Statement of Christopher R. Calabrese, Legislative Counsel

American Civil Liberties Union

Washington Legislative Office

On

The State of Online Consumer Privacy

Before the Senate Commerce, Science and Transportation Committee

March 16, 2011

Good morning Chairman Rockefeller, Ranking Member Hutchison, and Members of the Committee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU) its more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide, about the importance of online privacy. We support comprehensive protections for Americans' personal information and specifically support a "Do Not Track" option for online consumers. These protections are crucial for preventing harm to consumers and to safeguard Americans' First and Fourth Amendment rights online.

I. Introduction

Rapid technological advances and the lack of an updated privacy law have resulted in a system where Americans are routinely tracked as they surf the internet. The result of this tracking – often performed by online marketers – is the collection and sharing of Americans' personal information with a variety of entities including offline companies, employers and the government. As greater portions of our lives have moved online, unregulated data collection has become a growing threat to our civil liberties.

As one recent report explains, the internet has been an engine of radical, positive changes in the way we communicate, learn, and transact commerce.[1] The internet allows us to connect to one another and share information in ways we never before could have imagined. Many of the civil liberties benefits of the internet – the ability to access provocative materials more readily, to associate with non-mainstream groups more easily, and to voice opinions more quickly and at lower cost– are enhanced by the assumption of practical anonymity. Similarly, consumers are largely unaware of the breadth of information collection and the various uses to which it is put.

In short, Americans assume that there is no central record of what they do and where they go online. However in many instances that is no longer the case. Behavioral marketers are creating profiles of unprecedented breadth and depth that reveal personal aspects of people's lives including their religious or political beliefs, medical information, and purchase and reading habits. Even as behavioral targeting continues to grow, its practitioners have already demonstrated a disturbing ability to track and monitor an individual's actions online.

If this collection of data is allowed to continue unchecked, then capitalism will build what the government never could – a complete surveillance state online. Without government intervention, we may 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.

II. Americans have embraced technology, but they still expect privacy

[1]Federal Trade Commission (Bureau of Consumer Protection), *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, December 1, 2010.

Technology has moved rapidly and Americans have adopted these changes into their lives:

- Over 50% of American adults use the internet on a typical day.[2]
- 62% of online adults watch videos on video-sharing sites,[3] including 89% of those aged 18–29.[4]
- Over 70% of online teens and young adults[5] and 35% of online adults have a profile on a social networking site.[6]
- 83% of Americans own a cell phone and 35% of cell phone owners have accessed the Internet via their phone.[7]

Companies continue to innovate and create new ways for Americans to merge technology with daily activities. Google has spent the last five years building a new online book service and sales of digital books and devices have been climbing.[8] Americans increasingly turn to online video sites to learn about everything from current news to politics to health.[9] Location-based services[10] are also a burgeoning market.[11]

---

[2] Common daily activities include sending or receiving email (40+% of all American adults do so on a typical day), using a search engine (35+%), reading news (25+%), using a social networking site (10+%), banking online (15+%), and watching a video (10+%). Pew Internet & American Life Project, *Daily Internet Activities, 2000–2009*, http://www.pewinternet.org/Trend-Data/Daily-Internet-Activities-20002009.aspx.

[3] A "video-sharing site" or "video hosting site" is a website that allow users to upload videos for other users to view (and, often, comment on or recommend to others). Wikipedia, *Video Hosting Service*, http://en.wikipedia.org/wiki/Video_sharing (as of January 21, 2011). YouTube is the most common video-sharing site today.

[4] Pew Internet & American Life Project, *Your Other Tube: Audience for Video-Sharing Sites Soars*, July 29, 2009, http://pewresearch.org/pubs/1294/online-video-sharing-sites-use

[5] Pew Internet & American Life Project, *Social Media & Young Adults*, Feb. 3, 2010, http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx.

[6] "Social networking sites" allow users to construct a "semi-public" profile, connect with other users of the service, and navigate these connections to view and interact with the profiles of other users. danah m. boyd & Nicole B. Ellison, *Social Networking Sites: Definition, History, and Scholarship*, 13 J. of Comp.-Mediated Comm. 1 (2007); Pew Internet & American Life Project, *Adults & Social Network Sites*, Jan. 14, 2009, http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites.aspx.

[7] Pew Internet & American Life Project, *Internet, Broadband, and Cell Phone Statistics*, Jan. 5, 2010, http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx.

[8] *See generally* ACLU of Northern California, *Digital Books: A New Chapter for Reader Privacy*, Mar. 2010, *available at* http://www.dotrights.org/digital-books-new-chapter-reader-privacy.

[9] "More Americans are watching online video each and every month than watch the Super Bowl once a year.." Greg Jarboe, *125.5Million Americans Watched 10.3 Billion YouTube Videos in September*, SEARCHENGINEWATCH.COM, Oct. 31, 2009, http://blog.searchenginewatch.com/091031-110343.

[10] "Location-based services" is an information service utilizing the user's physical location (which may be automatically generated or manually defined by the user) to provide services. Wikipedia, *Location-Based Service*, http://en.wikipedia.org/wiki/Location-based_service (as of January 21, 2011).

[11] Recent location-based service Foursquare built a base of 500,000 users in its first year of operation. Ben Parr, *The Rise of Foursquare in Numbers [STATS]*, MASHABLE, Mar. 12, 2010, http://mashable.com/2010/03/12/foursquare-stats/.

However this rapid adoption of new technology has not eliminated Americans' expectations of privacy. To the contrary, Americans still expect and desire that their online activities will remain private, and express a desire for laws that will protect that privacy:

- 69% of Internet users want the legal right to know everything that a Web site knows about them.[12]
- 92% want the right to require websites to delete information about them.[13]

And consumers oppose online tracking:

- 67% rejected the idea that advertisers should be able to match ads based on specific websites consumers visit;[14] and
- 61% believed these practices were not justified even if they kept costs down and allowed consumers to visit websites for free.[15]

In sum, while Americans make great use of the internet, they are very concerned about their privacy and specifically troubled by the practice of behavioral targeting.

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

Behavioral targeting contravenes many American's expectation of privacy and how they should be treated online. Online advertising is one of the fastest growing businesses on the internet and it is based on collecting a staggering amount of information about people's online activities. Advertising has always been prevalent online, but instead of targeting websites – such as advertising shoes on a shoe store site - advertisers now use personal information to target individuals directly.

They do this using different surveillance tools. The simplest tools are cookies. A cookie is a file that a website can put on a user's computer when the user visits it so that when the user returns, or visits another affiliated site, it remembers certain information about the user. Cookies were initially used to help websites remember user passwords or contents in shopping bags, but as online marketing grew more sophisticated, cookies did too. Advertisers and aggregators modified cookies to track people's web page visits, searches, online purchases, videos watched, posts on social networking, and so on.

Another popular and even more invasive tool for tracking is the flash cookie. Flash cookies are often used by data aggregators to re-install a regular cookie that a user had detected

[12] Joseph Turow, et al., *Americans Reject Tailored Advertising* 4 (2009), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.
[13] *Id.*
[14] Lymari Morale, *U.S. Internet Users Ready to Limit Online Tracking for Ads*, USA TODAY, December 21, 2010
[15] *Id.*

and deleted. The newest and most aggressive form of tracking is the beacon. Beacons, also known as web bugs, are often used by sites that hire third party services to monitor user actions. These devices can track a user's movements extremely closely; to the point that they can monitor keystrokes on a page or movements by a user's mouse. The result of these practices is the collection and sale of a wealth of consumer data without any legal limits or protections for individuals.

As targeted ads become increasingly profitable, behavioral marketers are growing more ambitious and seeking to form an even more complete picture of unsuspecting citizens. The *Wall Street Journal* recently conducted a comprehensive study on the effects of online marketing on individual privacy and the results were alarming. The study found that the nation's 50 top websites installed an average of 64 pieces of tracking technology on user's computers, usually with no warning. A dozen sites installed over a hundred. For example, the study found that Microsoft's popular website, MSN.com, attached a tracking device that identified and stored user's detailed personal information. According to the tracking company that created the file, it could predict a user's age, zip code, and gender, as well as an estimate of a user's income, marital status, family status and home ownership status.[16] These new technologies allow marketers to combine a vast amount of information gleaned from different websites over time in order to paint an extremely detailed profile of potential consumers. Any particular website may have little information and this may not alarm some, but when a large number of these data points are aggregated, an extremely detailed picture results.

In addition, the *Wall Street Journal* found that tracking technology has become so advanced and covert that the website owner is often not even aware of its presence. Microsoft, one of the largest developers of computer software in the world, said it did not know about the tracking devices on its site until informed by the *Journal.*[17] If these technologies have become as surreptitious as to slip past sophisticated website owners, it is completely unreasonable to believe that the average user would be able to avoid their spying.

IV. Identifying individuals and the merger of online and offline identity

Online and offline data companies are combining forces to get an even more detailed profile of consumers and further erode privacy. For example, 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."[18]

[16] Angin Win, *The Web's New Gold Mine: Your Secrets*, WALL STREET JOURNAL, July 30, 2010
[17] *Id.*
[18] Why Comscore?, http://comscore.com/About_comScore/Why_comScore (last visited January 21, 2011).

In another example, the data firm Aperture has made the connection between online and offline identities by collecting data from offline data companies like Experian or Nielsen's Claritas and then combining it with a huge database of email addresses maintained by its parent company, Datran Media.[19] According to media reports, many major companies are working with Aperture.[20] ""The line between merging online and offline data isn't no-man's land anymore; it's becoming more of a common practice," said Mike Zaneis, Washington lobbyist for the Interactive Advertising Bureau."[21] A variety of services offer to merge names and postal addresses with collected IP and email addresses.[22]

To be clear: **such a merger of data is only possible when consumers are specifically identified**. As described above, markets are using personal identifiers like email addresses to connect online browsing habits to offline information from other databases. One venture capitalistic described it to the *Wall Street Journal*: ""They're trying to find better slices of data on individuals," says Nick Sturiale, a general partner at Jafco Ventures, which has largely avoided the sector. "Advertisers want to buy individuals. They don't want to buy [Web] pages.""[23] You can only "buy individuals" when you know who they are.

V. Regulation of behavioral targeting does not threaten the "Free Internet"

The ACLU believes the internet is the most advanced marketplace of ideas and one of the greatest tools ever created for advancing American's First Amendment rights. We would never endorse any regulation that endangered the robustness and variety of this medium. Laws protecting personal information and those that would create a "Do Not Track" mechanism would not harm the internet or end the provision of free products or services.

Behavioral targeting is different than "contextual advertising," another type of online ad service which shows ads to users based on the content of the web page they are currently viewing or the web search they have just performed. 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 IP address. The practice does not raise significant privacy concerns.

Nor would commonsense regulations necessarily foreclose the use of consumer data as part of advertising and services. For example, a consumer may want to allow significant data collection by websites with whom they already have a relationship. Companies like Google and Amazon gather information that has demonstrable benefit to the consumer – by providing book

---

[19] Michael Learmonth, *Holy Grail of Targeting is Fuel for Privacy Battle*, ADVERTISING AGE, March 22, 2010
[20] *Id.*
[21] *Id.*
[22] See: http://biz.freshaddress.com/RealTimePostalAppend.aspx For a long list of their clients please see: http://biz.freshaddress.com/ClientsByName.aspx
[23] Scott Thrum, *Online Trackers Rake in Funding*, WALL STREET JOURNAL, February 25, 2011 at: http://online.wsj.com/article/SB10001424052748704657704576150191661959856.html#ixzz1FYWLkEWm

recommendations or easy-to-use maps. Consumers may welcome targeted ads when they feel in control of their own information or may consider it a fair tradeoff for other goods or services.

Content has been supported for years (and in many cases for decades and even centuries) through advertising without the need for detailed targeting and tracking of consumers. But studies have demonstrated that the vast majority of the revenue from tracking consumers online goes not to content providers but rather to the behavioral targeters themselves. Industry sources say that 80% of the revenue from targeting – 4 in 5 dollars – went to create and enhance the targeting system, not to publishers.[24] Major publishers like the New York Times have endorsed a "Do Not Track" mechanism – clearly they are not concerned that such a mechanism will harm their ad revenue.[25]

VI. Access to extensive personal profiles threatens personal privacy and the First and Fourth Amendment

It is no exaggeration to say that data profiles — which may combine records of a person's entire online activity and extensive databases of real-world, personally identifiable information — draw a personal portrait unprecedented in scope and detail. Because the internet has become intertwined with so many personal facets of our lives, the same technology that has provided such tremendous advances also creates the possibility of tremendous intrusion by companies and the government.

i. Non-governmental actors

The harms caused by excessive and invasive data collection are real and pressing. They begin with straightforward invasions of privacy. Should anyone have the right to know and sell to others the fact that you are overweight, or depressed, or gay?[26] These are all commonplace occurrences with marketers and social networking sites routinely making and selling these determinations. They have significant consequences for consumers who have no say in the collection and use of their own information. As the *Wall Street Journal* explains:

> Yahoo's network knows many things about recent high-school graduate Cate Reid. One is that she is a 13- to 18-year-old female interested in weight loss. Ms. Reid was able to determine this when a reporter showed her a little-known feature on Yahoo's website, the

[24] The Jordan Edmiston Group, *M&A Overview and Outlook*, Slide 13, can be found at: http://www.jegi.com/files/docs/IABMIXX.pdf

[25] *Protecting Online Privacy*, NEW YORK TIMES, December 4, 2010

[26] See Testimony of Pam Dixon *The Modern Permanent Record and Consumer Impacts from the Offline and Online Collection of Consumer Information*, Before the Subcommittee on Communications, Technology, and the Internet, and the Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy and Commerce November 19, 2009 at http://www.worldprivacyforum.org/pdf/TestimonyofPamDixonfs.pdf; Brett Michael Dykes, *Latest Facebook privacy outrage: ad data outing gay users*, THE UPSHOT, October 22, 2010 at: http://news.yahoo.com/s/yblog_upshot/20101022/bs_yblog_upshot/latest-facebook-privacy-outrage-ad-data-outing-gay-users

> Ad Interest Manager, that displays some of the information Yahoo had collected about her.
>
> Yahoo's take on Ms. Reid, who was 17 years old at the time, hit the mark: She was, in fact, worried that she may be 15 pounds too heavy for her 5-foot, 6-inch frame. She says she often does online research about weight loss.
>
> "Every time I go on the Internet," she says, she sees weight-loss ads. "I'm self-conscious about my weight," says Ms. Reid, whose father asked that her hometown not be given. "I try not to think about it…. Then [the ads] make me start thinking about it."[27]

This tracking is ubiquitous around the internet with tracking technology on 80% of 1,000 popular sites, up from 40% of those sites in 2005.[28]

In the information age knowledge is power and personal information can be used for many other purposes. A data-mining firm called Rapleaf has said it can make determinations about creditworthiness and whether someone will be a good customer.[29] A defense attorney attempted to access the social networking pages of two teens in order to prove they were appropriately denied health care.[30] One employer demanded access to its employee's private Facebook account as part of a background check.[31]

When information escapes a consumer's control, it gives power to others to make decisions about them that have real consequences for their lives. In addition, the lack of control and transparency surrounding consumer personal information harms not just consumers but the internet as a whole. Uncertainty over the use or misuse of information by third parties retards the adoption of new technologies and makes consumers more anxious about revealing personal information.

Personal information can also reveal weaknesses that unscrupulous actors can exploit. Ninety-two year old veteran Richard Guthrie was bilked out of more than $100,000 by criminals who identified him from marketing lists.[32] InfoUSA routinely advertised lists of:

> "Elderly Opportunity Seekers," 3.3 million older people "looking for ways to make money," and "Suffering Seniors," 4.7 million people with cancer or Alzheimer's disease.

---

[27] Win article.
[28] *Id.*
[29] Lucas Conley, *How Rapleaf Is Data-Mining Your Friend Lists to Predict Your Credit Risk*, FAST COMPANY November 16, 2009 at http://www.fastcompany.com/blog/lucas-conley/advertising-branding-and-marketing/company-we-keep
[30] Mark Stein, Facebook Page? Or Exhibit A in Court?, PORTFOLIO.COM, February 5, 2008 http://www.portfolio.com/views/blogs/daily-brief/2008/02/05/facebook-page-or-exhibit-a-in-court/
[31] Matt Liebowitz Boss Demands Employee's Facebook Password, MSNBC.COM, March 1, 2011 http://www.msnbc.msn.com/id/41743732/ns/technology_and_science-security/
[32] Charles Duhigg, *Bilking the Elderly, With a Corporate Assist*, NEW YORK TIMES. May 20, 2007 http://www.nytimes.com/2007/05/20/business/20tele.html?_r=2

> "Oldies but Goodies" contained 500,000 gamblers over 55 years old, for 8.5 cents apiece. One list said: "These people are gullible. They want to believe that their luck can change."[33]

In other cases thieves purchased access to databases of Americans' personal information and used that information to commit identity theft.[34]

Collection of personal information online turbo-charges this process. One reporter asked a company to search out information about her online. She disclosed that, armed only with her name and email address, "Within 30 minutes, the company had my Social Security number; in two hours, they knew where I lived, my body type, my hometown, and my health status."[35]

ii. Governmental actors

As their contracts with the data aggregator industry demonstrate, government and law enforcement agencies have also found these personal data profiles irresistible. In 2006 the *Washington Post* reported that the federal government and states across the country have developed relationships with private companies that collect personal information about millions of Americans, including unlisted cell phone numbers, insurance claims, driver's license photographs, and credit reports through private data aggregators including Accurint, Entersect and LexisNexis. In fact, Entersect boasts that it is "the silent partner to municipal, county, state, and federal justice agencies who access our databases every day to locate subjects, develop background information, secure information from a cellular or unlisted number, and much more."[36]

The Central Intelligence Agency (CIA), via its investment arm In-Q-Tel, has invested in a software company that specializes in monitoring blogs and social networks[37] and the Department of Defense, the CIA, and the Federal Bureau of Investigation (FBI) have all purchased use of private databases from Choicepoint, one of the largest and most sophisticated aggregators of personal data.[38] In the words of the FBI, "We have the legal authority to collect certain types of information" because ChoicePoint is "a commercial database, and we purchase a

---

[33] *Id.*

[34] Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress*, January 26, 2006. http://www.ftc.gov/opa/2006/01/choicepoint.shtm

[35] Jessica Bennett, *What the Internet Knows about You*, NEWSWEEK, October 22, 2010. http://www.newsweek.com/2010/10/22/forget-privacy-what-the-internet-knows-about-you.html

[36] O'Harrow Jr Robert, *Centers Tap into Personal Databases*, WASHINGTON POST, April 2, 2008

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

[38] Shane Harris, *FBI, Pentagon Pay For Access to Trove of Public Records*, NATIONAL JOURNAL., Nov. 11, 2005 *at* http://www.govexec.com/story_page.cfm?articleid=32802; Robert O'Harrow Jr., *In Age of Security, Firm Mines Wealth Of Personal Data*, WASHINGTON POST, January 20, 2005, *at* http://www.washingtonpost.com/wp-dyn/articles/A22269-2005Jan19.html

lot of different commercial databases….They have collated information that we legitimately have the authority to obtain."[39]

The government has demonstrated an increasing interest in online user data in other ways as well. In 2006 the Department of Justice (DOJ) subpoenaed search records from Google, Yahoo!, and other search providers in order to defend a lawsuit.[40] In 2007, Verizon reported receiving 90,000 requests per year and in 2009, Facebook told *Newsweek* it was getting 10 to 20 requests each day. In response to increasing privacy concerns, Google started to publish the number of times law enforcement asked for its customers' information and reported over 4,200 such requests in the first half of 2010 alone. 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."[41] 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.

Our First Amendment rights to freedom of religion, speech, press, petition, and assembly are based on the premise that open and unrestrained public debate empowers democracy by enriching the marketplace with new ideas and enabling political and social change through lawful means. The Fourth Amendment shields private conduct from unwarranted government scrutiny. Together the exercise of these rights online has allowed the internet marketplace of ideas to expand exponentially.

Courts have uniformly recognized that government requests for records of which books, films, or other expressive materials individuals have received implicate the First Amendment and trigger exacting scrutiny.[42] These cases are grounded in the principle that the First Amendment protects not only the right of individuals to speak and to express information and ideas, but also the corollary right to receive information and ideas through books, films, and other expressive materials.[43] Within this protected setting, privacy and anonymity are vitally important. Anonymity "exemplifies the purpose behind the Bill of Rights, and of the First Amendment in

---

[39] Harris, supra n. 16 (quoting F.B.I. spokesman Ed Cogswell)
[40] Hiawatha Bray, *Google Subpoena Roils the Web, US Effort Raises Privacy Issues*, BOSTON GLOBE, January 21, 2006 *at* http://www.boston.com/news/nation/articles/2006/01/21/google_subpoena_roils_the_web/.
[41] Miguel Helft, *Google Told to Turn Over User Data of YouTube*, NEW YORK TIMES, July 4, 2008 *at* http://www.nytimes.com/2008/07/04/technology/04youtube.html.
[42] *In re Grand Jury Subpoena to Kramerbooks & Afterwords Inc.*, 26 Med. L. Rptr. 1599, 1600-01 (D.D.C. 1998) (Dkt. No. 21, Ex. B) (requiring government to show compelling interest and a sufficient connection between its investigation and its request for titles of books purchased by Monica Lewinsky); *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1053 (Colo. 2002) (holding that search of bookseller's customer purchase records necessarily intrudes into constitutionally protected areas)
[43] *See, e.g., Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council*, 425 U.S. 748, 757 (1976) (right to receive advertisements); *Stanley v. Georgia*, 394 U.S. 557, 564 (1969) (films); *Bantam Books v. Sullivan*, 372 U.S. 58, 64 n.6 (1963) (books).

particular," because, among other things, it serves as a "shield from the tyranny of the majority."[44] An individual may desire anonymity when engaging in First Amendment activities—like reading, speaking, or associating with certain groups—because of "fear of economic or official retaliation, . . . concern about social ostracism, or merely . . . a desire to preserve as much of one's privacy as possible."[45]

The Supreme Court has also recognized that anonymity and privacy are essential to preserving the freedom to receive information and ideas through books, films, and other materials of one's choosing. For example, in *Lamont v. Postmaster General*, the Court invalidated a postal regulation that required the recipient of "communist political propaganda" to file a written request with the postmaster before such materials could be delivered.[46] The regulation violated the First Amendment because it was "almost certain to have a deterrent effect … Any addressee [was] likely to feel some inhibition" in sending for literature knowing that government officials were scrutinizing its content.[47] Forced disclosure of reading habits, the Court concluded, "is at war with the 'uninhibited, robust, and wide-open' debate and discussion that are contemplated by the First Amendment."[48]

These words ring equally true today in the Information Age, with the prevalence of the internet and other new technologies. Although these technological advances provide valuable tools for creating and disseminating information, the unprecedented potential for government and companies to store vast amounts of personal information for an indefinite time poses a new threat to the right to personal privacy and free speech. In *In re Grand Jury Subpoena to Amazon.com*, the district court recognized this reality in holding that a grand jury subpoena to Amazon requesting the identities of buyers of a certain seller's books raised significant First Amendment concerns.[49] The court explained its concern over the chilling effect that would flow from enforcing such a subpoena in the age of the internet, despite its confidence in the government's good-faith motives:

> [I]f word were to spread over the Net—and it would—that [the government] had demanded and received Amazon's list of customers and their personal purchases, the chilling effect on expressive e-commerce would frost keyboards across America. Fiery rhetoric quickly would follow and the nuances of the subpoena (as actually written and served) would be lost as the cyberdebate roiled itself to a furious boil. One might ask whether this court should concern itself with blogger outrage

[44] *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995).
[45] *Id.* at 341-42.
[46] *Lamont v. Postmaster General*, 381 U.S. 301, 302 (1965).
[47] *Id.* at 307.
[48] *Id.* (quoting *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964)).
[49] 246 F.R.D. at 572-73

> disproportionate to the government's actual demand of Amazon. The logical answer is yes, it should: well-founded or not, rumors of an Orwellian federal criminal investigation into the reading habits of Amazon's customers could frighten countless potential customers into canceling planned online book purchases, now and perhaps forever. . . . Amazon . . . has a legitimate concern that honoring the instant subpoena would chill online purchases by Amazon customers.[50]

The internet is, and must remain, the most open marketplace of ideas in the history of the world. In order to guarantee this, we must provide consumers with the tools they need to control their personal information and meaningful mechanisms for assuring privacy and protecting the robust rights established by the Constitution.

VII. Solutions exist

Reasonable and workable solutions exist for grappling with the problems of excessive data collection. While the technology is new, the problem is not. As the preceding case law demonstrates, as a society we have always been concerned about problems like judging or attacking individuals based on their reading or viewing habits. That is why 48 states protect public library reading records by statute.[51] Congress has also recognized the privacy interests of users of expressive material and created strong protections in several other contexts. The Video Privacy Protection Act prohibits disclosure of video rental records without a warrant or court order.[52] The Cable Communications Policy Act similarly prohibits disclosure of cable records absent a court order.[53]

Moreover, more than 30 years ago the U.S. Department of Health, Education and Welfare (now the Department of Health and Human Services), crafted basic privacy principles to protect personal information.[54] Called the Fair Information Practice Principles (FIPPs), they have become the basis for comprehensive privacy laws in most of the industrialized world as well as sector specific privacy laws in the United States.[55] In 2008 the Privacy Office of the Department

---

[50] *In re Grand Jury Subpoena to Amazon.com*, 246 F.R.D. at 573.

[51] *See, e.g.*, N.Y. C.P.L.R. § 4509; Cal. Gov. Code §§ 6267, 6254(j). The two states that do not have library confidentiality laws are Hawaii and Kentucky. However, the Attorney Generals' Offices in each state have issued opinions in support of reader privacy. Haw. OIP Opinion Letter No. 90-30 (1990) (disclosure of library circulation records "would result in a clearly unwarranted invasion of personal privacy"); Ky. OAG 82-149 (1982) ("all libraries may refuse to disclose for public inspection their circulation records. . . . [W]e believe that the privacy rights which are inherent in a democratic society should constrain all libraries to keep their circulation lists confidential.").

[52] 18 U.S.C. §§ 2710(b)(2)(C), 2710(b)(2)(F), 2710(b)(3).

[53] 47 U.S.C. § 551(h).

[54] For a brief history on the principles please see Robert Gellman, Fair Information Practices: A Basic History at http://bobgellman.com/rg-docs/rg-FIPShistory.pdf

[55] *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* October 24, 1995; Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq.

of Homeland Security formally adopted them in its analysis of DHS programs. And in a recent report, the Department of Commerce recommended that the FIPPs as described by DHS be adopted as the basis for internet regulation.[56]

The FIPPs stand for eight relatively straightforward ideas:

- Transparency: Individuals should have clear notice about the data collection practices involving them.
- Individual Participation: Individuals should have the right to consent to the use of their information.
- Purpose Specification: Data collectors should describe why they need particular information.
- Data Minimization: Information should only be collected if it's needed.
- Use Limitation: Information collected for one purpose shouldn't be used for another.
- Data Quality and Integrity: Information should be accurate.
- Security: Information should be kept secure.
- Accountability and Auditing: Data collectors should know who has accessed information and how it is used.

While some adjustments will have to be made to conform to new technologies, international internet data collection practices, as well as the data collection practices of other sectors of the US economy, are already governed by the FIPPs.[57] To imply as some have done that application of these regulations in this case would cause serious harm to the internet and e-commerce seems overstated at best.

These protections must be embodied in law, not just in industry practice. For years government agencies have called on industry to provide privacy protections for consumers. However, as a recent Federal Trade Commission report explains, self-regulatory efforts "have been too slow, and up to now have failed to provide adequate and meaningful protection."[58] One example illustrates this fact well. In 1999 and 2000 when behavioral targeting first attracted

[56] Department of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, December 2010.
[57] *Id.*
[58] Federal Trade Commission (Bureau of Consumer Protection), *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, December 1, 2010.

regulatory attention, an industry group, the Network Advertising Initiative (NAI), claimed that self-regulation was a solution and that all NAI members would follow a common code of conduct.[59] As regulatory attention faded, so did participation in the NAI. By 2003 it had only two members. There is no reason to believe that things would be different now.

It is important to note that technology is already moving to help. Browser manufacturers are creating technical mechanisms so that web surfers can indicate their preference not to be tracked.[60] If given the force of law through the passage of a "Do Not Track" law, those mechanisms set a solid foundation for beginning to protect personal information online.

VIII. Conclusion

The current online data collection practices create detailed profiles on each of us. These practices are neither benign nor anonymous. They harm consumers and directly impact their fundamental rights. They are also unpopular – even when explicitly tied to the provision of free services. Good solutions exist and have been adopted in other countries and other parts of the U.S. economy. The Committee should look to these solutions like the "Do Not Track" mechanism and adopt legally enforceable rules to protect consumers and end this profiling.

[59] World Privacy Forum, *Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation*, Fall 2007 at: http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf

[60] Julia Angwin, *Web Tool on Firefox to Deter Tracking*, WALL STREET JOURNAL, January 24, 2011.