Written Statement of the
American Civil Liberties Union

Michael W. Macleod-Ball
Acting Director, Washington Legislative Office

Christopher Calabrese
Legislative Counsel

before the
House Energy & Commerce Committee
Subcommittee on Communications, Technology & the Internet
&
Subcommittee on Commerce, Trade & Consumer Protection

November 19, 2009

Hearing on "Exploring the Offline and Online Collection and Use of Consumer Information"

AMERICAN CIVIL LIBERTIES UNION

WASHINGTON LEGISLATIVE OFFICE
915 15th Street, NW Washington, D.C. 20005
(202) 544-1681 Fax (202) 546-0738

Written Statement of the
American Civil Liberties Union
Michael Macleod-Ball
Acting Director, Washington Legislative Office
Christopher Calabrese
Legislative Counsel
before the
House Energy & Commerce Committee
Subcommittee on Communications, Technology & the Internet
&
Subcommittee on Commerce, Trade & Consumer Protection
November 19, 2009

Chairman Boucher, Chairman Rush, Ranking Member Stearns, Ranking Member Radanovich and Members of the Committee:

On behalf of the American Civil Liberties Union (ACLU), a nonpartisan public interest organization dedicated to protecting the constitutional rights of individuals, and its half million members, activists, and fifty-three affiliates nationwide, we congratulate you for turning your attention to behavioral marketing, a widespread and often intrusive practice of tracking and using information about the online behavior of consumers. As you consider this important issue we hope you will focus not just on private actors but also government use of information collected online. For all the reasons that the collection and use of this information is intrusive when performed by individual companies, it is all the more troubling when the information is disclosed to the government. Because the existing legal framework provides little meaningful protection against this surveillance, it is vital that new laws addressing behavioral marketing also regulate the disclosure of this information to the government.

I. The data collected by behavioral marketers forms a personal profile of unprecedented breadth and depth.

As much of the testimony before your committee has already made clear,[1] behavioral advertising involves the collection of a staggering amount of information

[1] *Behavioral Advertising: Industry Practices and Consumers' Expectations: Hearing before the H. Subcomm. on Communications, Technology and the Internet of the H. Comm. on Energy and Commerce, and the H. Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 111th Cong. (2009) (Statement of Edward W. Felten, Professor of Computer Science and Public Affairs, Princeton University) *available at*

about people's online activities. At the outset this practice should be differentiated from "contextual advertising," another type of online ad service which shows ads to users based on the contents of the web page they are currently viewing or the web search they have just performed.[2] When this pairing of ads to users' interests is based only on a match between the content of an ad and a single page or search term, a website or advertising network requires no personal information about a user beyond an I.P address and the practice does not raise significant privacy concerns.[3]

As your committee hearings have demonstrated, behavioral marketers are far more ambitious and seek to form a much more complete picture of users. They do this by combining a vast amount of information gleaned from different web sites over time, including web page visits, searches, online purchases, videos watched, posts on social networking, and so on.[4] Any particular website may have little information, but when a large number of these data points are aggregated, the result is an extremely detailed picture.[5]

A striking recent development involves the potential to collect data from social networking sites like MySpace, Facebook, Twitter, and LinkedIn. A scholarly paper reports that eleven of twelve sites studied had the potential to "leak" personally identifiable information about users to third parties, including information such as name, address, phone number, gender, and birthday.[6] Approximately 90% of users did not take advantage of privacy controls to limit access by third parties, and those controls, when used, often proved ineffective against technically-savvy snoopers.[7] In the words of the Electronic Frontier Foundation, "The main theme of the paper is that when you log in to a social networking site, the social network includes advertising and tracking code in such a way that the 3rd party can see which account on the social network is yours. They can

---

http://energycommerce.house.gov/Press_111/20090618/testimony_felten.pdf (last visited October 7, 2009); *id.* (Statement of Jeff Chester, Executive Director, Center for Digital Democracy) *available at* http://energycommerce.house.gov/Press_111/20090618/testimony_chester.pdf (last visited October 7, 2009).

[2] Chester, *supra* n.1, at 3.

[3] *Id.*

[4] Felten, *supra* n.1 , at 3-4; CENTER FOR DIGITAL DEMOCRACY, ET AL., ONLINE BEHAVIORAL TRACKING AND TARGETING: LEGISLATIVE PRIMER 2009 3, *available at* http://www.uspirg.org/uploads/s6/9h/s69h7ytWnmbOJE-V2uGd4w/Online-Privacy---Legislative-Primer.pdf (last visited October 5, 2009); *see also* OMNITURE, THE RISE OF ONSITE BEHAVIORAL TARGETING 1 (May 2008) ("On-site Behavioral Targeting leverages each individual Web visitor's observed click-stream behavior, both on the current Web visit and from all previous visits, to decide what content is likely to be most effective to serve to that visitor."), *available at* http://www.omniture.com/offer/281) (last visited October 7, 2009).

[5] Felten, *supra* n.1, at 3-4; Chester, *supra* n.1, at 8-10; Electronic Frontier Foundation, How Online Tracking Companies Know Most of What You Do Online (and What Social Networks Are Doing to Help Them), Sept. 21, 2009, http://www.eff.org/deeplinks/2009/09/online-trackers-and-social-networks (last visited October 7, 2009).

[6] BALACHANDER KRISHNAMURTHY & CRAIG E. WILLS, ON THE LEAKAGE OF PERSONALLY IDENTIFIABLE INFORMATION VIA ONLINE SOCIAL NETWORKS (2009) *available at* http://conferences.sigcomm.org/sigcomm/2009/workshops/wosn/papers/p7.pdf (last visited October 6, 2009).

[7] *Id.*

then just go to your profile page, record its contents, and add them to their file."[8] Facebook recently settled a $9.5 million class action lawsuit involving its "Beacon" advertising program, which automatically creates posts on users' Facebook pages based on purchases or other actions on third-party websites.[9]

The collection of this online information is frequently being matched with real-world, offline identities. Professor Edward W. Felten testified before the committee about the process by which an online ad service might combine its user profile with information purchased from a commercial database: "If the ad service does know the identity, then third party services can provide a wealth of additional information, such as the user's demographics, family information, and credit history, which can be incorporated into the ad service's profile of the user, to improve ad targeting."[10] While Professor Felten was careful to make clear that "the fact that something is possible as a technical matter does not imply that reputable ad services actually do it,"[11] it seems likely the process is not uncommon. For example, the company Comscore, a leading provider of website analytic tools, boasts that "online behavioral data can…be combined with attitudinal research or linked with offline databases in order to diagnose cross-channel behavior and streamline the media planning process."[12]

The prevalence of online marketing is certainly growing—one online advertising CEO states that "[m]oving from site-targeting to people-targeting is the central dynamic of the industry"[13]—and consumers are increasingly concerned. A recent study from professors at the University of Pennsylvania and the University of California, Berkeley found that two-thirds of consumers objected to online tracking by advertisers, and that number rose on learning of the ways in which marketers are following their online behavior.[14]

II. Governmental access to these extensive personal profiles is possible and would be disastrous.

The issue before these subcommittees, then, is how to regulate the use of these profiles. It is no exaggeration to say these profiles—which may combine records of a person's entire online activity and extensive databases of real-word, personally identifiable information—draw a personal portrait unprecedented in scope and detail. Because the Internet has become intertwined with such personal facets our lives, the same

---

[8] EFF, *supra* n.5.
[9] *Internet Social Networking Sites Eye Privacy Expectations in Evolving Market*, BNA PRIVACY WATCH, Oct. 8, 2009 (discussing *Lane v. Facebook Inc.*, N.D. Cal., No. 08-3845).
[10] Felten, *supra* n.1 at 4.
[11] *Id.*
[12] Why Comscore?, http://comscore.com/About_comScore/Why_comScore (last visited October 6, 2009).
[13] Robert D. Hof, *Ad Networks Are Transforming Online Advertising*, BUSINESS WEEK, Feb. 19, 2009 (quoting Matt Spiegel of Omnicom Media) *available at* http://www.businessweek.com/magazine/content/09_09/b4121048726676.htm (last visited October 8, 2009).
[14] Stephanie Clifford, *Two-Thirds of Americans Object to Online Tracking*, N.Y. TIMES, Sept. 29, 2009 *available at* http://www.nytimes.com/2009/09/30/business/media/30adco.html (last visited October 8, 2009).

technology which has provided such tremendous advances also offers tremendous opportunities for government surveillance more intrusive than has ever before been possible. Imagine the government, without a warrant or any basis for individualized suspicion, reviewing records not just of what books a person had borrowed from a library, but also how she found the books, and what specific pages she read. We certainly wouldn't permit that in the offline world, and we shouldn't permit it online either.

We do not know if the government is already accessing these records, but we do know that the C.I.A., via its investment arm In-Q-Tel, has invested in a software company that specializes in monitoring blogs and social networks.[15] We also know the government has accessed, and likely continues to access, other private databases of personal information. For example, the Department of Defense, the C.I.A., and the F.B.I. have all purchased use of private databases from Choicepoint, one of the largest and most sophisticated aggregators of personal data.[16] In the words of the F.B.I., "We have the legal authority to collect certain types of information" because ChoicePoint is "a commercial database, and we purchase a lot of different commercial databases….They have collated information that we legitimately have the authority to obtain."[17]

The government has also sought access to some forms of online user data, for example the D.O.J. subpoenaed search records from Google, Yahoo!, and other search providers in order to defend a lawsuit.[18] In the words of Chris Hoofnagle, a senior fellow at the Berkeley Center for Law and Technology, "These very large databases of transactional information become honey pots for law enforcement or for litigants."[19] Given the government's demonstrated drive to access both online data and commercial databases of personal information, it seems nearly certain that law enforcement and other government actors will purchase or otherwise access the type of detailed profiles of online behavior compiled by behavioral marketers.

---

[15] Noah Shactman, *U.S. Spies Buy Stake in Firm That Monitors Blogs, Tweets*, WIRED, Oct. 19, 2009 *at* http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/ (last visited October 23, 2009).

[16] Shane Harris, *FBI, Pentagon Pay For Access to Trove of Public Records*, NAT'L J., Nov. 11, 2005, *available at* http://www.govexec.com/story_page.cfm?articleid=32802 (last visited October 7, 2009); Robert O'Harrow Jr., *In Age of Security, Firm Mines Wealth Of Personal Data*, WASHINGTON POST at A01, Jan. 20, 2005, *available at* http://www.washingtonpost.com/wp-dyn/articles/A22269-2005Jan19.html (last visited October 7, 2009).

[17] Harris, supra n.16 (quoting F.B.I. spokesman Ed Cogswell).

[18] Hiawatha Bray, *Google Subpoena Roils the Web, US Effort Raises Privacy Issues*, BOSTON GLOBE, January 21, 2006, *available at* http://www.boston.com/news/nation/articles/2006/01/21/google_subpoena_roils_the_web/ (last visited October 7, 2009).

[19] Miguel Helft, *Google Told to Turn Over User Data of YouTube*, NEW YORK TIMES, July 4, 2008 *available at* http://www.nytimes.com/2008/07/04/technology/04youtube.html (last visited October 6, 2009).

III. The existing law is inadequate.

Unfortunately, the existing law provides little protection:[20]

- Many legal analysts believe courts will find that the Fourth Amendment's guarantee against unreasonable search and seizures does not apply because of the "third party doctrine": the personal online data is "communicated" by a user to the web site owner, thus vitiating any reasonable expectation of privacy.[21]
- The Stored Communications Act, part of the Electronic Communications Privacy Act, is unlikely to provide substantial limitations on government access to the profiles created by behavioral marketers, because (1) the information may be in the possession of third-party entities not covered by the act,[22] and (2) if the Act applies, it is not clear what protection is accorded to clickstream data and the like, which may or may not constitute the "content" of a communication.[23]
- Although the Privacy Act of 1974[24] regulates systems of records that are created and maintained by the government, the Act does not apply to records obtained from a private party.[25]
- While a patchwork of other laws may provide some protection for certain kinds of records, like financial[26] and health[27] data or cable television[28] and video rental records,[29] these laws leave the vast majority of online data unprotected.

IV. Congress should pass new laws that restrict government access to this data, balancing effective law enforcement with the right to privacy.

A record of online behavior is at least as revealing as a record of a person's reading habits at a library. To safeguard autonomy, privacy, and intellectual freedom, our laws have long protected library records,[30] and to protect these same values, we need

---

[20] *See generally* John Palfrey, *The Public and the Private at the United States Border with Cyberspace*, 78 MISS. L.J. 241 (2008); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002).

[21] *See* ORIN S. KERR, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § I.B.3 (Jan. 2001); Solove, *supra* n.20 at 1141.

[22] *See* 18 U.S.C. §§ 2702-03

[23] *See* 18 U.S.C. § 2520(8), §§2702-03.

[24] 5 U.S.C. § 552a.

[25] *See* Solove, *supra* n.20, at 1066.

[26] *See* Right to Financial Privacy Act, 12 U.S.C. §§ 3401-22.

[27] *See* Health Insurance Portability and Accountability Act of 1996 § 264, Pub. L. 104-191, 110 Stat. 1936, § 2033 (codified at 42 U.S.C. 1320d-2 note); 45 C.F.R. §§ 164.

[28] *See* Cable Communications Policy Act of 1984, 47 U.S.C. § 551.

[29] *See* Video Privacy Protection Act of 1988, 18 U.S.C. § 2710.

[30] 48 states protect library reading records by statute, *see, e.g.*, N.Y. C.P.L.R. § 4509; Cal. Gov. Code §§ 6267, 6254(j), and federal and state courts have also often frowned upon attempts by the government or civil litigants to gain access to such records, *see, e.g.*, *In re Grand Jury Subpoena to Amazon.com*, 246 F.R.D. 570, 573 (W.D. Wis. 2007) (quashing a government subpoena seeking the identities of 120 book buyers because "it is an unsettling and un-American scenario to envision federal agents nosing through the

similar protections for the privacy of our online behavior. Likewise, under existing law, the government must obtain a warrant supported by probable cause to gain access to stored electronic communications, even when those records are in the possession of a third party.[31] The digital profiles compiled by behavioral marketers are every bit as revealing as emails or other communications and so require the same level of protection. Therefore:

- To obtain access to personal profiles compiled by behavioral marketers, the government should be required to obtain a *warrant based on a showing of probable cause*, that a crime is being or has been committed.[32]
- Third party civil litigants seeking to subpoena such information should be required to provide notice to the subject of the information, and to show
    - a compelling interest in the information,[33]
    - that no less intrusive means exists,[34]
    - a prima facie validity of the action, and
    - that these factors outweigh the subject's First Amendment right to receive information anonymously.
- Persons aggrieved should have a private right of action.[35]

The Internet has been the engine of radical, positive changes in the way we communicate, learn, and transact commerce. And a number of the most important actors in this space are supported by advertising revenue. Still, as we appreciate what the Internet brings us, we must be wary. Behavioral marketers are creating digital portraits of unprecedented breadth and depth—portraits that will be irresistible to government investigators. Without the necessary legal restrictions on government access to these portraits, we will soon find the Internet has been transformed from a library and playground to a fishbowl, and that we have unwittingly ceded core values of privacy and autonomy.

---

reading lists of law-abiding citizens while hunting for evidence against somebody else."); *In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc.*, 26 Media L. Rep. (BNA) 1599, 1601 (D.D.C. 1998) (First Amendment requires government to "demonstrate a compelling interest in the information sought . . . [and] a sufficient connection between the information sought and the grand jury investigation" prior to obtaining book records); *Tattered Cover v. City of Thornton*, 44 P.3d 1044, 1059 (Colo., 2002) (government access to book records only passes muster under Colorado Constitution if "warrant plus" standard is met by the government—i.e, prior notice, adversarial hearing, and showing of a compelling need).

[31] *See* Electronic Communications Privacy Act, 18 U.S.C. § 2703(a).

[32] *See, e.g.*, *Dumbra v. United States*, 268 U.S. 435, 439, 441 (1925); FED. R. CRIM. P. 41.

[33] See, e.g., *Kramerbooks*, 26 Media L. Rep. at 1601.

[34] *See, e.g.*, *Tattered Cover*, 44 P.3d at 1059.

[35] *See* ECPA, 18 U.S.C. § 2707.

Thank you for your efforts to highlight this important privacy issue. If you have any questions, please contact Christopher Calabrese at 202-715-0839 or by email at ccalabrese@dcaclu.org.

Sincerely,

Michael W. Macleod-Ball
Acting Director, Washington Legislative Office

Christopher Calabrese
Legislative Counsel