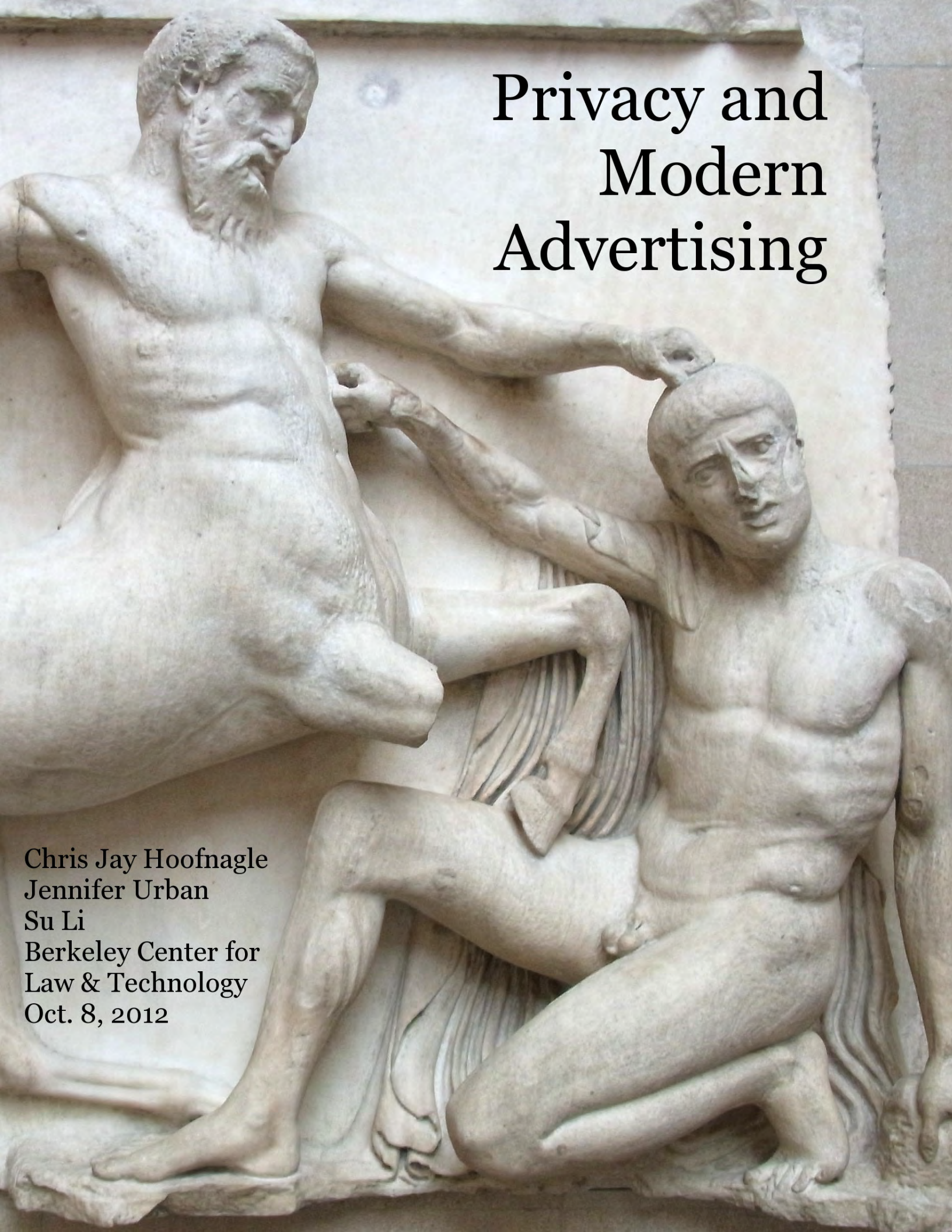

Privacy and Modern Advertising

Chris Jay Hoofnagle
Jennifer Urban
Su Li
Berkeley Center for Law & Technology
Oct. 8, 2012

Privacy and Modern Advertising: Most US Internet Users Want "Do Not Track" to Stop Collection of Data About their Online Activities

Chris Jay Hoofnagle,[1] Jennifer M. Urban,[2] & Su Li[3]
Berkeley Consumer Privacy Survey
BCLT Research Paper[4]
October 8, 2012

Abstract

Most Americans have not heard of "Do Not Track," a proposal to allow Internet users to exercise more control over online advertising. However, when probed, most prefer that Do Not Track block advertisers from collecting data about their online activities. This is a much more privacy-protective approach for Do Not Track than what has been proposed by the advertising industry.

In previous studies, we have found that Americans think they are protected by strong online privacy laws. Here, we probed beliefs about tracking on medical websites and "free" websites, with most not able to answer true/false questions

[1] Chris Jay Hoofnagle is a Lecturer in Residence at UC Berkeley Law and Senior Staff Attorney to the Samuelson Law, Technology & Public Policy Clinic.
[2] Jennifer M. Urban is Assistant Clinical Professor of Law at UC Berkeley Law, and Director of the Samuelson Law, Technology & Public Policy Clinic.
[3] Dr. Su Li is Statistician of Empirical Legal Studies at UC Berkeley Law.
[4] The underlying survey research for this paper was fully funded by Nokia, Inc. as part of an unrestricted research gift to the Berkeley Center for Law and Technology.

correctly about tracking. This result brings into question notice-and-choice models that depend on consumer understanding of the terms for their legitimacy.

We also probed Internet users' attitudes towards advertising. Most Internet users say that they do not find utility in online advertising, with half claiming that they never click on ads.

Advertisers and consumers are at an impasse on privacy. Advertisers seem to be seeking a kind of total information awareness for behavioral advertising, and have proposed self-regulatory guidelines with little bite. At the same time, both our survey evidence and media reports show consumer opposition to tracking.

Do Not Track has emerged from the current skirmish between consumers and advertisers, but it is a relatively modest intervention that does little to shift the underlying incentives that have driven increasing tracking and aggregation of information about consumers. It is foreseeable that regardless of the form Do Not Track takes, websites will simply require consumers to disable it in order to access content. A fundamental change in incentives may be necessary to relieve this impasse and find an approach for advertising that is not so dependent upon third-party tracking and aggregation of information, both online and off.

Introduction

The rise of detailed profiling techniques that track web users as they move around websites and from website to website has the potential to upend consumer expectations about what third parties know about them and how marketing campaigns are targeting them. Emerging and existing behavioral tracking techniques can build highly detailed dossiers on individual consumers. The hope is that these dossiers can help advertiser target ads in a manner that is more effective at selling products and services. Given, however, the possibilities of toppling consumer expectations, price and product discrimination, and the use of profiles for purposes well beyond offering advertising, privacy and consumer groups, the Federal Trade Commission,[5] and members of Congress[6] have all called for consumer control over the collection and use of behavioral tracking data.

There exist competing visions of how to manage the privacy issues raised by tracking data. An important set of approaches, generally referred to as "Do Not Track" (DNT) center on giving consumers the ability (usually via browser controls) to exercise some measure of control over behavioral tracking.

There is at present active debate over the best meaning and operation of DNT. In this research, we sought to understand Americans' attitudes about and understanding of important

---

[5] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE; A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, Dec. 2010, *available at* http://www.ftc.gov/opa/2010/12/privacyreport.shtm

[6] Cecilia Kang, *Sen. Rockefeller introduces 'do not track' bill for Internet*, WASHINGTON POST, May 9, 2011, *available at* http://www.washingtonpost.com/blogs/post-tech/post/sen-rockefeller-introduces-do-not-track-bill-for-internet/2011/05/09/AF0ymjaG_blog.html.

aspects of DNT as a policy option. We found that Americans have a low level of knowledge about DNT, but prefer that it mean that websites do not collect tracking data.

The Scope of "Do Not Track"

A recent series of articles published by the Wall Street Journal has focused public attention on how advertisers follow users online.[7] The most basic and popular method is through "cookies." A cookie is a small text file stored on a user's computer. Cookies are employed for a variety of reasons to enhance users' experience online, for example, by saving preferences or serving targeted content or advertisements.[8] A common distinction is drawn between first-party and third-party cookies. The former is issued by the website the user is visiting, the latter by some other website, often an advertiser serving an ad through the website the user is visiting.[9]

Third-party cookies (TPCs) are commonly used to track users across different websites[10] by companies that have no relationship with consumers. Whereas a consumer has chosen to visit the first-party site, third-party cookies represent tracking from parties the consumer may passively come into contact with and about which she is likely to have limited or no information. Thus for privacy-sensitive users, blocking TPCs is seen as a convenient and effective way of preventing tracking by advertising and other companies

---

[7] THE WALL STREET JOURNAL, WHAT THEY KNOW, *available at* http://online.wsj.com/public/page/what-they-know-digital-privacy.html.
[8] David M. Kristol, *HTTP Cookies: Standards, privacy, and politics*, 1 ACM TRANS. INTERNET TECHNOL. 151-198 (2001).
[9] MICROSOFT CORP., UNDERSTANDING COOKIES, n.d., *available at* http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sec_cook.mspx
[10] *Id.*

without disabling the basic functionality of the web.[11] By 2005, over 12% of users were rejecting TPCs.[12] In a previous Berkeley Consumer Privacy Survey, we found in 2009 that 39% of American internet users delete all their cookies "often;" only 21% never deleted cookies or did not know what they were.[13]

As consumers have learned about blocking TPCs, some companies have adjusted their tracking mechanisms to make it more difficult for users to avoid tracking.[14] The techniques used to track consumers online now are centralized, ubiquitous, robust, and often redundant.[15] For instance, in 2009 author Hoofnagle and colleagues found that half of the most popular websites were using Flash-based cookies instead of the traditional HTTP cookies that consumers often delete, and that some sites were using the technology to

---

[11] "...I've had my browsers set to block third-party cookies for the past few years. I haven't met the slightest inconvenience as a result." Rob Pegoraro, *How to Block Tracking Cookies*, THE WASHINGTON POST, July 17, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/07/16/AR2005071600111.html.

[12] Mickey Alam Khan, *Rising Cookie Rejection Bites Into Metrics*, DIRECT MARKETING NEWS, July 11, 2005, *available at* http://www.dmnews.com/rising-cookie-rejection-bites-into-metrics/article/88103/.

[13] Chris Jay Hoofnagle, Jennifer King, Su Li & Turow, Joseph, *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?* (Apr. 14, 2010), *available at* http://ssrn.com/abstract=1589864

[14] WEBTRENDS INC. WEBTRENDS ADVISES SITES TO MOVE TO FIRST-PARTY COOKIES BASED ON FOUR-FOLD INCREASE IN THIRD-PARTY COOKIE REJECTION RATES, May 23, 2005, *available at* http://www.webtrends.com/aboutwebtrends/newsroom/newsroomarchive/2005/cookierejection.

[15] Chris Jay Hoofnagle, Ashkan Soltani, Nathan Good, Dietrich J. Wambach & Mika D. Ayenson, *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARVARD L. & POLICY R. 273 (2012), *available at* http://ssrn.com/abstract=2137601.

respawn (recreate) HTTP cookies deleted by users.[16] More recently, researchers at Carnegie Mellon University found that thousands of websites had installed code that causes Microsoft's Internet Explorer browser to unblock cookies that Internet Explorer blocks by default.[17] A number of other tracking vectors are presently difficult for consumers to avoid, because they enable server-side tracking, because they are not well known by consumers, or because privacy controls for these tools are not popularly available. These include device fingerprinting,[18] HTML5 local storage,[19] Document Object Model (DOM) objects,[20] and Silverlight cookies.[21]

During most of these developments, the Federal Trade Commission has taken a self-regulatory approach, in which industry actors develop and implement guidelines themselves. More recently however, because of various factors including public attention, the technical sophistication of recent online tracking methods, and the apparent shortcomings of self-regulatory efforts in protecting

---

[16] Soltani, Ashkan, Canty, Shannon, Mayo, Quentin, Thomas, Lauren and Hoofnagle, Chris Jay, *Flash Cookies and Privacy* (Aug. 10, 2009). *available at*: http://ssrn.com/abstract=1446862

[17] Pedro Giovanni Leon, Lorrie Faith Cranor, Aleecia M. McDonald, Robert McGuire, *Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens*, Sept. 10, 2010, *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab10014.pdf.

[18] Peter Eckersley, *How Unique Is Your Browser?*, Proceedings of the Privacy Enhancing Technologies Symposium (PETS 2010), *available at* https://panopticlick.eff.org/browser-uniqueness.pdf.

[19] Jacqui Cheng, *Advertisers get hands stuck inside HTML5 database cookie jar*, ARS TECHNICA, Sept. 7, 2010, *available at* http://arstechnica.com/apple/news/2010/09/rldguid-tracking-cookies-in-safari-database-form.ars.

[20] MICROSOFT CORP., INTRODUCTION TO DOM STORAGE (2009), *available at* http://msdn.microsoft.com/en-us/library/cc197062%28VS.85%29.aspx

[21] MICROSOFT CORP., ISOLATED STORAGE (n.d.), *available at* http://msdn.microsoft.com/en-us/library/bdts8hk0%28v=VS.95%29.aspx

consumer choice and privacy, agency staff recommended a "Do Not Track" mechanism.[22] The agency's final report specified that an acceptable Do Not Track ("DNT") mechanism would include five elements:

> *First, a Do Not Track system should be implemented universally to cover all parties that would track consumers. Second, the choice mechanism should be easy to find, easy to understand, and easy to use. Third, any choices offered should be persistent and should not be overridden if, for example, consumers clear their cookies or update their browsers. Fourth, a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes. Finally, an effective Do Not Track system should go beyond simply opting consumers out of receiving targeted advertisements; it should opt them out of collection of behavioral data for all purposes other than those that would be consistent with the context of the interaction (e.g., preventing click-fraud or collecting de-identified data for analytics purposes).*[23]

This last requirement—that DNT address collection of data in the online behavioral advertising context—is the subject of

---

[22] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE; A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, Dec. 2010, *available at* http://www.ftc.gov/opa/2010/12/privacyreport.shtm; *see generally* Christopher Soghoian, *The History of the Do Not Track Header*, Jan. 21, 2011, *available at* http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html.

[23] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 53 (Mar. 2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf.

considerable debate and is the focus of the main findings of this survey research report.

Beyond the FTC's version, several different approaches to online tracking termed "Do Not Track" have been proposed.[24] For example, a much narrower version of DNT is articulated by the advertising industry, as represented by the Interactive Advertising "Bureau" ("IAB"). Under this version, consumers would be able to limit *uses* of personal information, but not the *collection* of this data as they move around the Web.[25]

It has been unclear which, if any, of these competing versions of DNT match Internet users' expectations of how online tracking should be treated. The IAB proposal may challenge common assumptions of what it means to "track." And as Omer Tene and Jules Polonetsky note, the FTC's proposal itself may be narrower than consumers' expectations. They note, "The self-regulatory principles proposed by the Federal Trade Commission also exclude from their scope any non-advertising behavioral targeting; contextual advertising; [and] first party tracking."[26]

Observing that, "The debates on DNT have notably lacked much information about what users expect and want online," Aleecia M. McDonald and Jon M. Peha performed the first

---

[24] *Track Gap: Policy Implications of User Expectations for the 'Do Not Track' Internet Privacy Feature*, TPRC 2011, Sept. 25, 2011, *available at* http://ssrn.com/abstract=1993133 (summarizing a wide variety of approaches to DNT).

[25] INTERACTIVE ADVERTISING BUREAU, COMMENTS OF THE INTERACT ADVERTISING BUREAU ON ONLINE BEHAVIORAL ADVERTISING PROPOSED PRINCIPLES, Apr. 11, 2008, *available at* http://www.iab.net/media/file/IAB_Comments_on_FTC_Behavioral_Advertising_Principles.pdf.

[26] Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising* 15 (2011)(internal citations omitted), *available at* http://ssrn.com/abstract=1920505 or http://dx.doi.org/10.2139/ssrn.1920505.

user survey on DNT in 2011.[27] McDonald and Peha administered an online survey to 293 Americans using Amazon's cloud-based crowdsourcing platform, Mechanical Turk. McDonald and Peha explain that Mechanical Turk's demographics skews towards female and younger users, and thus their sample reflects the site's population; nonetheless, this first study elucidated some complexities in understanding of DNT. They explored a wide range of tracking issues.[28]

McDonald and Peha found that 34 percent of respondents thought that DNT would prevent all data collection on websites. Importantly, large groups still thought that DNT would allow collection of certain information. For instance, 61 percent thought that websites could still tell what Internet browser was being used, 49 percent thought sites could still collect IP addresses, and 39 percent thought that sites could still track which pages a user views on a website.

The McDonald/Peha team also tested how respondents thought data could be used by tracking companies where consumers had enabled DNT. Thirty-five percent thought websites could still use data to tailor ads, 29 percent thought sites could still create profiles of users, and 24 percent thought that websites could still use data for any purpose.

McDonald and Peha then turned to asking respondents about hypothetical implementations of DNT. They presented users with three different possible implementations, the most stringent of which would prevent websites from retaining data about users, even if the user chose to log in. The least

---

[27] *Track Gap: Policy Implications of User Expectations for the 'Do Not Track' Internet Privacy Feature*, TPRC 2011, Sept. 25, 2011, *available at* http://ssrn.com/abstract=1993133

[28] Some of these issues are not discussed here, for instance whether users differentiate between first and third parties, and whether they trusted a DNT mechanism to work properly.

stringent was closely aligned with industry proposals, which allow collection and use of data for many purposes. They found that users preferred that DNT take the most stringent approach. They concluded:

> *Over all, we find that participants did not have an overwhelmingly strong expectation for what DNT will be, but would prefer DNT have a wide scope covering data collection, even at the cost of losing personalization they might enjoy. Participants did not like the idea of DNT working via data use changes rather than data collection changes.*[29]

Tracking versus Use

Seeking to broaden McDonald and Peha's inquiry to a larger, representative sample, we also inquired about the meaning of DNT and its application. In our pretest of survey questions, we asked respondents what DNT meant, but almost two-thirds of the respondents simply did not know. Indeed, the vast majority of American consumers have never heard of DNT.

As a result of the pretest, we changed approaches, and instead of asking what they expected DNT would do, we asked consumers what they preferred it do. We also explicitly asked the full sample whether DNT was something they had heard of, or not.

We asked American consumers, "Policymakers are considering creating a "do not track" option for the internet. Have you heard of proposals for a "do not track" system, or not?" Thirteen percent had heard of it, and fully 87 percent

---

[29] Aleecia M. McDonald & Jon M. Peha, *Track Gap: Policy Implications of User Expectations for the 'Do Not Track' Internet Privacy Feature* 25, TPRC 2011, Sept. 25, 2011, *available at* http://ssrn.com/abstract=1993133

had not. (N=1203.) This is similar to McDonald and Peha's findings, where 81 percent had not heard of DNT prior to the study.[30]

We then asked what Americans would prefer Do Not Track to do. Three options were presented to respondents in random order. One option would prevent collection of information; the other two would prevent two different actions on the part of the website.

Table 1: What Americans Want "Do Not Track " to Do

If a 'do not track' option were available to you when browsing the internet, which of the following things would you most want it to do? Should do not track... (READ AND RANDOMIZE)(N=1203)	
Prevent websites from collecting information about you	60%
Block websites from showing you advertisements	20%
Prevent websites from tailoring advertisements based upon the websites you have previously visited	14%
Don't know/refused	6%

A majority—60 percent—said they wanted DNT to stop websites from collecting information about the user. This was the closest option to the FTC's proposal and the proposals of privacy groups, although simplified. The next largest group, 20 percent, wanted DNT to block advertisements. We presented that option because we suspected that many users expected DNT to simply block ads. Only 14 percent chose the option that most closely matches the industry's suggested use-restriction proposal.

There are good reasons, independent of survey evidence, to seriously consider collection limitations instead of laws that allow unlimited collection and focus only on regulating uses of the collected data. We point to consumer reporting agencies, companies such as Experian, Trans Union, and

[30] McDonald & Peha at 7.

Equifax, as examples of entities that are subject mainly to use restrictions and transparency mandates rather than collection restrictions. Despite being subject to transparency requirements, including the duty to provide free reports to consumers and to maintain audit trails of access to such reports, these companies remain largely unaccountable for their uses of data and are notoriously unresponsive to consumers with problems. As a group, consumer reporting agencies are the topic of tens of thousands of consumer complaints annually,[31] and all three have been subject to enforcement actions by the Federal Trade Commission.[32] Trans Union sold sensitive consumer personal information in violation of the Fair Credit Reporting Act, arguing that they had a First Amendment right to do so.[33]

More fundamentally, it is practically impossible for consumers to monitor and control unwanted uses of personal information, especially by third parties, once data are collected. Berkeley's Web Privacy Census recently found that the most popular websites placed 50 third-party cookies on average, with one placing 234.[34] These trackers then share

---

[31] FEDERAL TRADE COMMISSION, FTC RELEASES TOP COMPLAINT CATEGORIES FOR 2011, IDENTITY THEFT ONCE AGAIN TOPS THE LIST, Feb. 28, 2012, *available at* http://ftc.gov/opa/2012/02/2011complaints.shtm.

[32] Federal Trade Commission, Consumerinfo.com Settles FTC Charges, Feb. 21, 2007, *available at* http://www.ftc.gov/opa/2007/02/cic.shtm; FEDERAL TRADE COMMISSION, EQUIFAX TO PAY $250,000 TO SETTLE CHARGES, FTC ALLEGES BLOCKED AND DELAYED CONSUMER CALLS VIOLATED CONSENT DECREE , Jul. 30, 2003, *available at* http://www.ftc.gov/opa/2003/07/equifax.shtm; FEDERAL TRADE COMMISSION, NATION'S BIG THREE CONSUMER REPORTING AGENCIES AGREE TO PAY $2.5 MILLION TO SETTLE FTC CHARGES OF VIOLATING FAIR CREDIT REPORTING ACT, Jan. 13, 2000, *available at* http://www.ftc.gov/opa/2000/01/busysignal.shtm.

[33] *Trans Union LLC v. Federal Trade Commission*, 245 F.3d 809 (D.C. Cir. 2001).

[34] Nathan Good & Chris Jay Hoofnagle, *The Web Privacy Census*, June 2012, *available at* http://law.berkeley.edu/privacycensus.htm

data with ad networks including chains of buyers and sellers of data that are invisible to the first-party site itself, let alone the consumer. More generally, for many companies, the temptation to use data for new purposes can be very strong. The IAB argues explicitly that information collected for targeted advertising should be able to be used for secondary purposes, noting that these uses are often disclosed in privacy policies and do not harm consumers.[35] We suspect that this may be especially true where consumers are unlikely to detect the use.[36]

Consumer Knowledge of Tracking

In previous surveys, we have explored consumers' understanding of privacy, and in particular, the protections offered by privacy policies. In a series of studies, starting in 2008, we have found that consumers think that strong, opt-in laws protect them in many contexts.[37] In the context of the

---

[35] INTERACTIVE ADVERTISING BUREAU, COMMENTS OF THE INTERACT ADVERTISING BUREAU ON ONLINE BEHAVIORAL ADVERTISING PROPOSED PRINCIPLES, Apr. 11, 2008, *available at* http://www.iab.net/media/file/IAB_Comments_on_FTC_Behavioral_Advertising_Principles.pdf. ("...it has been a long-standing practice for companies to use collected information for multiple purposes, including within the context of online advertising, for related business matters, as well as purposes related to regulatory and law enforcement demands.")

[36] Well-known examples of this type of backlash include DoubleClick's original attempt, in the year 2000, to connect web tracking with offline information, Stefanie Olsen, *FTC Drops Probe into DoubleClick Privacy Practices*, CNET.com, Jan. 22, 2001, *available at* http://news.cnet.com/2100-1023-251325.html, and consumer reaction to the revelation that Facebook was collecting contact lists from consumers' smartphones through the Facebook app. Dan Tynan, *Facebook's phonebook fiasco*, IT World (Aug. 11, 2011), at http://www.itworld.com/it-managementstrategy/192399/facebooks-phonebook-fiasco.

[37] Chris Jay Hoofnagle and Jennifer King, *Research Report: What Californians Understand About Privacy Offline* (May 15, 2008), *available at* http://ssrn.com/abstract=1133075; Chris Jay Hoofnagle

Internet, our work and research by Professor Joseph Turow has revealed a serious disconnect between consumers' understanding of privacy rules and actual business practices.[38]

In the 2009 study, author Hoofnagle and colleagues asked a national sample of US internet-using consumers a series of true/false questions concerning privacy.[39] The questions tested, for instance, whether consumers believed that websites with a privacy policy must refrain from selling data, whether websites must delete information about a customer upon request, and whether individuals have the right to sue websites for violating privacy policies. For each of these questions, a majority answered "true" or "don't know." In each case, however, the correct answer was "false." On average, the consumers to whom we administered this quiz failed it, thinking that they have broader privacy rights than they have in reality. On average, they correctly answered only

---

and Jennifer King, *What Californians Understand about Privacy Online* (September 3, 2008), *available at* http://ssrn.com/abstract=1262130. *See also* Jennifer M. Urban, Chris Jay Hoofnagle, and Su Li, *Mobile Phones and Privacy* (July 12, 2012), *available at* http://ssrn.com/abstract=2103405 (finding that Americans strongly preferred court oversight before phones were searched during an arrest, despite the fact that a variety of courts have held otherwise). *See generally id.* and Chris Jay Hoofnagle, Jennifer M. Urban, and Su Li, *Mobile Payments: Consumer Benefits & New Privacy Concerns* (Apr. 24, 2012) (finding high levels of consumer rejection of a variety of existing business models and government practices.)

[38] See e.g. Joseph Turow, *Americans & Online Privacy, The System is Broken,* Annenberg Public Policy Center (June 2003); Joseph Turow, Lauren Feldman, & Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline*, Annenberg Public Policy Center of the University of Pennsylvania, Jun, 1, 2005.

[39] Joseph Turow, Jennifer King, Amy Bleakly, Michael Hennessy, and Chris Jay Hoofnagle, *Americans Reject Tailored Advertising and Three Activities that Enable It* (September 29, 2009), *available at* http://ssrn.com/abstract=1478214.

1.5 of the 5 statements about online practices and 1.7 of the 4 statements offline practices.[40]

Given this track record, we decided to ask questions in this survey that would allow us to explore consumer understanding of some additional topics, focusing on tracking on medical websites and on websites that offer "free" services.

Tracking on Medical Websites

Most Internet users search for medical information online.[41] The Internet can be a powerful tool for those interested in learning about medical conditions, and it allows one to explore sensitive or embarrassing topics in the comfort of one's home. Advertisers are along for this exploration, however. For decades, advertisers have profiled consumers based upon their medical conditions in offline contexts.[42] Online, many companies allow third-party tracking companies to monitor consumer health websites.[43]

Medical information is recognized as particularly sensitive. It is one of the few data types explicitly protected under federal

---

[40] *Id.* at 21.
[41] Susannah Fox, *Pew Internet: Health*, Mar. 1, 2012, Pew Research Center's Internet & American Life Project, *available at* http://pewinternet.org/Commentary/2011/November/Pew-Internet-Health.aspx ("80% of internet users, or 59% of U.S. adults, look online for health information.").
[42] *See e.g.* AMERICANS WITH AILMENTS, n.d., *available at* http://listfinder.directmag.com/market?page=research/datacard&id=93742 (postal mail list of 16 million Americans, "...experiencing one or more of the following ailments or illnesses...").
[43] *See e.g.*, Jacquelyn Burkell and Alexandre Fortier, *Consumer Health Websites and Behavioural Tracking* (2012), proceedings of CAIS/ACSI, *available at* http://www.cais-acsi.ca/ (examining behavorial tracking on health-related websites, and finding "that over three quarters of the websites in these groups employ tracking technologies, potentially aggregating information across websites and allowing the assembly of detailed user profiles.").

law.[44] As early as 2000, the advertising industry itself recognized the sensitive nature of medical information and promised not to use it for advertising. In July 2000, the major network advertising companies[45] articulated the Network Advertising Initiative (NAI) "Self-Regulatory Principles for Online Preference Marketing by Network Advertisers." Under this framework, the NAI promised to not use "sensitive" personally identifiable data for "online preference marketing." The group explained, "Network advertisers shall neither use personally identifiable information about sensitive medical or financial data, sexual behavior or sexual orientation, nor social security numbers, for OPM [online preference marketing]."[46]

Almost ten years later, the advertising industry has retreated from its 2000 position, and the 2000 principles can no longer be found on the NAI's website.

The leading proposal to address behavioral advertising now comes from the Digital Advertising Alliance (DAA). In its self-regulatory principles for online behavioral advertising, the DAA advises that companies not, "collect financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records about specific individuals for Online Behavioral Advertising purposes without Consent."[47]

It is important to note the limits of this rule. First, it only pertains to patients' actual prescription and medical records. This information is likely held only by health care providers, not advertiser-supported consumer websites like WebMD or

---

[44] Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d-9 (2010).
[45] 24/7 Media, AdForce, AdKnowledge, Avenue A, Burst! Media, DoubleClick, Engage, L90, MatchLogic.
[46] http://www.ftc.gov/os/2000/07/NAI%207-10%20Final.pdf.
[47] DIGITAL ADVERTISING ALLIANCE, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING, Jul. 2009, *available at* http://www.aboutads.info/obaprinciples.

HealthCentral.com. Unlike these websites, health care providers are subject to comprehensive state and federal privacy laws, and are unlikely to place advertising tracking beacons on their medical record sites.

Thus, an Internet user searching for information about or discussing a specific medical condition may still be tracked under the DAA's principles. Arguably, the NAI's principles limited this practice.

Second, recall that the 2000 NAI principles discussed information that was "personally identifiable." This suggested that NAI members would not use information that *could* be directly tied to individuals. The DAA's rules only cover information about "about specific individuals."

Third, the prohibition only applies to collection of information related to "Online Behavioral Advertising" purposes, and thus, tracking services could collect medical record information about specific individuals so long as it was for some different purpose. Finally, "Consent" here is vaguely defined as "…an individual's action in response to a clear, meaningful and prominent notice regarding the collection and use of data for Online Behavioral Advertising purposes." This definition would seem to leave room for "consent" to be found if a consumer merely uses a website after receiving a warning about behavioral advertising.

In 2009, we asked several questions concerning Internet tracking. To set a baseline, we asked whether tracking internet use across multiple websites required permission from the user. Forty-eight percent incorrectly answered "true" to this question, and 19 percent did not know the answer. Only 33 percent correctly answered "false."

When we turned to tracking on medical websites in this survey, we found that large numbers of consumers do not know what the rules are. We asked respondents whether it

was true or false that advertisers are not allowed to track users using the internet to learn about medical conditions. While 36 percent correctly answered that this statement was false, 63 percent either did not know or responded incorrectly. Specifically, 22 percent thought permission was necessary, and 41 percent said they did not know the answer.

Table 2: Tracking on Medical Websites

Knowledge of tracking on medical websites (bold = correct answer)	True	False	Don't Know/ Refused
If a company wants to follow your internet use across multiple sites on the internet, it must first obtain your permission (2009)(N=1000)	48%	**33%**	19%
When you use the internet to learn about medical conditions, advertisers are not allowed to track you in order to target advertisements (2011)(N=1203)	22%	**36%**	41%

Free Websites

Offers of "free" services abound on the Internet.[48] We wished to explore whether Internet users thought these sites were subject to different rules than sites to provide services on a subscription or other obviously "paid" basis. In other words, do consumers think that they are trading their privacy or personal information in exchange for free services?

We asked three questions surrounding free websites. As with other areas of Internet privacy, there was a high level of ignorance concerning the rules governing such sites. For

[48] Jan Whittington & Chris Jay Hoofnagle, *Unpacking Privacy's Price*, 90 NORTH CAROLINA LAW REVIEW 1327 (2012), *available at* http://ssrn.com/abstract=2059154 (applying transaction cost economics to internet exchanges).

instance, while 40 percent correctly answered "true" to a question asking whether free websites could sell data to third parties, 19 percent incorrectly answered "false," and 40 percent simply did not know. Similarly, confusion surrounded a right to delete personal information from free websites. Twenty-five percent mistakenly thought that they enjoyed this right, and 42 percent did not know. Only 32 percent answered this question correctly—false.

Table 3: What Americans Think "Free" Websites Can Do with Information About Them

Free Websites and Privacy Rules (bold = correct answer)	True	False	Don't Know
Free websites that are supported by advertising are allowed to sell information gathered from users of the site, even if they have a privacy policy	**40%**	19%	40%
When visiting free websites supported by advertising, you have the right to require the website to delete the information it has about you	25%	**32%**	42%

We also asked whether consumers thought they generally had more or less privacy rights on free websites. Forty percent thought they had less, 36 percent answered "about the same amount," and 22 percent did not know.

Table 4: "Free" Websites and Privacy Rights

Free Websites and Privacy Rights	More	Less	About the Same	Don't Know/ Refused
When you use a free website, one that is supported by advertising, do you have more privacy rights, less privacy rights, or about the same amount of rights as when you use a website that charges a fee for its use?	2%	40%	36%	22%

Attitudes Towards Online Advertising Generally

We suspected that Internet users' attitudes towards DNT would be related to feelings about advertising more generally. The desire for DNT to mean "do not collect tracking data" may be based upon concern about privacy and an aversion to advertising more generally. We thus asked a series of questions about advertising.

We first asked, "In general, how often do you find online advertising, such as the advertising that appears on search results webpages and banner advertisements, useful?" Thirty percent do find utility in advertising, with 10 percent reporting that they find search and banner advertisements useful often, and 20 percent sometimes find this information useful. Thirty-six percent answered "hardly ever," and 33 percent answered "never."

We followed the utility question by asking whether users actually clicked on advertisements. We asked, "How often do you click on advertisements when using the internet?" Fifty percent claimed that they never click on ads, and 35 percent responded hardly ever. It may be that this is incorrect—that consumers do not remember or selectively remember their interaction with advertising.[49] We have no way to test this directly; however, there is some indirect evidence supporting our respondents' claims. It is true, for example, that accidental and fraudulent clicks are a pervasive problem,[50] and that as of this writing, the most popular add-on for the Firefox web browser is AdBlock Plus, with over 14 million users.[51]

Table 5: Americans' Attitudes Toward Online Ads

Online Ad Attitudes	Often	Sometimes	Hardly Ever	Never	Don't Know/ Refused
Do you find ads useful?	10%	20%	36%	33%	1%
Do you click?	2%	12%	35%	50%	*

[49] We note that we did not have a way to verify whether this claim is borne out by actual behavior, but it is clear that our respondents subjectively found online ads of limited value.

[50] Ryan Kim, Report: *40 Percent of Mobile Clicks are Fraud or Accidents*, GIGAOM, Aug. 31, 2012, *available at* http://gigaom.com/2012/08/31/report-40-percent-of-mobile-clicks-are-fraud-or-accidents/

[51] MOZILLA FOUNDATION, MOST POPULAR EXTENSIONS, visited Sept. 23, 2012, *available at* https://addons.mozilla.org/en-US/firefox/extensions/?sort=users.

Conclusion

In a series of surveys on consumer attitudes, we have confirmed that Americans care about privacy. We have argued that meeting the aspiration for increased privacy is challenging because the online marketplace is optimized to maximize collection of data. The modern consumer acts as an individual in a medium where hundreds of companies compete to encourage revelation of information from the consumer, and to track consumer behavior and associations pervasively. Even if one pays for content with money, this tracking still occurs. It is in this context that advocates and regulators have called for an option to give individuals more control over internet privacy—Do Not Track.

In light of consumer attitudes and marketplace realities, Do Not Track is a modest intervention. Yet the advertising industry has argued for systemically weakening what "Do Not Track" means, and has retreated from earlier, stronger promises to limit tracking.

We found that most consumers want Do Not Track to mean exactly that: do not collect information that allows companies to track them across the Internet. This may seem obvious, but even the definition articulated by the FTC may fall short of these consumer expectations. Further, advertising industry groups presently are lobbying for a different interpretation that would allow pervasive tracking and use of information derived from online experiences, even if the consumer opts out.

This disconnect appears pervasive and strong. In addition to the fact that a strong majority of respondents prefer that Do Not Track allow them to opt out of collection, there is a lack of understanding about what trackers can do. We found that only about 1 in 3 internet users understands that advertisers can track them on medical sites. Here too, despite broad consensus that medical information is especially sensitive

and despite widespread consumer ignorance of the rules governing the collection and use of behavioral tracking on medical websites, advertising lobbying groups have stuck to a "notice and no choice" approach. Their self-imposed rules appear to allow tracking of individuals as they engage with some of the most sensitive topics in their lives, even if those individuals attempt to opt out of the tracking.

Consumers and advertisers seem to be at an impasse on privacy. This impasse is the product of consumers' anxiety about tracking, and advertisers' concern that any imposition upon data collection will undermine an existing and growing business model. Subjectively at least, nearly 70% of consumers say that they find little if any value in online ads. Half claim to never click on ads at all. Yet advertisers' position on tracking is that consumers should be tracked even if they opt out of tracking, suggesting that consumers' subjective opinions about tracking do not matter.

Lost in the present debate is the fact that DNT essentially responds to a specific business model, one in which third parties attempt to build advertising value by tracking individuals in all aspects of their lives. This model seems to require continually ratcheting up data collection and ratcheting down privacy protections in an attempt to show value to ad buyers.

Targeting consumers based upon specific information about them appears to be increasing across a variety of internet and mobile marketing models, with an apparent goal of linking online and offline purchase behavior. In previous work, we have explored mobile payments models that promise to connect more payments ecosystem players with detailed "Level 3" purchase data (lists of the specific things consumers buy) for individual consumers shopping at bricks-and-mortar stores and mobile app models that use app users' address

books to target offers.[52] And as this paper was being prepared, for example, newspapers reported that Facebook was beginning to buy data on Facebook users' specific purchases in CVS drugstores in order to show whether targeted ads served to individual profiles actually resulted in increased sales of the advertised products.[53] As another example, a different recently announced Facebook scheme allows retailers to match their offline marketing lists with Facebook's databases in order to target ads to specific Facebook users.[54]

Some of these models threaten to seriously undermine privacy expectations and echo models that prompted backlash and regulation in the past.[55] If present trends continue, we will soon find ourselves in a world where ultra-large tracking platforms will have data about almost all online and offline consumer transactional behavior. Consumers will find themselves subject to these platforms' power to collect and use that data, and with little recourse or say about that collection and use.

---

[52] Chris Jay Hoofnagle, Jennifer M. Urban, and Su Li, *Mobile Payments: Consumer Benefits & New Privacy Concerns* (Apr. 24, 2012); and Jennifer M. Urban, Chris Jay Hoofnagle, and Su Li, *Mobile Phones and Privacy* (July 12, 2012), *available at* http://ssrn.com/abstract=2103405.

[53] Rebecca Greenfield, *Facebook Now Knows What You're Buying at Drugstores*, THE ATLANTIC WIRE (Sept. 24, 2012), *available at* http://www.theatlanticwire.com/technology/2012/09/facebook-tracking-you-drug-store-now-too/57183/.

[54] Jon Constine, *Facebook Lets Businesses Plug In CRM Email Addresses To Target Customers With Hyper-Relevant Ads*, TECHCRUNCH, Sept. 20, 2012, *available at* http://techcrunch.com/2012/09/20/facebook-crm-ads/

[55] Combining web tracking and offline data, for example, caused DoubleClick to experience a severe consumer backlash in the early 2000s. Stefanie Olsen, *FTC Drops Probe into DoubleClick Privacy Practices*, CNET.com, Jan. 22, 2001, *available at* http://news.cnet.com/2100-1023-251325.html.

We think that there are ways around the impasse between advertising models and consumers' apparent expectations of privacy. There are alternative approaches to the "track everyone, everywhere" model. Academics including Steven Bellovin,[56] Eric Goldman,[57] and Helen Nissenbaum[58] have proposed alternative models that would allow highly targeted ads without creating dossiers of internet behavior held by third parties.

At the very least, regulators and industry should consider the models proposed by Bellovin, Goldman, and Nissenbaum as alternatives to the present one. In addition, regulators could put into place consumer-protective rules that could be implemented through some of these models. Surely this approach would pose trade-offs as well. But given our respondents' preferences, as gauged over the three tranches of data we have released so far, continuing with the ever-increasing collection and use of specific consumer data demanded by the existing business model threatens to prompt a strong consumer backlash.

As such, we think that the information provided by our survey respondents suggests a revised approach to consumer tracking and targeted advertising by advertisers, platform providers, and regulators.

---

[56] Elli Androulaki and Steven M. Bellovin, *A secure and privacy-preserving targeted ad-system*, *in* Proceedings of the 1st Workshop on Real-Life Cryptographic Protocols and Standardization, Jan. 2010.
[57] Eric Goldman, *A Coasean Analysis of Marketing*, 2006 WIS. L. REV. 1151 (2006).
[58] Vincent Toubiana, Arvind Narayanan, Dan Boneh, Helen Nissenbaum, Solon Barocas, *Adnostic: Privacy Preserving Targeted Advertising*, NDSS 2010, *available at* http://crypto.stanford.edu/adnostic/.

Appendix 1: Methods

The Berkeley Consumer Privacy Survey obtained telephone interviews with a nationally representative sample of 1,203 adult Internet users living in the continental United States. Telephone interviews were conducted by landline (678) and cell phone (525, including 235 without a landline phone). Overall, 6,906 working landlines and 8,688 working cell phones were dialed. The response rate for the landline samples was 16 percent. The response rate for the cellular samples was 14 percent. Statistical results were weighted to correct known demographic discrepancies.

The survey was conducted by Princeton Survey Research Associates International (PSRAI), and was fully funded by Nokia, Inc. as part of an unrestricted gift to the Berkeley Center for Law and Technology. The content of the survey was entirely composed by Berkeley Law's Chris Jay Hoofnagle & Jennifer M. Urban. Interviews were done in English by Princeton Data Source from January 27-February 12, 2012. Statistical results are weighted to correct known demographic discrepancies. The margin of sampling error for the complete set of weighted data is ± 3.4 percentage points.