 44, 44-50, (Spring 2006).

[16] *See* S. Romanosky, R. Telang, & A. Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?* (Nov. 9 2010) SSRN Working Paper No. 1268926, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1268926.

[17] *See* R. Anderson, R. Boehme, R. Clayton, and T. Moore, *Security Economics and European Policy*, MANAGING INFORMATION RISK AND ECONOMICS OF SECURITY (M. Johnson, ed.) (Springer 2009).

suggest mandated disclosure of vulnerabilities. Firms suffering breach could be assigned liability for all damages caused, leading them to internalize the security externality.[18] In the case of TJX, EPIC suggested the assignment of $10 million in additional civil penalties, but it is not clear why liability for damages caused would not be the efficient remedy.[19] Large breaches are hard to hide, so it is not as though high damages were necessary to maintain efficient expectation damages.

There are a variety of other options available as well, but our purpose is not to catalog them or to assess them, but to point out that if information security is the problem, the debate should center on the means to address this problem. Privacy concerns should not distract from the debate over what regulatory tools to use, if any, to improve information security, and reduce the costs of breach. Privacy advocates have missed or ignored this point.

Members of the Increased Privacy movement further neglect the *benefits* created by the current system of information collection, which supports personal ads, which in turn support free online applications. At the heart of economics is the idea that *incentives matter*, and if the money that funds online applications is reduced, or if the returns from developing these applications are reduced, fewer online applications will be provided. Privacy advocates do not seem to see the connection, and when confronted with it, deny it. For example, when interviewed by ABC News, privacy and security advocate Christopher Soghoian asserted "The web was free for the last 15 years before they were tracking people, and it will continue to be free after they track people."[20] The web that was free in the 1990s was very different from the web today, with its wide variety of online applications. Advocates act as if the question is "either/or" (will there be an internet or not?) when it is actually "How much?" (what sort of functions will the internet perform?). Economists should not assume that everyone understands supply curves slope upward. Again, we will return to the scope of the benefits of these applications shortly.

There has also been concern about sites like Spokeo.com.[21] Spokeo collects personal information from a variety of online sources, including social networking sites. It purports to have information on income, wealth, property value, number and age of people in the household, addresses, phone numbers, email addresses, and other personal information. For users to access

---

[18] For discussion of liability for security failure, *see* Anderson et al. *Supra* note 14, and House of Lords, *Personal Internet Security,* 39 (Aug. 2007), *available at* *http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf* ; and for a theoretical analysis, *see* H. Ogut, N Menon, & S. Raghunathan, *Cyber Insurance and IT Security Investment: Impact of Interdependent Risk*, 4th Workshop on the Economics of Information Security (June 2 to 3, 2005).

[19] *See supra* note 12.

[20] *See* S. Kessler, *Online Behavior Tracking and Privacy: 7 Worst Case Scenarios*, ABC NEWS (Nov. 6, 2010), *available at* http://abcnews.go.com/Technology/online-behavior-tracking-privacy-worst-case-scenarios/story?id=12068346&page=4.

[21] *See* R. McRill, *Spokeo Privacy Violation Warnings Spread by Facebook Users*, Associated Content from Yahoo (Jan. 2, 2011), *available at* http://www.associatedcontent.com/article/6175590/spokeo_privacy_violation_warnings_spread.html.

any information beyond the basics requires paying a fee. This causes concern because of fears of identity fraud, and perhaps a general "creepiness" from finding out that other people can obtain information about oneself. It is important to keep in mind, however, that it has long been possible to pay someone to find information about other people. This is not a new phenomenon; it is an old phenomenon that has moved to a new medium.. Finally, we should keep in mind that this information contained online was either put there willingly by consumers themselves, or it is public record (such as property records).

What can we say about the balance between the Privacy Advocates and the Status Quo proponents? What are the costs and benefits to consumers of lost online privacy? Consumers are clearly harmed by online identity fraud, which occurs when someone is able to impersonate the consumer, gaining access to his or her accounts. In addition to creating debts for the consumer, the consumer's credit record may be harmed, and resolving these problems may create additional expense. In the next section, we discuss the size of these costs, as well as the benefits of the current system.

## III. Opt-In, Opt-Out, and the Costs and Benefits of Targeted Advertisements

The current system of privacy protection in the United States is "opt-out." Consumers must take actions to prevent personal information from being collected, by: running software or establishing non-default settings that routinely remove cookies; explicitly telling websites not to use their data (when such an option is available); refraining from putting personal information on sites like Facebook; and taking whatever other measures they can. This is a default rule. That is, by default, consumers are assumed to have given permission to collect personal information; they must intentionally opt out to deny permission.

Advocates of increased privacy argue that an "opt-in" default rule would be superior. Consumers would have to give explicit permission any time their information was collected, sold, used, or reused. Groups such as the Consumer Electronics Association, Consumer Watchdog,[22] Center for Democracy and Technology,[23]and the Center for Digital Democracy and U.S. Public Research Interest Groups[24] favor opt-in as the default rule. The 2009 changes to the European Union's E-Privacy Directive[25] require that cookies should only be stored on a user's computer if

[22] *See* M Shiels, *Personal Data Could Become a Commodity,* BBC MOBILE (Oct. 19, 2010), *available at* http://www.bbc.co.uk/news/technology-11571513.

[23] *See* Center for Democracy and Technology, *Online Behavioral Advertising: Industry's Current Self-Regulatory Framework is Necessary, But Still Insufficient On Its Own To Protect Consumers* (Dec 9, 2009), *available at* http://www.cdt.org/policy/online-behavioral-advertising-industry%E2%80%99s-current-self-regulatory-framework-necessary-still-in,

[24] *See* J. Chester & E. Mierzwinski, *supra* note 10.

[25] *See* Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, Official Journal of the European Union, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF.

the user consents, and Europe's privacy regulation prior to that was generally more restrictive of the collection and use of personal information than that in the United States.

If transactions costs were zero, the decision as to which default rule to apply would not matter; Coasean bargaining[26] would put the personal information in the hands of firms if the firms valued the data more highly than consumers valued their privacy. The transactions costs are not zero, however. Under both opt-in and opt-out consumers must take the time to become informed, make a decision, and implement it across all their computers and software. If the transactions costs are too high, consumers and firms will not be able to bargain to the efficient outcome. It is therefore important that the rights be assigned efficiently by law and regulation. What, then, is the efficient default rule: opt-out, or opt-in? Do the benefits of information collection under the current opt-out default rule exceed the costs? What would happen under opt-in?

Bouckaert & Degryse[27] develop a theoretical model that suggests that opt-out is the efficient default rule unless the costs of opt-in are zero (in which case opt-out and opt-in are equally efficient). This is because fewer consumers buy from the socially optimal supplier under opt-in, and they pay higher prices as a result.

There are several empirical studies of opt-in and opt-out. Staten and Cate (2003)[28] conducted a case study of MBNA (a bank subsequently bought by Bank of America), finding that opt-in would make it more difficult to match credit offers to customers, and make it more difficult for MBNA to fight fraud. The authors did not examine the effect on consumers, but two outcomes are likely: consumers could receive more credit offers of a less targeted (and therefore less useful and more annoying) nature, and fewer consumers would get the credit appropriate for their personal needs.

Johnson & Goldstein[29] found that there is a 16 percent increase in organ donations in countries in which opt-out (that is, one must take action to prevent oneself from being an organ donor) is the default rule, relative to countries in which opt-in (one must take action to become an organ donor) is the default rule. This is despite the fact that opting in or opting out is often no more costly than checking a box on a driver's license application. The simple switch of the default rule can be more effective than campaigns to encourage people to opt into donating. Thaler & Sunstein[30] found a similar result for 401 (k) plans: Enrollment increases dramatically when moving from opt-in to opt-out. Clearly default rules matter; people may not opt-in simply to

[26] R. Coase, *The Problem of Social Cost,* 3 J.L. & ECON. 1-44 (1960).

[27] *See* J. Bouckaert & H. Degryse, *Opt In Versus Opt Out: A Free-entry Analysis of Privacy Policies*, CESifo Working Paper Series No. 1831, CentER Discussion Paper No. 2006-96 (Sep. 2006), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=939511.

[28] M. Staten & F. Cate, *The Impact of Opt-in Privacy Rules On Retail Credit Markets: A Case Study of MBNA* 52 DUKE L. J. 745 (2003) *available at* http://www.law.duke.edu/shell/cite.pl?52+Duke+L.+J.+745.

[29] E. Johnson & D. Goldstein, *Do defaults save lives?,* 302 SCIENCE 1338 (2003).

[30] R. THALER & C. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008).

avoid the costs of having to think about it. In the case of organ donation, this means people avoid thinking about death. With online privacy, it means that consumers avoid thinking about the costs and benefits of allowing personal information to be collected and, perhaps more importantly, they avoid thinking about the very small chance that their data might in some way be abused. The possibility that poorly chosen default rules can allow consumers to *avoid* making careful decisions does not encourage us to believe that the outcome of opt-in will be efficient.

Given this "sticking" of default rules, it is important to choose the right one. If the value of privacy is greater than the value of targeted advertising and the online applications that targeted advertising funds, then opt-in is the efficient default rule. If the value of targeted advertising and online applications is greater than the value of privacy, then opt-out is the efficient default rule. There are several empirical studies that can help determine which is the case.

First, what are the measureable, concrete costs to consumers of online breaches[31] and identity fraud? The 2010 Javelin Identity Fraud Survey Report[32] found that damage from identity fraud (both online and offline) was $54 billion in 2009. For the sake of comparison, a 2003 FTC report[33] found that the total costs from identity fraud were $52.6 billion, of which $5 billion was losses to consumers, and $47.6 billion was losses to business. A 2006 report[34] found that the losses were only $15.6 billion total, but survey methods changed, and costs were not broken down by incidence.

We will assume the high cost estimate of $54 billion from the 2010 Javelin report. The 2010 Javelin report preview does not provide the fraction of cases in which personal information was obtained online, but the 2008 report[35] says that 12 percent of identity fraud in 2008 was accomplished by information obtained online. This number comes from victims who knew how their personal information was obtained; it may be the case that victims who do not know how their information was obtained were more or less likely to have had it taken online, but we will use the 12% number as it is the best we have. This means that around $6.48 billion in damage from online identity fraud was inflicted in 2009. Compared to the costs of fraud overall, the size of the online economy,[36] or the overall economy, this is not an enormous cost. With around 220

[31] Note that here we are treating security problems as privacy problems, for the sake of argument.

[32] Javelin Strategy and Research, *The 2010 Identity Fraud Survey Report* (2010). There is a fee for the full report, but a summary is *available at* https://www.javelinstrategy.com/news/831/92/Javelin-Study-Finds-Identity-Fraud-Reached-New-High-in-2009-but-Consumers-are-Fighting-Back/d,pressRoomDetail.

[33] Synovate, *Federal Trade Commission – Identity Theft Survey Report* (2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf .

[34] Synovate, *Federal Trade Commission – 2006 Identity Theft Survey Report* (2006), *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

[35] Javelin Strategy and Research, *The 2008 Identity Fraud Survey Report* (2010). The consumer version is *available at* https://www.javelinstrategy.com/uploads/files/803.R_2008_Identity_Fraud_Survey_Report_Consumer_Version.pdf.

[36] The Census Bureau estimates business-to-consumer shipments were around $288 billion in 2008. *See* U.S. Census Bureau, *E-Stats* (May 27 2010) *available at* http://www.census.gov/econ/estats/2008/2008reportfinal.pdf.

million Americans online,[37] that works out to about $29.44 in online identity fraud damage per user.

A 2010 IAB Europe study[38] found that the value to consumers of preventing online ad disturbance (defined as the risk of abusing personal information and the annoyance of advertisement intrusion) is around EUR 20 billion, or around $28 billion. It appears that this number is the sum of the value of protection in the United States and Europe, and separate numbers are not provided. For sake of argument, and to be conservative, let us assume that the entire $28 billion applies to the United States alone—that is, for U.S. consumers, the value of avoiding the costs of having their information collected is around $28 billion.

What are the benefits to consumers of advertising-funded applications online? The IAB report finds that, after netting out the costs of disturbances and paid services (including internet access), consumer surplus from web services is around $100 billion for the United States and Europe combined. More than half of this consumer surplus comes from free services. Again, they do not provide separate consumer surplus estimates for Europe and the United States,[39] although they do show that there are differences across countries in the fraction of consumer surplus generated by different online services. The report also projects that consumer surplus will continue to grow at around 13 percent per year, based on current trends.

This shows that the consumer surplus of the current regimes in the United States and Europe have enormous benefits in excess of costs, but what of the difference between U.S. and European privacy policies? Goldfarb & Tucker[40] find that European privacy regulation reduces the effectiveness of targeted online advertising, resulting in ads that are less relevant to consumers and generate less revenue. This reduced effectiveness may also result in more ads being served; in order to raise consumer purchase intent by the same amount as an ad prior to the tightening of E.U. privacy regulation, an advertiser must buy 2.85 times more advertising. Goldfarb & Tucker estimate that by changing the privacy regulations in the United States, revenue from online advertising could fall from $8 billion to $2.8 billion. If ads become less effective, and generate less revenue, then we should expect less funding for ad-supported applications, and a loss of value to consumers.

---

[37] *See* Internet World Stats, *Internet Usage and Population in North America* (last accessed Feb. 26 2011) *available at* http://www.internetworldstats.com/stats14.htm#north.

[38] *See* McKinsey and Company for IAB Europe, *Consumers Driving the Digital Uptake: The Economic Value of Online Advertising-based services for Consumers* (Sep. 2010) *available at* http://www.iab.net/media/file/White-Paper-Consumers-driving-the-digital-uptake_FINAL.PDF.

[39] A 2009 IAB report found a wide range of estimates of the value of the ad-supported internet in the U.S., depending on how one calculated its value, and in some cases it is unclear whether the authors use "ad-supported internet" to refer to the entire internet, or just part of it. *See* J. Deighton, J. Quelch, and Hamilton Consultants, Inc. for IAB, *Economic Value of the Advertising-Supported Internet Ecosystem* (June 10, 2009), *available at* http://www.iab.net/media/file/Economic-Value-Report.pdf .

[40] A. Goldfarb, and & C. Tucker, "Privacy Regulation and Online Advertising", 57 Management Science 57 (2011).

We draw several conclusions from this body of research. First, a switch to opt-in as a default rule would likely result in a dramatic reduction in the amount of information collected, and this would cause targeted ads to be less valuable. Second, the costs of identity fraud committed online—a concrete, measureable privacy concern—appear to be relatively small. Third, the benefits to consumers of online services such as search, free email, Google docs, mapping services, Facebook, search, and so on, are enormous. Decreased advertising revenue would reduce the incentive to provide these online services or reduce their quality.

There is an important caveat, however. Some of these online applications might persist without targeted advertising. We know that the total benefits of the current system exceed the total costs, but we cannot be sure that the marginal benefits equal the marginal cost. Currently Europe's privacy regulations, though stricter than in the United States, are not *radically* stricter. We do not have the data to tell us whether a marginal change toward slightly more privacy creates benefits greater than costs. Radical changes are more likely to reduce the benefits of free online applications (supported by targeted advertising). Still, we cannot be sure what sort of equilibrium would emerge if a radically different system, under which consumers were paid for their personal information (perhaps with access to online applications), were implemented. However, since the current system evolved in a free market situation, it is unlikely that any radically different alternative would be preferable.

## IV. Consumer Views of Privacy and Targeted Advertisements

Surveys often show that consumers do not want advertisement targeted toward them, and that they do not feel their loss of privacy is worth any of the benefits provided. A 2008 Harris Interactive/Westin Survey[41] asked survey respondents how comfortable they were with sites like Google using personal information to tailor advertisements to their interests, using the revenue to provide free services like email. 59 percent of consumers were not comfortable with this. When asked if they would be comfortable with targeted ads if a list of privacy protections were implemented, 55 percent said they would be comfortable.

A December, 2010 Gallup Poll[42] of U.S. internet users found similar results: 67 percent opposed targeted ads based on behavioral tracking, and 61 percent did not believe that the support for free online services made possible by targeted ads justified their use. 61 percent of users reported having seen such ads, and 90 percent of them stated that they paid little or no attention to them.

[41] *See* A. Westin, *How Online Users Feel About Behavioral Marketing and How Adoption of Privacy and Security Policies Could Affect Their Feelings* (Mar. 27 2008) *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/Westin.pdf.

[42] *See* Gallup, *U.S. Internet Users Ready to Limit Online Tracking for Ads* (Dec. 21 2010), *available at* http://www.gallup.com/poll/145337/Internet-Users-Ready-Limit-Online-Tracking-Ads.aspx.

Strangely, a plurality of users said they would prefer to allow advertisers of their choice to target them, as opposed to allowing all advertisers or no advertisers.

Turow et al.[43] conducted a survey and found that 66 percent of respondents did not want websites to show them ads tailored to their interests, although 47 percent would like sites to give them discounts tailored to their interests. Consumers were more accepting of ads that were targeted based on the site they were currently visiting, but not of ads based on sites they had previously visited. Younger respondents were more accepting of targeted ads, but still had 55 percent opposition. Survey respondents were also strongly in favor of laws increasing their online privacy. They did not understand current regulations, however, believing that the law provided more privacy than it actually does. For example, 54 percent believed incorrectly that websites with privacy policies must delete one's personal information if one asks them to do so.

Spiekerman et al. (2005)[44] surveyed consumers in 2000 about their privacy preferences and their behavior, using an online shopping experiment. They found that while most consumers expressed privacy concerns, their behavior did not "live up to their self-reported privacy preferences." They provided personal information for no clear reason—even some users categorized as privacy fundamentalists. Aquisti & Grossklags[45] conducted a survey and found that 87.5 percent of consumers who said they were highly concerned about the collection of personally identifying information (like a name or address) signed up for a shopping loyalty card—which required using their real personal information. Of those respondents concerned about credit card and identity fraud, only 25.9 percent used credit alert features. Of those who said that consumers should use technology to protect their privacy, 62.5 percent said they had never used encryption[46] and half never used shredders to destroy documents containing personal information. Clearly there is a disconnect between what consumers say and do.

McDonald & Cranor[47] conducted in-depth interviews with 14 subjects regarding internet advertising and privacy. They found that the consumers disagreed over what constitutes an advertisement, and sometimes do not recognize ads for what they are. They do not understand exactly what cookies are, how they work, how information about their browsing behavior is collected, and only three of them understood that cookies were related to targeted

---

[43] J. Turow, J. King, C. Hoofnagle, A. Bleakley, & M. Hennessy, *Americans Reject Tailored Advertising and Three Activities that Enable It,* SSRN Working paper (Sep. 29, 2009) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[44] *See* S. Spoiekermann, J. Grossklags, & B. Berendt, *E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior,* Proceedings of the 3rd ACM Conference On Electronic Commerce 38 (2001) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=761107.

[45] A. Aquisti & J. Grossklags, *Privacy and Rationality: A Survey*, PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS -DISCIPLINARY CONVERSATION, 15-29 (K. Strandburg and D. Raicu, eds) (2006).

[46] This is hard to believe. Anyone who has shopped online has surely used https, which relies on encryption. They probably did not understand what encryption meant.

[47] *See* A. McDonald & L. Cranor, *An Empirical Study of How People Perceive Online Behavioral Advertising*, CyLab Technical Report 09-015, *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09015.pdf.

advertisements. Some subjects preferred ads that were more relevant, while others were concerned about the privacy implications of targeted ads. Regarding specific harms of lost privacy, users identified the loss of privacy itself as the primary harm, with one user suggesting concern over privacy would cause users to withdraw from online life.

Members of the Increased Privacy movement quite reasonably cite these robust survey results as an argument for stricter regulation. We believe that this position is incorrect, however. Consumer opinion, while certainly important for policymakers (particularly those looking for votes), is not necessarily a guide to efficient policy. As Bryan Caplan[48] has shown, consumers-as-voters are often *rationally irrational*; they often support policies that make little economic sense, such as agricultural subsidies, and disagree with experts (economists, toxicologists, climatologists, etc.) despite lacking the information on which to base an informed opinion.

A better phrase to describe this phenomenon would be *rational systematic bias.*[49] Consider free trade, for example. Most economists favor free trade, and believe that the benefits of reducing trade barriers outweigh the costs. They base this on hundreds of years of theory and evidence. If poorly informed laypeople were *rationally ignorant*, then we would expect some of them to think that free trade is less beneficial than it actually is, while an equal number would think that free trade is *more* beneficial than it actually is. This is not what we observe, however. Voters' views on trade are *systematically* biased; they err consistently on the side of believing that trade is *bad.* Averaging the opinions of all the voters does not result in something close to the truth; it results in an average opinion that is biased away from the truth (with truth, in Caplan's model, being represented by the averaged opinions of experts).

This is rational, Caplan argues, because voters do not face the cost of holding incorrect beliefs. Their one vote will not change policy, and when it comes to policy issues, holding unpopular (but more correct) opinions will not benefit them. Voters therefore hold (incorrect) opinions as a result of culture or the early evolutionary environment.[50] Consumers making shopping decisions are faced with a very different situation: they face all the costs and benefits of their decisions. We expect them to be better informed, because holding incorrect beliefs is costly. If a product is risky, consumers take action to protect themselves, such as paying a home inspector to make sure the house they are looking at has no hidden dangers, or hiring a mechanic to make sure the car they are about to buy is fully functional. Consumers collect product information and reviews to help make decisions while shopping online. They do these things because the costs of poor decisions, and the benefits of good decisions, fall entirely on them.

[48] B. CAPLAN, THE MYTH OF THE RATIONAL VOTER (2007).

[49] Caplan says that he chose the term *rational irrationality* to "emphasize both its kinship with and divergence from, rational ignorance."

[50] P. RUBIN, DARWINIAN POLITICS (2002).

How, then, does this relate to online privacy? It is natural for consumers to be uncomfortable with the idea that someone is collecting information about them. We are not used to the idea of a machine collecting data, which is then fed through algorithms and used, impersonally, to send us advertisements. Consumers' reaction is concern, and they support policy changes to increase their privacy. In two books,[51] Clifford Nass has carefully shown that people fundamentally misunderstand the nature of intelligent machines. For example, people are more likely to rate a computer's performance as good if they are asked while working on that specific computer than if they are asked while working on a different computer.[52] That is, people are "polite" to computers. We hypothesize that the same principle applies to tracking by websites: people cannot conceive of being tracked by a machine, and instead respond as if some human knows what they are doing. Our brains did not evolve to understand the nature of relatively intelligent machines, and we treat them as if they were people.

This instinct does not necessarily make for good policy, however. The available data on costs and benefits suggest that the risks of having data on one's browsing habits collected are low; the damage from identity fraud is relatively small. It is hard to believe that consumers recognize the extent to which free online sites and applications are funded by advertising. There is a free rider problem here, as well. When asked individually, a consumer might prefer not to be tracked, and thereby obtain a free ride off of the creation of online applications funded by advertising targeted at *other* consumers.

Public opposition to the online collection of personal information is not *per se* evidence that consumers are being harmed and need regulation to protect them, just as voter support for agricultural subsidies is not evidence that we would run out of food without such subsidies. To put it another way, surveys have shown that consumers do not understand how cookies and online information collection techniques work. They have also shown that consumers see information collection as dangerous. Why do privacy advocates consider the second result to be evidence of consumer wisdom, given the first result?[53] Would it not be more reasonable to conclude that consumers' views of information collection are of dubious value?[54]

This raises another point. Privacy advocates often claim that if consumers fully understood how much information was collected and how it was being used, then they would be much more concerned. But the very ignorance of consumers is itself evidence of the lack of harm.

---

[51] *See* C. NASS & C. YEN, THE MAN WHO LIED TO HIS LAPTOP: WHAT MACHINES TEACH US ABOUT HUMAN RELATIONSHIPS (2010), and B. REEVES & C. NASS, THE MEDIA EQUATION: HOW PEOPLE TREAT COMPUTERS, TELEVISION, AND NEW MEDIA LIKE REAL PEOPLE AND PLACES (1996, 2002).

[52] The Media Equation, chapter 2, *supra note 48*.

[53] On the other hand, consumer ignorance of how online privacy works could be simple rational ignorance—the benefits of being informed are nearly zero, while the costs of becoming informed can be high.

[54] Note that we are not arguing that consumers cannot judge whether they are annoyed by targeted advertisements, or any sort of advertisements; clearly that is the sort of subjective consumer judgment that economists must respect.

Consumers learn about things that are actually harmful, such as tainted foods or dangerous products. The fact that consumers do not bother to learn about data collection is itself evidence that this process is not harmful. Privacy advocates have for many years been warning consumers about this danger, but consumers have blithely been ignoring these warnings, because they have not observed or suffered any real harm.

If consumers desire greater online privacy, entrepreneurs should find it rewarding to provide protective services. In fact, there are a variety of tools available to consumers right now. Based on our own casual experience, we have noted that Google Chrome has an incognito mode, which does not either record webpages or files downloaded in browsing or maintain download histories, and deletes cookies after the window is closed. Firefox has a similar Private Browsing mode, and Internet Explorer 8 has an InPrivate Browsing mode. The Dolphin browser for Android devices has an option to delete cookies automatically after each session.

These modes do not prevent all tracking, but they can drastically reduce the amount of information collected, at a very low cost (an occasional extra click, at most). Future versions of Firefox and Internet Explorer will support the Do Not Track flag, although this does not work unless websites support it, and whether they will do so remains to be seen. People can easily add a free Gmail or Yahoo email account and use this for some online activities where an email address is required, in order to avoid using their actual email address. For near-total online anonymity, programs like Anonymizer and Ghostsurf will hide one's IP address and erase browser information for a relatively low cost ($80 and $40 for one-year subscriptions, respectively, as of February 2011), although they apparently make the browsing process slower.

The market has provided these tools. How often consumers use these programs is unclear, but we would guess they are not used very often, and rationally so. Nonetheless, there are privacy solutions available to consumers who are truly concerned.

## V. Conclusion

We have argued that the current system of personal information collection, targeted advertisements, and free online services and applications works very well in the United States. The critics of this system have done an insufficient job describing and quantifying the dangers that they fear. They have also mistakenly tried to address security problems as privacy problems, and generally seem reluctant to view the issue of online privacy in economic terms. Of course, there is more to life and policy than economics, but every policy decision involves costs and benefits, whether one recognizes them explicitly or not. We believe they should be made explicit, if possible.

The damage from identity fraud and the value to consumers of protecting their personal information are small relative the huge value provided by ad-supported online services. There is

some evidence that Europe's stricter privacy regulation has reduced the value of targeted ads, which should, in turn, be expected to reduce funding for free online services. This does not prove that there are no privacy regulation changes that would create benefits greater than costs, but radical changes could upset the system that has created so much consumer surplus.

Surveys have repeatedly shown that consumers do not like targeted ads or the collection of personal information, and they suggest that consumers do not understand cookies or online privacy in general. They also suggest that most consumers who say they care about protecting their personal information fail to take basic steps to do so. We argue that their support for stricter privacy regulation is an example of rational irrationality. Politicians and regulators will certainly pay attention to the opinions of consumers—they ignore consumers and voters at their own peril—but that does not mean that the policy views of consumers are necessarily correct.