HENRY A. WAXMAN, CALIFORNIA
CHAIRMAN

JOE BARTON, TEXAS
RANKING MEMBER

ONE HUNDRED ELEVENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225–2927
Minority (202) 225–3641

MEMORANDUM

November 30, 2010

To: Members of the Subcommittee on Commerce, Trade, and Consumer Protection

Fr: Subcommittee on Commerce, Trade, and Consumer Protection Democratic Staff

Re: Hearing on "Do Not Track Legislation: Is Now the Right Time?"

On Thursday, December 2, 2010, at 10:30 a.m. in Room 2123 of the Rayburn House Office Building, the Subcommittee on Commerce, Trade, and Consumer Protection will hold a hearing to examine the feasibility of establishing a mechanism that provides Internet users a simple and universal method to opt-out from having their online activity tracked by data-gathering firms (a.k.a. a "Do Not Track List").

I. BACKGROUND

In the Internet age, each keystroke or click of a mouse can betray the most mundane or even sensitive details of our lives, and those details are being collected and packaged into profiles by a data-gathering industry with an increasing hunger for information that can be sold and used to target consumers based on their tastes, needs, and even perceived desirability. Many Americans don't know that the details of their online lives are being gobbled up and used in this way, much less how to stop it in the event that such collection offends their expectations of privacy.

This summer, the *Wall Street Journal* began reporting about the online gathering of information about Internet users in an ongoing investigative series called "What They Know." For its first piece, the *Journal* uncovered the extent to which Internet users' activity is being tracked. The *Journal* found that visiting the top 50 most popular websites in the U.S. resulted in the placement on a single test computer of 2,224 files by 131 companies that track Internet users' activity across the Internet.[1] In addition, not only is tracking of Internet users pervasive, but it has become more invasive through the use by some in the tracking industry of more

[1] Julia Angwin & Tom McGinty, *What They Know: Sites Feed Personal Details To New Tracking Industry*, Wall Street Journal (July 30, 2010).

sophisticated technologies that can keep tabs on an Internet users activity on a website (rather than collecting just the fact that the website was visited) and some can even re-spawn themselves if an Internet user tries to delete them.[2]

This surreptitious monitoring results in detailed profiles that can include, among other things, age, gender, race, zip code, income, marital status, health concerns, recent purchases, and favorite TV shows and movies.[3] These profiles are then sold -- sometimes for a fraction of a penny each through exchanges that can sell 50 million pieces of information about Internet users' activity instantaneously each day -- for the purpose of targeting ads to particular consumers (so-called "behaviorally targeted ads").[4]

In addition, some tracking industry firms are starting to combine information about online activity with offline records to deliver an entire web experience based on statistically generated assumptions about individual Internet users.[5] As noted by the *Journal*, these firms are stripping away the anonymity of the Internet and "gaining the ability to decide whether or not you'd be a good customer, before you tell them a single thing about yourself."[6] For example, life insurance website *AccuquoteLife.com* has tested a system that would show visitors determined to be "suburban, college-educated baby-boomers a default policy of $2 million to $3 million," while visitors determined to be "rural, working class senior citizens might see a default policy for $250,000".[7] Capital One Financial Corp. has also used statistical assumptions from a tracking firm "to instantly decide which credit cards to show first-time visitors to its website."[8]

The industry contends that tracking does not pose a threat to privacy because people are not identified by name.[9] Instead, Internet users are identified by a string of numbers and

---

[2] *Id*. *See also* Julia Angwin, *What They Know: The Web's New Gold Mine: Your Secrets*, Wall Street Journal (July 30, 2010) ("Beacons . . . are small pieces of software that run on a Web page. They can track what a user is doing on the page, including what is being typed or where the mouse is moving. . . . Flash cookies can also be used by data collectors to re-install regular cookies that a user has deleted. This can circumvent the user's attempt to avoid being tracked online.").

[3] Angwin & McGinty, *What They Know: Sites Feed Personal Details To New Tracking Industry*.

[4] *Id*; Angwin, *What They Know: The Web's New Gold Mine: Your Secrets*.

[5] Emily Steel & Julia Angwin, *What They Know: On the Web's Cutting Edge, Anonymity in Name Only*, Wall Street Journal (Aug. 4, 2010).

[6] *Id*.

[7] Angwin, *What They Know: The Web's New Gold Mine: Your Secrets*.

[8] Steel & Angwin, *What They Know: On the Web's Cutting Edge, Anonymity in Name Only*.

[9] Angwin & McGinty, *What They Know: Sites Feed Personal Details To New Tracking Industry*.

letters.[10] However, according to experts in the field of re-identification science, just a few random pieces of information -- including such commonplace things as a zip code, gender, age, car model, computer operating system, and specific browser -- are enough to pinpoint a specific person.[11] Moreover, while the practice of tying information collected by tracking firms with a person's name has been a line most firms were reticent to cross, at least one firm, RapLeaf, Inc., is known to have connected both names and email addresses to profiles it maintains.[12] In addition, the use of information about people's online behavior is beginning to creep beyond the delivery of targeted ads. Life insurers are experimenting with the possibility of using detailed profiles compiled by data-collection firms from a vast array of offline and online sources -- which could include information about online behavior -- to predict potential customers' expected life span as a part of the insurance application process.[13] The life insurance industry has traditionally relied on lab analysis of bodily fluids for this purpose.[14]

The delivery of online behaviorally targeted ads is a booming business. Spending on behaviorally targeted ads reached $925 million in 2009, and that figure is expected to reach $1.125 billion by the end of 2010.[15] By 2014, spending on behaviorally targeted ads is projected to more than double to $2.6 billion.[16] In addition, those in the business of selling behaviorally targeted ads can generally command more for those ads than non-targeted ads. In 2009, advertising networks on average charged $1.98 per thousand displays of an untargeted ad, while they charged on average $4.12 per thousand displays of a behaviorally targeted ad.[17]

The revenue generated by this type of advertising helps finance the free content that many Internet users have come to expect. In fact, "more than half of ad network revenue goes to publishers who host the [targeted] ads."[18] Because of this, tracking industry proponents have argued that regulation of this industry to protect consumers' privacy could reduce the availability

---

[10] Angwin, *What They Know: The Web's New Gold Mine: Your Secrets.*

[11] Julia Angwin & Jennifer Valentino-DeVries, *The Information That is Needed to Identify You: 33 Bits*, Wall Street Journal (Aug. 4, 2010).

[12] Emily Steel, *What They Know: A Web Pioneer Profiles Users by Name*, Wall Street Journal (Oct. 25, 2010).

[13] Leslie Scism & Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients*, Wall Street Journal (Nov. 19, 2010).

[14] *Id.*

[15] David Hallerman, *Is Behavorial Targeting Outmoded?*, The eMarketer Blog (Mar. 12, 2010) (online at www.emarketer.com/blog/index.php/behavorial-targeting-outmoded/#more-2005).

[16] *Id.*

[17] Howard Beales, *The Value of Behavioral Targeting* (2009) (online at www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf).

[18] Daniel Castro, *Stricter Privacy Regulations for Online Advertising Will Harm the Free Internet*, The Information Technology & Innovation Foundation (Sept. 2010) (online at www.itif.org/files/2010-privacy-regs.pdf).

of free content on the Internet and the proliferation of more unwanted and irrelevant ads.[19] However, despite the staggering growth in revenue from behaviorally targeted ads, this revenue stream remains a small portion of the overall revenue from internet advertising. In 2009, overall revenue from all types of internet advertising was $22.661 billion, while spending on behaviorally targeted ads was $925 million.[20]

II. CURRENT LAW & SELF-REGULATORY EFFORTS

No federal law specifically governs the online advertising industry or the practice of tracking internet consumers to deliver behaviorally target ads. Nor are there any federal laws that comprehensively govern the collection, use, and dissemination of consumer information across the board.[21]

Specific federal laws, however, do address certain categories of personal information or specific entities. For example, the Fair Credit Reporting Act (FCRA) governs consumer report information,[22] Title V of the Gramm-Leach-Bliley Act addresses the sharing of certain nonpublic personally identifiable information by financial institutions,[23] and rules promulgated pursuant to the Health Insurance Portability and Accountability Act apply to the privacy of medical records.[24] In addition, the FTC may bring actions for unfair or deceptive acts or practices under the FTC Act, which includes the authority to bring actions related to a company's information collection and use.[25]

In addition, this past October a coalition of media and marketing trade associations launched a self-regulatory program for the behavioral advertising industry.[26] The voluntary

---

[19] *Id*.

[20] Interactive Advertising Bureau, *IAB Internet Advertising Revenue Report: 2010 First Half-Year Results* (Oct. 12, 2010) (online at http://www.iab.net/media/file/PwC-IAB-presentation-final.pdf); Hallerman, *Is Behavioral Targeting Outmoded?*

[21] *See generally* Congressional Research Service, *Information Brokers: Federal and State Laws* (May 5, 2006) (RL-33005); Congressional Research Service, *Privacy Law and Online Advertising: Legal Analysis of Data Gathering By Online Advertisers Such as Double Click and NebuAd* (Feb. 20, 2009) (RL-34693).

[22] 15 U.S.C. §1681 *et seq.*

[23] 15 U.S.C. §§ 6801-6809.

[24] 45 C.F.R. Part 164.

[25] 15 U.S.C. § 45(a)(2).

[26] American Association of Advertising Agencies, American Advertising Federation, Association of National Advertisers, Better Business Bureau, Digital Marketing Association, Interactive Advertising Bureau, and Network Advertising Initiative, *Major Marketing/Media Trade Groups Launch Program to Give Consumers Enhanced Control Over Collection and Use of Web Viewing Data For Online Behavioral Advertising* (Oct. 4, 2010) (online at www.networkadvertising.org/pdfs/Associations104release.pdf).

initiative began by encouraging companies that track Internet users to display on or near behaviorally targeted ads a clickable "Advertising Option Icon." Once fully implemented, the icon will signal to Internet users that an ad was served based online tracking and provide an avenue for consumers to get more information about the company's data practices and to opt-out from receiving behaviorally targeted ads served by some or all participating companies.[27]

III. H.R. 5777, the BEST PRACTICES Act

On July 19, 2010, Rep. Bobby L. Rush introduced H.R. 5777, the BEST PRACTICES Act. The purpose of this bill is to foster transparency about the commercial use of personal information and provide consumers with choice about the collection, use, and disclosure of such information. The bill applies to both the online and offline contexts.

The bill requires a covered entity to make available to individuals information about the covered entity's privacy practices, including a description of the information collected and the specific purposes for such collection. The FTC is directed to determine the means and timing of notices, may allow for or require shorter notices, and may issue model notices. A covered entity must provide an individual with the ability to opt out of the collection and use of covered information and must obtain express affirmative consent before collecting, using, or disclosing sensitive information. A covered entity that participates in a Safe Harbor Self-Regulatory Choice Program approved by FTC is not subject to certain requirements.

The bill also includes data security, access, data minimization, accountability, and accuracy requirements. The bill grants enforcement authority to the FTC and the states, including civil penalty authority, and grants the FTC streamlined rulemaking authority to implement the bill. Finally, the bill authorizes a limited private right of action and contains a preemption provision of certain state laws that expressly require covered entities to implement requirements with respect to the collection, use, or disclosure of covered information. The preemption provision does not apply to State laws that address health information or financial information, data breach laws, trespass, contract, or tort laws, and other laws that relate to acts of fraud.

H.R. 5777 does not include a provision to establish a mechanism that provides consumers a simple and universal method to opt-out from having their online activity collected and used by the tracking industry. Privacy advocates first proposed a version of such a "Do Not Track List" in 2007.[28] The growing awareness about the pervasiveness and invasiveness of online tracking has sparked renewed interest in such a mechanism by privacy advocates, and the FTC is

---

[27] *Id.*

[28] Center for Democracy and Technology, Consumer Action, Consumer Federation of America, Electronic Frontier Foundation, Privacy Activism, Public Information Research, Privacy Journal, Privacy Rights Clearinghouse, and World Privacy Forum, *Privacy and Consumer Groups Recommend "Do Not Track List" and Other Policy Solutions to Offer Consumers More Control Over Online Behavioral Tracking* (October 31, 2007) (online at www.cdt.org/pr_statement/privacy-and-consumer-groups-recommend-do-not-track-list-and-other-policy-solutions-offe).

expected to address the issue in upcoming report on online privacy.[29] The Subcommittee's hearing will examine the feasibility of establishing such mechanism.

IV. WITNESSES

The following witnesses have been invited to testify:

Panel I

Mr. Daniel Weitzner
Associate Administrator for Policy
National Telecommunications and Information Administration
U.S. Department of Commerce

Mr. David Vladeck
Director, Bureau of Consumer Protection
Federal Trade Commission

Panel II

Ms. Susan Grant
Director of Consumer Protection
Consumer Federation of America

Mr. Joseph Pasqua
Vice President of Research
Symantec Corporation

Ms. Joan Gillman
Executive Vice President and President, Media Sales
Time Warner Cable

Dr. Eben Moglen
Legal Advisor, Diaspora
Professor of Law, Columbia University
Founding Director, Software Freedom Law Center

Mr. Daniel Castro
Senior Analyst
Information Technology and Innovation Foundation

[29] Edward Wyatt & Tanzina Vega, *Stage Set for Showdown on Online Privacy*, New York Times (Nov. 9, 2010).