



9-2009

Americans Reject Tailored Advertising and Three Activities That Enable It

Joseph Turow

University of Pennsylvania, jturow@asc.upenn.edu

Jennifer King

University of California, Berkeley, School of Law, Berkeley Center for Law & Technology

Chris Hoofnagle

University of California, Berkeley, School of Law, Berkeley Center for Law & Technology

Amy Bleakley

Annenberg Public Policy Center, University of Pennsylvania

Michael Hennessy

Annenberg Public Policy Center, University of Pennsylvania

Follow this and additional works at: https://repository.upenn.edu/asc_papers

 Part of the [Communication Commons](#)

Recommended Citation (OVERRIDE)

Turow, J., King, J., Hoofnagle, J.C., Bleakley, A., and Hennessy, M. (2009). Americans Reject Tailored Advertising and Three Activities That Enable It. Annenberg School for Communication (U of Pennsylvania) and Berkeley School of Law (U California, Berkeley).

This paper is posted at ScholarlyCommons. https://repository.upenn.edu/asc_papers/524

For more information, please contact repository@pobox.upenn.edu.

Americans Reject Tailored Advertising and Three Activities That Enable It

Disciplines

Communication | Social and Behavioral Sciences

Contrary to what marketers say,

AMERICANS REJECT TAILORED ADVERTISING

Cookie:TShram@google.com/mobile
Cookie:TShram@www.msnbc.msn.com/id/234355
Cookie:TShram@tvguide.com/PartnerGrid
Cookie:TShram@www.dell.com/phpvm2
Cookie:TShram@voip.fabphone.co.uk/voip/promo
Cookie:TShram@www.toadhammer.com/publication
Cookie:TShram@www.comcastsupport.com/sccuser/rnfi
Cookie:TShram@www.ebay.com/rtm/main
Cookie:TShram@stat.upe.com/sb/
Cookie:TShram@www.comcastrupport.com/sdCookie:TShram@user
Cookie:TShram@bing.com/search
Cookie:TShram@www.google.com/mobile
Cookie:TShram@onlinestores.metaservices.microsoft.com/swservice/wiiching
Cookie:TShram@www.librarything.com/tag
Cookie:TShram@www.google.com/talk
Cookie:TShram@ytsa.net/tase
Cookie:TShram@community.adobe.com/help/api/thumbs
Cookie:TShram@google.com/verify

AND THREE ACTIVITIES THAT ENABLE IT

27=1JR2BZwybn9ozsGG7nzQprKfpqOX_Ai6QDcxTmOf4Q=SSDIBYXE3on3iWwc

google.com/verify

9728

2320728704

30067751

406026352

30030938

*

ach-search

UjiezX7sFgNwJhrie19zsC69Vu8=

community.adobe.com/help/api/v1/thumbs/

1536

2784647552

30759988

3564042032

30025733

*

sik_client_guid

47aeeb428-73bc-ada9-bb60-728dc6367a7

www.comcastsupport.com/sccuser/rnfi

1088

284664448

30089887

2560430544

30016461

*

SynZCSI

K_25_503=10036:80001

tvguide.com/PartnerGrid

Joseph Turow

Annenberg School for Communication, University of Pennsylvania

Jennifer King

University of California, Berkeley, School of Law, Berkeley Center for Law & Technology

Chris Jay Hoofnagle

University of California, Berkeley, School of Law, Berkeley Center for Law & Technology

Amy Bleakley

Annenberg Public Policy Center, University of Pennsylvania

Michael Hennesy

Annenberg Public Policy Center, University of Pennsylvania

Joseph Turow, Ph.D., is Robert Lewis Shayon Professor of Communication at the Annenberg School for Communication, University of Pennsylvania. Among his several books are *Niche Emy: Marketing Discrimination in the Digital Age* (MIT Press, 2006) and *Breaking Up America: Advertisers and the New Media World* (U of Chicago Press, 1997). Since 1999 he has conducted national telephone surveys that have moved forward public discourse on digital media, marketing, and privacy. Several can be found at the Annenberg Public Policy Center website, APCCPenn.org.

Jennifer King, MIMS, is a Ph.D. student at the UC Berkeley School of Information. Most recently she was a researcher at the Samuelson Law, Technology, and Public Policy Clinic at UC Berkeley's School of Law. Her research areas include information privacy and security, usability and human-computer interaction, video surveillance and other sensor networks. With Chris Hoofnagle, King has published three reports exploring Californians' privacy attitudes; these are available at ssrn.com.

Chris Jay Hoofnagle, J.D., is director of the Berkeley Center for Law & Technology's information privacy programs and senior fellow to the Samuelson Law, Technology & Public Policy Clinic. He is an expert in information privacy law. Hoofnagle co-chairs the annual Privacy Law Scholars Conference. He is licensed to practice law in California and Washington, DC.

Amy Bleakley, Ph.D., MPH, is a Research Scientist in the Health Communication Group of the Annenberg Public Policy Center at the University of Pennsylvania. Dr. Bleakley studies adolescent sexual behavior, sexual and reproductive health policies, health behavior theory, and contextual influences on health behavior. Her current research focuses investigating the effect of sexual content in the media on adolescent sexual development.

Michael Hennessy, Ph.D., is Project Manager and Statistician in the Health Communication Group of the Annenberg Public Policy Center. His major interest is the integration of structural equation modeling and intervention program/behavioral theory, growth curve analysis of longitudinal data, and using factorial surveys to design both behavioral intervention programs and community-based clinical trials for experimental vaccines. He has published over 90 articles in *Evaluation Review*, *Structural Equation Modeling*, *AIDS and Behavior*, *Psychology Health & Medicine*, *The American Journal of Evaluation*, and *Evaluation and the Health Profession* among other journals.

September, 2009

This survey was supported by the Rose Foundation for Communities and the Environment, Tim Little, Executive Director, under grant 025629-003, Chris Jay Hoofnagle, Principal Investigator; and by The Annenberg School for Communication—Michael Delli Carpini, Dean.

Overview

Contrary to what many marketers claim, most adult Americans (66%) do not want marketers to tailor advertisements to their interests. Moreover, when Americans are informed of three common ways that marketers gather data about people in order to tailor ads, even higher percentages—between 73% and 86%—say they would not want such advertising.

These are two findings from the first nationally representative telephone (wireline and cell phone) survey to explore Americans' opinions about behavioral targeting by marketers, a controversial issue currently before government policymakers. Behavioral targeting involves two types of activities: following users' actions and then tailoring advertisements for the users based on those actions. While privacy advocates have lambasted behavioral targeting for tracking and labeling people in ways they do not know or understand, marketers have defended the practice by insisting it gives Americans what they want: advertisements and other forms of content that are as relevant to their lives as possible.

We conducted this survey to determine which view Americans hold. In high percentages, they stand on the side of privacy advocates. That is the case even among young adults whom advertisers often portray as caring little about information privacy. Our survey did find that younger American adults are less likely to say no to tailored advertising than are older ones. Still, more than half (55%) of 18-24 year-olds do not want tailored advertising. And contrary to consistent assertions of marketers, young adults have as strong an aversion to being followed across websites and offline (for example, in stores) as do older adults. 86% of young adults say they don't want tailored advertising if it is the result of following their behavior on websites other than one they are visiting, and 90% of them reject it if it is the result of following what they do offline. The survey uncovered other attitudes by Americans toward tailored content and the collection of information about them. For example:

- Even when they are told that the act of following them on websites will take place anonymously, Americans' aversion to it remains: 68% "definitely" would not allow it, and 19% would "probably" not allow it.
- A majority of Americans also does not want discounts or news fashioned specifically for them, though the percentages are smaller than the proportion rejecting ads.
- 69% of American adults feel there should be a law that gives people the right to know everything that a website knows about them.
- 92% agree there should be a law that requires "websites and advertising companies to delete all stored information about an individual, if requested to do so."
- 63% believe advertisers should be required by law to immediately delete information about their internet activity.

- Americans mistakenly believe that current government laws restrict companies from selling wide-ranging data about them. When asked true-false questions about companies' rights to share and sell information about their activities online and off, respondents on average answer only 1.5 of 5 online laws and 1.7 of the 4 offline laws correctly because they falsely assume government regulations prohibit the sale of data.
- Signaling frustration over privacy issues, Americans are inclined toward strict punishment of information offenders. 70% suggest that a company should be fined more than the maximum amount suggested (\$2,500) "if a company purchases or uses someone's information illegally."
- When asked to choose what, if anything should be a company's single punishment beyond fines if it "uses a person's information illegally," 38% of Americans answer that the company should "fund efforts to help people protect privacy." But over half of Americans adults are far tougher: 18% choose that the company should "be put out of business" and 35% select that "executives who are responsible should face jail time."

It is hard to escape the conclusion that our survey is tapping into a deep concern by Americans that marketers' tailoring of ads for them and various forms of tracking that informs those personalizations are wrong. Exactly why they reject behavioral targeting is hard to determine. There may well be several reasons. One may be a general antagonism to being followed without knowing exactly how or with what effects. Americans may not want their behavior on one site to somehow affect the interaction with subsequent sites. Consumers may intend to divide their web browsing into different subjective contexts (e.g. shopping, work, play, education), and they may worry that tracking across those contexts may subject them to embarrassment (e.g. while using the computer in the work context, ads may be displayed that are relevant to play). Another reason might be a fear that selective presentation of advertisements, discount offers, or news will put them at a monetary or social disadvantage: some people might get more useful or interesting tailored content than others depending on the conclusions marketers draw about them. The rejection of even anonymous behavioral targeting by large proportions of Americans may mean that they do not believe that data about them will remain disconnected from their personally identifiable information. It may also mean that anonymity is not the only worry they have about the process. Being labeled in ways they consider unfair by marketers online and off may be just as important a concern.

Whatever the reasons, our findings suggest that if Americans could vote on behavioral targeting today, they would shut it down. The findings also suggest that marketers and government policymakers may be faced with a backlash if Americans were to organize around complaints that the laws they think protect them from the sale of their data actually don't exist. It is also important to note that this rejection of tailoring and behavioral tracking by marketers and media firms does not mean Americans reject the idea of customizing ads, discounts, and news themselves. To the contrary, evidence from around the digital world shows that they want to control and shape what

content they receive. The problem for marketers is that Americans are worried about others' use of data about them in ways they do not know or understand, and might not like.

In fact, our survey found that Americans want openness with marketers. If marketers want to continue to use various forms of behavioral targeting in their interactions with Americans, they must work with policymakers to open up the process so that individuals can learn exactly how their information is being collected and used, and then exercise control over their data. At the end of this report, we offer specific proposals in this direction. An overarching one is for marketers to implement a regime of *information respect* toward the public rather than to treat them as objects from which they can take information in order to optimally persuade them.

Background

Behavioral targeting (BT) has quickly become one of the central, yet most controversial, vehicles for reaching consumers in the digital age. Critics' calls for its restriction run parallel to marketers' statements about its crucial nature as a lifeline for the new media age. Yet the arguments about the process, which include claims about public attitudes, discuss it as if it is a single act, when it is really made up of many parts that can and should be evaluated separately from a public interest standpoint. To help with that evaluation, policymakers, social advocates, and marketers need public-opinion benchmarks about the distinct yet related activities that make up the process.

With that goal in mind, this study for the first time disentangles Americans' attitudes toward tailored content from their opinions about three common behavioral tracking methods. Behavioral tracking involves following an individual's activities over time and the using the information to select which advertisements to display to that individual. Advertisers believe the practice helps them deliver their persuasive messages to audiences who are most likely to be interested. Tailoring of content involves the creation or alteration of media material to suit marketers' perceived interests of an individual or individuals.

This study concerns three types of companies—websites, advertising networks, and offline retailers—that carry out contemporary behavioral targeting. Websites closely follow the movements of visitors—for example, what articles they read, what ads they clicked, what products they started to buy but didn't purchase. The site can serve up ads to the person based on the topic selected—for example, a movie ad if the person is viewing movie reviews. The sites can also save the records of these actions and link them to the visitor by placing identifying text files called *persistent cookies* on the visitor's computer. When a user of that computer returns, the site can serve relevant advertisements based on the visitor's previous activity patterns. For example, if the past visits indicate particular attention to newspaper site's travel section, the website can serve ads from its travel advertisers to that visitor.

Advertising networks also track visitors and store their peregrinations, but across thousands, even tens of thousands, of websites that accept ads from those firms and share in the revenues. This approach means that ads served to site visitors by networks owned by Google, Yahoo, AOL,

ValueClick and many other firms may reflect a history of movements through the online world. In the most basic sense, a person who visited an auto site to search for used Mini Coopers might find himself shown a Mini Cooper ad on a newspaper site he visits the next day if the newspaper is part of the same advertising network.

Offline retailers also track visitors, most often through frequent shopper cards. As in the online world, supermarkets and drug stores may use the data to selectively send advertisements to different cardholders based on the different shopping experiences. The stores may also present special prices and shopping experiences to individuals whom they identify while they are in the stores. The Stop-and-Shop supermarket chain, for example, has experimented with giving people carts with devices activated by their frequent-shopper cards to which they can email shopping lists and which present them with offers based on past and present shopping behavior. Beyond bringing digital technology to the physical store, merchants are also merging the data they have about their customers from the web, the phone, and the store floor in an attempt to get a unified view of individual customers' behavior.

Websites, advertising networks, and offline retailers often rely on database technology companies to help them carry out behavioral targeting in the most sophisticated ways possible. One such firm, Audience Science, states that its work involves “recording billions of behavioral events daily and reaching over 385 million unique Internet users” who then make the data available to its clients: “Web publishers, marketers, networks, exchanges, and agencies to create intelligent audience segments to connect people with relevant advertising driving the transition to data-driven audience marketing online.”¹ To further enhance their knowledge of individual customers, offline stores and individual websites often go beyond tracking behavior to explore the backgrounds of members of their audience who seem to be particularly good prospects for sales or to present to advertisers. Over the past few decades, the sale and purchase of information on individuals has become big business. American privacy law is sectoral, meaning that certain businesses are restricted from selling information without consumer consent, but those rules apply in limited circumstances. Generally, companies have virtually free rein to use data in the U.S. for business purposes without their customers' knowledge or consent. Websites and stores can therefore easily buy and sell information on valued visitors with the intention of merging behavioral with demographic and geographic data in ways that will create social categories that advertisers covet and target with ads tailored to them or people like them.

Unlike individual websites and offline retailers, however, advertising networks today typically don't know the names or postal addresses of the people they track across the web. The networks consequently can't buy personally identifiable data about them. They have, however, parlayed the desire to know consumers' personalities and demographics into major enterprises to connect the millions of information dots they have about their users in ways that will appeal to advertisers. Complex dot-connecting formulas are used by ad networks of Google, Yahoo, AOL, Value Click and other firms to label millions of people according to categories that reflect inferences about gender—whether a person's search habits are feminine or masculine—as well as lifestyle and

personality—for example, whether a person is a soccer mom and/or world traveler. Ad networks still hold rather few geographic, demographic, and psychographic and lifestyles categories about individual web users. Nevertheless, the knowledge in these networks is growing and the tracking is spreading beyond the web to mobile handsets and television set-top boxes.

The reason websites, advertising networks and offline retailers are so intent on keeping track of their visitors has to do with the desire to tailor the messages that they deliver. Many advertisers believe that learning customers' present and past browsing and shopping habits can suggest what products would appeal to them and what advertising messages will catch their attention. Just as the process of making inferences about consumers is proceeding apace, so the technology to tailor commercial messages to them is becoming increasingly efficient across a variety of digital media, including television. Coupons are already tailored for individuals in physical stores, websites, and mobile handsets based on data-driven shopping, traveling and demographic patterns. And although advertisers' contemporary focus is on ads and coupons, it is also possible to present people with different offerings of entertainment and news based on analyses of their interests or their marketing profiles—starting with the kinds of recommendation engines characterized by Amazon.com and going far beyond them. News and entertainment distributors may increasingly explore the proposition that tailoring material—even just headlines and promotional materials—based on what they have learned from tracking audiences will encourage return visitors who will provide yet more information to use for targeting ads to them. Technology companies such as Visible World already offer technology that can insert products into television entertainment programs in real time based on information about the family that their cable company has placed into their set boxes based on their viewing behaviors and additional information the firm has learned about them.

Critics and Defenders

Critics of behavioral targeting complain that it is wrong to gather so much data about individual Americans, create dossiers about them without their awareness, and use the data to surround them with ads based on social and consumer categories that the citizens have not validated and might not agree with. While deleting one's browser cookies is often recommended as a quick fix for preventing tracking, it's a practice users must repeat often because websites place new cookies at each new visit. In addition, an increasing number of websites are installing *Flash cookies*, which also allow site visits to be tracked. More than half of the internet's top websites use them, according to a recent UC Berkeley study led by Ashkan Soltani and Chris Hoofnagle.² Also known as local shared objects (LSOs), Flash cookies are stored in connection with the Adobe Flash player and cannot be erased through the cookie privacy controls in a browser. In order to delete Flash cookies on a user's computer, a user must visit Adobe's website and use an online settings manager tool.³ The consequence, noted a *Wired* magazine article, is that “even if a user thinks they have cleared their computer of tracking objects, they most likely have not.” Moreover, sites have even begun to use the Flash cookies as backups to reinstate traditional cookies that a user deleted, a process that is called *re-spawning*.

Calls for an opt-in approach whereby individuals would have to consent to being tracked, are often dismissed by the advertising industry as unrealistic. Demands to let users opt out have met with half-hearted assent. Companies that allow opt out possibilities often make it hard for consumers to learn how to do it. Regardless, when a consumer clears his or her browser cookies, any opt out cookies are erased along with regular cookies, putting consumers in an impossible bind between refusing to allow cookies (causing most websites to be completely unusable), or deleting unwanted cookies manually, one by one. The difficulty even applies to sites belonging to the National Advertising Initiative's Opt-Out Program: Note 11 of its FAQ points out that "If you ever delete the 'opt-out cookie' from your browser, buy a new computer, or change Web browsers, you'll need to perform the opt-out task again."⁴ Note, too, that in some cases opting out of advertising does not prevent websites from tracking. Instead, it stops them from sending tailored ads. If one conceives of the privacy objection to online advertising as related to tracking, opting out does nothing to quell that concern.

TRUSTe, a company that promotes privacy practices and a related approval seal to websites as a way to gain consumer confidence, noted in March 2009 that "Behavioral advertising still represents uncharted territory, without clearly applicable laws or regulations." In February 2009, the Federal Trade Commission (FTC) published guidelines for companies collecting behavioral data of web users with the aim of presenting tailored advertising to them. The principles encourage transparency and customer control, security of customer data and the retention of customer information for a limited period.⁵ Seemingly in response to such pressure, Google now allows visitors to its site to learn the categories it identifies with their browser's cookie, and to opt out of such cookie-linking if they wish. Google's "permanent opt-out" process takes several steps, however, and neither Google nor any other major company explains where it received such information, how it arrived at its conclusions, or gives people the right to challenge what they consider misperceptions.⁶ In fact, as *Wired* magazine noted in August 2009, the attempts at self-regulation by the online tracking and advertising industry "have conspicuously failed to make the industry transparent about when, how and why it collects data about internet users."⁷

A key reason advertising executives have held back allowing transparency and offering consumers choices regarding behavioral tracking might be the activity's immense value—it is "the future in digital advertising," in the words of a TRUSTe executive⁸—together a parallel concern that consumers would opt out if they learned about it. *New York Times* reporter Louise Story put their dilemma concisely:

Underscoring all the debates about online privacy, behavioral targeting and Internet advertising is a hard, cold reality: content costs money. . . .

As mass advertising dies, there is more pressure for media companies to develop audiences with more specific interests and characteristics. From an economic standpoint, the drop in the total number of eyeballs means the eyeballs that remain must become more lucrative.

Media companies are also using targeting, often called behavioral targeting, to provide more valuable eyeballs. . . .⁹

Marketing executives typically justify behavioral targeting by making two claims related to tailoring and tracking. The first is that Americans want advertisements tailored to their interests; implicitly this requires learning about them through tracking their behavior. The other assertion is that only older consumers worry about the privacy issues related to behavioral tracking.

The notion that the younger generations really don't care about tracking was repeated recently by Disney CEO Robert Iger who told a July 2009 Fortune Brainstorm Tech conference that media companies should use individual tracking data to target ads and that younger people "don't care" about the privacy aspects around this. "Kids don't care," Iger said, adding that his own adult children "can't figure out what I'm talking about" when he asks them about their online privacy concerns.¹⁰

Iger went on to herald the value for Disney of using tracked data to tailor ads: "If we know that you've gone online and looked at five different autos online, you are a great consumer for us to serve up a 30-second ad for a car," he said. To marketers, it is self-evident that consumers want customized commercial messages. Typical of this claim for tailoring is the perspective of an executive at customer-relationship-management firm Dunnhumby USA. He notes that "Something amazing happens when marketing efforts are actually relevant to people. We see this step as initiating that crucial dialogue. And shoppers, for their part, are replying; essentially giving their permission to marketers to learn their habits and respond accordingly."¹¹ Reflecting that assumption, AudienceScience states that its "sophisticated behavioral targeting technology enables the company to improve its user experience by making the ads shown more relevant to each viewer, as well as offer its advertisers a higher level of engagement and return."¹² Similarly, Google's light description for the public of its AdSense contextual and behavioral advertising program states that "It's our goal to make these ads as relevant as possible for you. While we often show you ads based on the content of the page you are viewing, we also developed new technology that shows some ads based on interest categories that you might find useful."¹³ And the National Advertising Initiative, in its web page that allows opting out of member advertising networks, informs visitors thinking about the decision in bold type that "Opting out of a network does not mean you will no longer receive online advertising. It does mean that the network from which you opted out will no longer deliver ads tailored to your Web preferences and usage patterns."¹⁴

The Right Questions of the Right Samples

The advertising industry's stress on the utility of behavioral targeting for Americans because they enjoy relevant advertising raises a number of basic questions: First, do Americans in fact want advertisers to tailor advertising to their interests? Second, if they say they want tailored advertising, would they continue to want it when told that it results from following their activities—for example,

on individual websites, across websites, and in physical stores? And is it indeed the case that younger American adults tend not to be concerned about tracking and tailoring?

Prior to the research reported here, we did not have straightforward answers to these separate questions. Several studies do show strong concern for internet privacy among Americans and a desire for firms not to collect information about them online. It seems clear, too, that Americans value the right to opt out from this sort of collection. For example, in a 2008 national telephone survey, Consumers Union found that 72% of Americans 18 years and older “want the right to opt out when companies track their online behavior.” But regarding Americans’ response to behavioral targeting and tailoring, the findings are less clear. As far as we can tell the only publicly available studies on the subject are from a 2008 survey by TRUSTe that was repeated in 2009 and a 2009 survey from the Privacy Consulting Group, led by Alan Westin. Both suffer from a number of conceptual and methodological problems which we had to consider when developing our own questions and methods.

TRUSTe’s questionnaire, fielded two years in a row by TNS, asked about behavioral targeting and tailoring in a way that asked respondents whether they agreed or disagreed with a statement about both activities that also added the promise of anonymity: “I am comfortable with advertisers using my browsing history to serve me relevant ads, as long as that information cannot be tied to my name or any other personal information.” In response, about 57% said they either strongly agreed (18%) or agreed (39%). The Westin study, conducted by Harris Interactive online, also posed a standalone question about how “comfortable” people felt with behavioral targeting and tailoring: “As you may know, websites like Google, Yahoo! And Microsoft (MSN) are able to provide free search engines or free e-mail accounts because of the income they receive from advertisers trying to reach users on their websites. How comfortable are you when those websites use information about your online activity to tailor advertisements or content to your hobbies or interests?” Westin found that 59% said they were uncomfortable, with younger people (18-24 and 25-29) having lower percentages than older people—though still over 50%. Westin then asked people to assume that “websites” adopted four stringent privacy and security policies (explaining how the tailoring process would work, offering choices of tailoring, safeguarding information, and promising not to share any user’s name or address) and found that now most people apart from those 63+ were “comfortable” with behavioral targeting and tailoring. Still, the percentages “not comfortable” despite these stringent standards were substantial—38% for 18-31 year olds, 44% for 32-43 year olds, 48% for 44-62 year olds and 54% for those 63+.

Both surveys have the major limitation of being online investigations in which people responded to ads to partake in the companies’ research. The survey firms acknowledge that the sample is not representative and no confidence levels can be presented. The particular nature of the topic of this survey makes the findings particularly suspect. One might worry that people who volunteer to participate would feel less concerned about companies using their data online than would a representative sample of adults who use the internet but would not volunteer for an online survey. Another drawback to emphasize is that both these surveys combined two ideas into one question:

the issue of whether sites should serve tailored content and whether the tailoring should be based on a certain kind of tracking. A further problem is that both surveys say nothing about the particular nature of the targeted behavior. Westin's explanation of tracking said "those websites use information about your online activity," while TRUSTe described it as "using my browsing history." Neither is specific about whether the tracking takes place on a particular website or across websites, and neither suggests the possibility that data collected offline might be used to serve tailored ads. The latter is an increasing activity that is beginning to receive attention from policymakers.

It is also important to know whether Americans consider the very idea of tailored advertising a good idea, irrespective of how data are collected. To justify behavioral targeting, marketers in recent months been insisting that Americans do in fact want tailored ads. Westin's report suggests that people would want tailored advertising if the four FTC self-regulatory policies were observed. The TRUSTe study uses responses to a statement having nothing to do with tailoring—"If given the option, I would choose to only see online ads from online stores and brands that I know and trust"—to conclude that "individuals want their advertising to be more relevant."

Marketing executives who speak to the trade press tend to take for granted that Americans want tailored ads because they are relevant ads. So, for example, a Facebook executive recently noted that "there is nothing controversial" about using member profiles and wall postings to create tailored ads for them. "The controversy," he added "comes in when a user's behavior without their knowledge is tracked across the internet, which is not something we do."¹⁵ The contention underscores the point that tailoring can take place through a variety of methods other than behavioral targeting. It also raises key questions: Do Americans consider tailoring of advertising, discounts or news suited their interests to be a service they appreciate? Separately, do Americans accept behavioral tracking as the means for providing that tailored content?

The Study and the Population

We explored these questions as part of a larger survey of Americans' opinions about and understanding of a variety of online and offline privacy issues. We cast our population net broadly. We included people in our study if they were 18 years or older said yes to one of the following questions: "Do you go on online or use the internet, at least occasionally?" and "Do you send or receive email, at least occasionally?"

The survey questions we included in this report focus on four areas. One explores Americans opinions about tailored content and three different forms of behavioral tracking. A second investigates people's knowledge of rules of the marketplace when it comes to sharing information in the online and the offline world. A third area of questions asks Americans their opinions about laws that might associate with the tracking their information as well as misusing their information. And a fourth area inquires into people's beliefs about their control over their personal information, whether businesses "handle the personal information they collect about consumers in a proper and

confidential way” and whether they believe “existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.”

The survey was conducted from June 18 to July 2, 2009 by Princeton Survey Research Associates International. PSRA conducted telephone interviews with a nationally representative, English-speaking sample of 1,000 adult internet users living in the continental United States. A combination of landline (n=725) and wireless (n=275) random digit dial (RDD) samples was used to represent all adults in the continental United States who have access to either a landline or cellular telephone. The interviews averaged 20 minutes. Based on a 7-callback procedure and using the American Association of Public Opinion research (AAPOR) RR3 method, a standard for this type of survey, the overall response rates were a rather typical 18 percent for the landline sample and 22 percent for the cellular sample. Statistical results are weighted to correct known demographic discrepancies.* The margin of sampling error for the complete set of weighted data is ± 3.6 percent at the 95% confidence level. The margin of error is higher for smaller subgroups within the sample.

Table 1 provides an introductory snapshot of the population we interviewed. As Table 1 indicates, women slightly outnumber men; 78% designate themselves as White; 9% identify themselves as blacks or African American; Asian Americans make up 4%; and Native Americans comprise about 1%. Hispanics (white and black) comprise about 11% of the sample. About 56% are under age 45 and 53% are married. Most have at least some higher education, and 33% report over \$75,000 household income while 21% list it as below \$30,000; 10% refused to reveal their household income.

Rejecting Tailored Content and Behavioral Tracking

The telephone interviewer asked all these people the following questions in a randomly rotated manner:

- Please tell me whether or not you want the websites you visit to show you ads that are tailored to your interests

* A two-stage procedure was used to weight this dual-frame sample. A first-stage weight was applied to account for the overlapping sample frames. The first stage weight balanced the phone use distribution of the entire sample to match population parameters. The phone use parameter was derived from an analysis of the most recently available National Health Interview Survey (NHIS) data along with data from recent dual-frame surveys. (See Blumberg SJ, Luke JV, “Wireless substitution: Early release of estimates from the National Health Interview Survey, July-December, 2008.” National Center for Health Statistics. May 2009.) This adjustment ensures that the dual- users are appropriately divided between the landline and cell sample frames.

The second stage of weighting balanced total sample demographics to population parameters. The total sample was balanced to match national population parameters for sex, age, education, race, Hispanic origin, region (U.S. Census definitions), population density, and telephone usage. The basic weighting parameters came from a special analysis of the Census Bureau’s 2008 Annual Social and Economic Supplement (ASEC) that included all households in the continental United States. The population density parameter was derived from Census 2000 data. The telephone usage parameter came from the analysis of NHIS data.

Table 1: Characteristics of U.S. Adults in Sample (N=1,000)*

	%
Sex	
Male	48
Female	52
Age	
18-24	14
25-34	21
35-49	30
50-64	26
65-89	9
Race	
White	78
Black or African American	9
Asian or Pacific Islander	4
American Indian or Alaskan Native	1
Mixed Race	2
Other/Don't Know/Refused	6
Hispanic or Latino Background?	
Yes	11
No	88
Don't Know/Refused	1
Household Income	
Under \$30,000	21
\$30,000 to under \$50,000	19
\$50,000 to under \$75,000	17
\$75,000 and Over	33
Don't Know/Refused	10
Region of the Country	
Northeast	19
Midwest	22
South	33
West	26

*When the numbers don't add to 100% it is because of a rounding error.

- Please tell me whether or not you want the websites you visit to give you discounts that are tailored to your interests.
- Please tell me whether or not you want the websites you visit to show you news that is tailored to your interests.

If a subject answered “yes” to any of the above questions about ads, discounts, and news, its corresponding question below as then asked:

- Would it be OK or not OK if these ads [discounts/news] were tailored for you based on following what you do on the website you are visiting?
- Would it be OK or not OK if these ads [discounts/news] were tailored for you based on following what you do on OTHER websites you have visited?
- Would it be OK or not OK if these ads [discounts/news] were tailored for you based on following what you do OFFLINE—for example, in stores?

The interviewer also asked a general question about the acceptability of behavioral tracking for the purpose of tailored ads if the tracking is anonymous. The lead-up to the question noted that marketers “often use technologies to follow the websites you visit and the content you look at in order to better customize ads.” The interviewer then asked whether the respondent would “definitely allow, probably allow, probably NOT allow, or definitely not allow advertisers” to “follow you online in an anonymous way in exchange for free content.”

Tables 2 and 3 present the findings. Table 2 shows that fully 66% of the respondents do not want advertisements tailored for them. The proportions saying no are lower when it comes to tailored discounts and news, but they still represent around half the population—49% and 57% respectively.

Table 3 shows whether people who said yes to tailored ads, discounts or news continued to say they wanted the tailored content when the interviewers told them the three ways that the information the facilitate tailoring would be gathered. Two interesting patterns show up. One is that for each topic—ads, discounts, and news—the increase in the proportion of people saying no was substantially lower when told that the tracking would take place “on the website you are visiting” compared to tracking based on “*other* websites you have visited” and on “what you do *offline*—for example, in stores.” Another notable pattern is for advertisements, discounts, and news, around 80% of the respondents reject tailoring either outright or when they learn they will be followed at other websites or offline.

So, for example, 66% of the 1,000 respondents said no to tailored ads before being told about the forms of tracking. When told the tailored advertising would be based on following them on other websites they have visited, 18% *more* of those 1,000 respondents said no to tailored advertising. That means that 84% of the respondents rejected tailored ads outright or when they found out it would

Table 2: Please Tell Me Whether Or Not You Want Websites You Visit to . . . (N=1,000)*

	No, Would Not (%)	Yes, Would (%)	Maybe, DK (%)
Show you <i>ads</i> that are tailored to your interests.	66	32	2
Give you <i>discounts</i> that are tailored to your interests.	49	47	4
Show you <i>news</i> that is tailored to your interests.	57	40	3

*See text for explanation. DK=Don't Know

Table 3: Would It be OK or not OK if . . . (N=1,000)*

	OK (%)	Not OK (%)	Maybe/ DK (%)	Didn't Want Tailoring (%)	Not OK + Didn't Want Tailoring (%)
<i>these ads were tailored for you based on following</i>					
what you do on the website you are visiting.	24	7	3	66	73
what you did on <i>other</i> websites you have visited.	13	18	3	66	84
what you do <i>offline</i> —for example, in stores.	11	20	3	66	86
<i>these discounts were tailored for you based on following</i>					
what you do on the website you are visiting.	34	13	4	49	62
what you did on <i>other</i> websites you have visited.	18	29	4	49	78
what you do <i>offline</i> —for example, in stores.	18	29	4	49	78
<i>this news was tailored for you base on following</i>					
what you do on the website you are visiting.	25	14	4	57	71
what you did on <i>other</i> websites you have visited.	14	26	3	57	83
what you do <i>offline</i> —for example, in stores.	12	28	3	57	85

*See text for explanation. DK=Don't Know

happen through tracking them on other sites. The corresponding numbers for discounts and news are 78% and 83%, respectively.

Assurance of anonymous tracking doesn't seem to lower Americans' concerns about behavioral targeting. They are quite negative when it comes to the general scenario of free content supported by tailored advertising that results from "following the websites you visit and the content you look at" in a manner that keeps them anonymous. 68% definitely would not allow it, and 19% would probably not allow it. 10% would probably allow, and only 2% would definitely do it; 1% say they don't know what they would do.

Differences by Age

Americans' negative response to tailored ads, discounts, and news goes up with age in a statistically significant manner (Rho = -.24, -.22, and -.12 respectively). When we divide age into traditional marketing categories, however, we find that only the differences in ads and discounts emerge as statistically significant. Through cruder than the statistically significant correlations, the categorical approach allows us to see sharp variations between familiar social groupings. The spread is most pronounced between young adults and seniors. Specific comparison of these two groups revealed their differences are significant statistically across all three forms of content. As Table 4 shows, 55% of Americans 18 and 24 years old say no to tailored advertising, 37% say no to tailored discounts, and 54% reject tailored news. By contrast, among Americans over 65 the numbers are 82%, 70%, and 68% for ads, discounts, and news.

Note that while younger Americans are more welcoming of tailored content than are older ones, well over half of young adults nevertheless do say no to tailored advertising and news. Moreover, the percentage of young adults saying no to the three forms of tailored content becomes substantially higher when we include those who said yes to tailoring alone but then balked when told that their actions would be tracked in order for tailoring to be implemented. Tables 5-7 display the age breakdowns regarding the respondents who said *Not OK* or *OK* to tailoring and tracking. (We left out the 3% or 4% that answered *maybe*, *it depends*, or *don't know*). As Table 5 indicates, 67% of the 18-24 year old Americans say they do not want tailored advertising when we include those saying it is not OK to tailor for them based on what they do on the website they are visiting. 86% of 18-24 year olds say they don't want tailored ads when we include those saying it is not OK to tailor for them based on tracking on "other websites" they have visited. The rejection of tailored content goes up to 90% when what they do "offline—for example, in stores"—is the behavioral-tracking method.

Tables 6 and 7 show that the percentages of young adults saying no to tailored discounts and news are also quite high when we take into account those who say no to the types of behavioral-tracking. Looking across all the age groups, we see that not all the differences between them are significant statistically. Nevertheless, three broad patterns do emerge:

Table 4: Please Tell Me Whether Or Not You Want Websites You Visit to Show You Ads/Discounts/News That Are Tailored To Your Interests.*

	Age 18-24	Age 25-34	Age 35-49	Age 50-64	Age 65-89	Total
Tailored Ads*						
No	55	59	67	77	82	66
Yes	45	41	33	23	18	34
Tailored Discounts*						
No	37	44	50	58	70	51
Yes	64	56	50	42	30	49
Tailored News						
No	54	52	57	62	68	58
Yes	46	48	43	38	32	42

* Using the Chi² statistic, the differences are significant at the .05 level. The table excludes the small percentages that said *Don't Know* or *Maybe*. See text for further explanation.

Table 5: Saying *Not OK* or *OK* to Ads Tailored Based on Age and Three Tracking Activities[§]

.. based on	Age 18-24	Age 25-34	Age 35-49	Age 50-64	Age 65-89	Total
“the website you are visiting”*						
Not OK	67	70	72	82	87	75
OK	33	30	27	18	13	25
“other websites you have visited”						
Not OK	86	82	86	91	95	87
OK	14	18	14	9	5	13
“what you do offline—for example, in stores.”						
Not OK	90	88	86	92	95	89
Not OK	10	12	14	8	5	11

[§]*Not OK* includes those who said no to tailored advertising at the outset. The table excludes the small percentages that said *Don't Know* or *Maybe*. See text for further explanation. *Using the Chi² statistic, the differences are significant at the .05 level.

Table 6: Saying *OK* or *Not OK* to Discounts Tailored Based on Age and Three Tracking Activities[§]

..based on -	Age 18-24	Age 25-34	Age 35-49	Age 50-64	Age 65-89	Total
“the website you are visiting”*						
Not OK	61	58	62	74	81	66
OK	39	42	38	26	19	34
“other websites you have visited”*						
Not OK	77	76	80	86	90	81
OK	23	24	20	14	10	19
“what you do <i>offline</i> — for example, in stores.”*						
Not OK	74	80	80	86	91	82
OK	26	20	20	14	9	18

Table 7: Saying *OK* or *Not OK* to News Tailored Based on Age and Certain Tracking Activities[§]

..based on -	Age 18-24	Age 25-34	Age 35-49	Age 50-64	Age 65-89	Total
“the website you are visiting”						
Not OK	68	73	72	77	85	74
OK	32	27	28	23	15	26
“other websites you have visited”*						
Not OK	79	82	85	90	94	85
OK	21	18	15	10	6	15
“what you do <i>offline</i> — for example, in stores.”						
Not OK	84	85	85	91	96	87
OK	16	15	15	9	4	13

[§] In Tables 6 and 7, *Not OK* includes those who said no to tailored advertising at the outset. The table excludes the small percentages that said *Don't Know* or *Maybe*. See text for further explanation. *Using the Chi² statistic, the differences are significant at the .05 level.

- In the tables where the comparisons are statistically significant, older groups of Americans reject tailoring and the forms of behavioral tracking in higher percentages than do groups of younger Americans.
- All age groups have somewhat more tolerance for tailoring and behavioral tracking when carried out for discounts than when carried out for advertisements and news.
- Every age group has somewhat more tolerance for behavioral tracking when carried out on the website they are visiting compared to when carried out on other websites or offline, as in stores.

These interesting distinctions should not let us lose sight of the overarching finding: *When we combine Americans who reject tailored content outright with those who said they would want it but changed their minds when told of one or another form of tracking that would yield the tailored content, we find that substantially over 60% of all groups—and often over 80%—say no to the activity.* That includes the younger Americans who marketing executives have asserted don't care about being tracked as long as they can get relevant content.

Attitudes Toward Tailored Ads By Privacy Experience, Institutional Confidence, And Privacy Knowledge

Because of current policy interests in advertising-related behavioral targeting, we sought to understand whether Americans' acceptance or rejection of toward tailored advertising related to three aspects of their lives—bad experiences they might have had with information theft, their confidence in the way businesses and the law handle their information, and their knowledge of laws that relate to whether or not firms can sell their information in the online and offline worlds. We defined “bad privacy experiences” as ever having had one or more of the following happen: someone “used or revealed personal information about you without your permission” (it happened to 39%), someone “made a purchase on your credit card or opened a new credit card in your name without your permission” (that happened to 28%), and you “receive a notice in your postal mail that your personal information has been lost or stolen—for example, in a security breach” (it happened to 31%). We defined confidence in business and law through three statements noted in Table 8 that are borrowed from privacy researcher Alan Westin.¹⁶ And we defined online and offline knowledge via the true-false questions in Table 8.

Each of these areas in itself provides an important insight into Americans' relation to their personal information. Further analysis of the answers revealed that 38% of Americans have never had one of the bad privacy experiences noted, 32% have had one experience, 21% have had two, and 9% have had all three. We also found that 47% of our respondents agree and 20% agree strongly that “consumers have lost all control over how personal information is collected and used by consumers.” Despite these bad experiences and a belief that they have no control over their personal information, Americans have confidence that businesses and laws do protect them: 53% of our respondents agreed and 5% agreed strongly that “most businesses handle the personal

information they collect about consumers in a proper or confidential way.” Most also express confidence in “laws and organizational practices,” with 50% agreeing and 4% agreeing strongly that they “provide a reasonable level of protection for consumer privacy today.”

Part of the reason that majorities believe that businesses or laws protect them may well be because Americans mistakenly assume that laws do not allow businesses to sell personal information . Table 9 shows that, in fact, a substantial majority does not know the correct answers to most true-false statements about companies’ rights to share and sell information about them online and off. Further analysis revealed that individual respondents on average answered only 1.5 of the 5 online statements and 1.7 of the 4 offline statements correctly.

The score on the online or offline privacy indexes—that is, knowledge a person has about privacy law—has no statistical relationship with whether or not a person will agree to tailored ads. Likewise, having one or more bad privacy experiences does not associate with being for or against receiving tailored ads. By contrast, beliefs about personal control and social protection do make a difference, as Table 10 indicates: Agreeing that consumers have lost all control over personal information is significantly associated with not wanting tailored advertising. And having confidence that companies and existing laws protect people increases the statistical likelihood that that a person will want tailored advertising.

Asserting Rights Around Behavioral Tracking

Shifting attention from tailored content to behavioral tracking of people online and off, Table 11 presents the responses to five questions about an individual’s opinions about laws that ought to apply to firms’ behavioral tracking. Large majorities share the same views:

- 69% feel there should be a law that gives people the right to know everything that a website knows about them.
- 92% believe there should be a law that requires “websites and advertising companies to delete all stored information about an individual, if requested to do so.”
- 63% believe advertisers should be required by law to immediately delete information about their internet activity.
- 70% stated that a company should be fined more than the maximum amount suggested (\$2,500) “if a company purchases or uses someone’s information illegally.”

The responses about the maximum fine suggested a level of indignation, even anger, by the public when it comes to misusing information. More evidence of this reaction can be seen in the belief by 18% that a company that uses a person’s information illegally should “be put out of business” and the additional 35% who agree that “executives who are responsible should face jail time.” (See Table 12.)

Table 8: Americans' confidence in the way businesses and the law handle their information
(N=1,000)

	Strongly Agree (%)	Agree (%)	Disagree (%)	Strongly Disagree (%)	DK (%)
Consumers have lost all control over how personal information is collected and used by companies.	20	47	27	4	2
Most businesses handle the personal information they collect about consumers in a proper and confidential way.	5	53	32	6	4
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	4	50	34	8	4

DK=Don't Know

Table 9: Americans' Knowledge of Laws Online and Offline* (N=1,000)

Online:	<i>False*</i> (%)	True (%)	DK (%)
If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission.	22	62	16
If a website has a privacy policy, it means that the site cannot give your address and purchase history to the government.	46	26	28
If a website has a privacy policy, it means that the website must delete information it has about you, such as name and address, if you request them to do so.	20	54	26
If a website violates its privacy policy, it means that you have the right to sue the website for violating it.	19	46	35
If a company wants to follow your internet use across multiple sites on the internet, it must first obtain your permission.	48	33	19
Offline:			
When you subscribe to a newspaper or magazine by mail or phone, the publisher is not allowed to sell your address and phone number to other companies without your permission.	49	36	15
When you order a pizza by phone for home delivery, the pizza company is not allowed to sell your address and phone number to other companies without your permission.	31	44	25
When you enter a sweepstakes contest, the sweepstakes company is not allowed to sell your address or phone number to other companies without your permission.	57	28	15
When you give your phone number to a store cashier, the store is not allowed to sell your address or phone number to other companies without your permission.	33	49	18

*For each statement, *false* is the correct answer.

Table 10: Americans' Desire For Tailored Ads Based on Confidence In The Way Businesses And The Law Handle Their Information

Please tell me whether or not you want websites you visit to show you ads tailored to your interests. ▶	No, would Not (%)	Yes, Would (%)
<hr/>		
Consumers have lost all control over how personal information is collected and used by companies.*		
Agree	71	29
Disagree	60	40
<hr/>		
Most businesses handle the personal information they collect about consumers in a proper and confidential way. *		
Agree	61	39
Disagree	77	23
<hr/>		
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.*		
Agree	61	39
Disagree	76	24

* Using the Chi² statistic, the differences are significant at the .05 level.

Table 11: Asserting Rights Around Behavior Tracking

	N=1,000 (%)
<i>Do you think there should be a law that gives people the right to know everything that a website knows about them, or do you feel such a law is not necessary?</i>	
Yes, there should be a law	69
No, a law is not necessary	29
DK	2
<i>Do you think there should be a law that requires websites and advertising companies to delete all stored information about an individual, if requested to do so.</i>	
Yes, there should be a law	92
No, a law is not necessary	7
DK	1
<i>Advertisers would like to keep and store information about your internet activity. How long should they be able to keep it? Do you think--</i>	
They should have to delete it immediately, OR	63
They should be allowed to keep it for a few months, OR	25
They should be allowed to keep it for a year, OR	6
They should be allowed to keep it for as long as they want	4
DK	2
<i>If a company purchases or uses someone's information illegally, about how much—if anything—do you think that company should be fined?</i>	
\$100	2
\$500	4
\$1,000	9
\$2,500	7
More than \$2,500	70
It depends	4
DK	4
<i>Beyond a fine, companies that use a person's information illegally might be punished in other ways. Which one of the following ways to punish companies do you think is most important?</i>	
The company should fund efforts to help people protect privacy	38
Executives who are responsible should face jail time	35
The company should be put out of business	18
The company should not be punished in any of these ways	3
It depends	2
DK	4

DK=Don't Know

Table 12: “Beyond a fine, companies that use a person’s information illegally might be punished in other ways. Which *one* of the following ways to punish companies do you think is most important?”

	N=1,000 (%)
The company should fund efforts to help people protect privacy.	38
Executives who are responsible should face jail time.	35
The company should be put out of business	18
The company should not be punished in any of these ways	3
It depends; don’t know	6

Conclusion

It is noteworthy that 38% of Americans told us that companies that use a person’s information illegally should “fund efforts to help people protect privacy.” While the choice doesn’t suggest the anger of “the company should be put out of business” or “executives who are responsible should face jail time,” it does reflect concern about the state of information privacy that is demonstrated in the answers about tailored content and behavioral tracking. Americans’ widespread rejection of relevant tailored advertising is particularly startling because it flies in the face of marketers’ consistent contention that Americans desire for relevant commercial messages justifies a variety of tracking activities. When three contemporary forms of behavioral tracking are highlighted, rejection of tailored ads is even more widespread. The finding applies across all age groups, including young adults, a cohort that media executives have insisted cares little about information privacy.

The desire by a majority of Americans not to be followed for the purpose of tailored content comes at a time when behavioral targeting is a fast-growing advertising practice upon which many content providers have staked their businesses. A mini-industry is growing up around the process, with companies such as DoubleClick, Audience Science, and Akamai following the activities of individuals in ways that yield detailed suggestions about what kinds of people they are, what that means for their perspectives on life, how that has translated into what they bought recently, and how that might transfer into the products and services they might buy in the near future. At this point the sketches are often not connected to a person’s “offline” or real name and postal address. However, a political consensus is emerging that this point hardly matters when the person’s digital trail is a treasure trove of data that marketers can use to de facto identify the individual across the internet, drawing inferences about personality, gender, location, interests, purchasing power, and more.

Our research did not inquire into why Americans do not want companies to tailor relevant advertising, discounts, or news for them. We can suggest, however, that many of them understand that behavioral targeting can lead to hidden forms of social discrimination. Many may be

uncomfortable with the realization that tailored content and tracking go hand-in-hand. They may know that these activities can lead marketers to retail policies that place them at a disadvantage compared to other consumers. They may fear receiving tailored ads for products that are not as upscale and tailored discounts that are not as generous as the ones their neighbors get. They may worry, too, that news served to them based on criteria they don't understand may separate them from views of the world received by others whom marketers judge differently.

Whatever the reasons explaining Americans' dislike of behavioral targeting, our findings indicate that they expect companies to take privacy rules extremely seriously. Our results show that Americans consumers believe (albeit mistakenly) that an array of strong laws prohibit companies from sharing or selling of data about them. Recall, too, that 70% went beyond the highest option we provided for fines resulting from illegal use of people's data, and that a substantial proportion wanted significant non-monetary sanctions, including liquidation of companies and jail time for employees. Moreover, when asked whether or not they want regulations demanding control and transparency, they say "Yes" in large proportions. 63% prefer immediate deletion of data marketers hold about them, and 25% choose the next most restrictive option—"a few months." 92% percent want a law requiring websites and advertising companies to delete all stored information upon request. While data-intensive companies have resisted calls to reduce data retention and have grudgingly accepted shorter retention times, Americans want them to go farther.

Such a strong preference for a right to delete means that consumers want a way to meaningfully object and withdraw from certain practices around the collection and use of their data. This response is not possible today short of engaging in some very disciplined internet browsing habits or refusing to use the internet at all. And even if they do opt out, their actions are still tracked, and data about their internet use can still be collected. Moving forward, policymakers must be savvy to similar self-regulatory proposals that create illusory protections. There is a real risk that future industry proposals will use technical means to ensure continued website ("first party") and cross-website or even cross-media ("third party") tracking while leading the consumer to believe that such tracking has been limited--for example, by masking third-party tracking to imply it is carried out by the first party.

This survey's findings support the proposition that consumers should have a substantive right to reject behavioral targeting and its underlying practices. Rejection could take the form of a reinvigorated opt out right that actually pertains to collection of information. It could also be implemented through a procedure to enforce an option to delete records. In fact, default rules creating opt in and opt out may be less important than time limits for keeping data. While some accommodations may need to be made for keeping data for security reasons, firms should not be able to use data for marketing purposes for periods longer than those consumers want.

In recent months, a variety of suggestions have been made in this direction by industry and advocacy groups.¹⁷ Our survey findings indicate that the most persuasive of these approaches

encourage transparency and retention limits in marketers' actions and consumers' ability to exercise control over the data companies collect about them. To these important suggestions, we would like to add a broad operating value: Companies need to *respect* their publics rather than to treat them as objects from which they can take information in order to optimally persuade them with no clear option not to participate. Traditionally the potential for harm and unwanted intrusion have been cited as justifications for protecting the privacy of people's information. Respect ought to be encouraged as a positive, trust-building reason for protecting information privacy. Respect as a value requires marketers to promote information reciprocity. That is, in return for collecting and using consumers' data, marketers should allow those consumers to learn exactly where the information came from and how it is being used. Marketers should also allow consumers to decide which of the collected data should be used and for what purposes, and which should be deleted.

Joseph Turow has suggested that marketers create a privacy dashboard that would allow consumers to interact with data the firms have collected about them.¹⁸ Beyond informing people about the information circulating about them, their interaction with data through these dashboards will do more to make the public savvy about their information and how to protect it than will wordy paragraphs and lengthy privacy policies on websites. Implementing a regime of respect around the collection and use of consumer information will not be easy. Our findings in this survey suggest, however, that such activities are imperative for a public that broadly dislikes the emerging contemporary data-gathering regime.

REFERENCES

¹ Audience Science Press Release, "AudienceScience Behaviorally Targets Video Advertising With Hulu," *Marketwire*, July 14, 2009, via Lexis Nexis.

² Ashkan Soltani et al., "Flash Cookies and Privacy," University of California School of Information, 2009, http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=1446862

³ See http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html

⁴ NAI, "FAQs," http://www.networkadvertising.org/managing/faqs.asp#question_11, accessed August 31, 2007.

⁵ Federal Trade Commission, "Self-Regulatory Principles for Online Behavioral Advertising," February 2009.

⁶ See Holly Sanders Ware, "Google Is Faulted On Privacy," *New York Post*, July 10, 2009, p. 37.

⁷ Ryan Singel, "You Deleted Your Cookies? Think Again," *Wired*, August 10, 2009.

⁸ Collin O'Malley, VP of Strategic Business at TRUSTe, in TRUSTe press release, "Behavioral Targeting: Not that Bad?!" *Marketwire*, March 4, 2009, via Lexis Nexis.

⁹ Louise Story, "Bits" *New York Times*, November 5, 2007, p. C-6.

-
- ¹⁰ Noelle McElhatton, Noelle McElhatton, Marketing Direct, July 27, 2009, <http://www.marketingdirectmag.co.uk/channel/directmarketing/article/922859/Disney-CEO-says-young-consumers-dont-care-behavioural-targeting-privacy/>, accessed September 3, 2009.
- ¹¹ Mark Wilmot, “The Welcome Mat,” *Marketing Daily*, July 28, 2009, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=110489
- ¹² Audience Science Press Release, “AudienceScience Behaviorally Targets Video Advertising With Hulu,” *Marketwire*, July 14, 2009, via Lexis Nexis.
- ¹³ Google, “Make the Ads You See More Interesting,” accessed on August 31, 2009.
- ¹⁴ National Advertising Initiative, “Opt Out of Behavioral Advertising,” http://www.networkadvertising.org/managing/opt_out.asp accessed August 31, 2009. Emphasis in original.
- ¹⁵ Mediapost, August 14, 2009
- ¹⁶ See Ponnurangam Kumaraguru and Lorrie Faith Cantor, “Privacy Indexes: A Survey of Westin’s Studies,” Carnegie Mellon University (CMU-ISRI-5-138), December 2005.
- ¹⁷ See, for example, “Online Behavioral Tracking and Targeting, Legislative Primer,” produced by the Center for Digital Democracy, Consumer Federation of America, Consumers Union, Consumer Watchdog, Electronic Frontier Foundation, Privacy Lives, Privacy Rights Clearinghouse, Privacy Times, U.S. Public Interest Research Group, and World Privacy Forum, September 2009; and Arnold and Porter, LLP, “The Great Behavioral Advertising (BA) Debate Continues,” *Consumer Advertising Law Blog*, Sept 17, 2009, <http://www.consumeradvertisinglawblog.com/2009/09/the-great-ba-debate-continues.html>
- ¹⁸ See Saul Hansell, “An Icon That Says They’re Watching You,” *New York Times*, March 19, 2009, <http://bits.blogs.nytimes.com/2009/03/19/an-icon-that-says-theyre-watching-you/>