Spring 2010

Protecting Consumers by Tracking Advertisers Under the National Broadband Plan

Courtney A. Barclay

PROTECTING CONSUMERS BY TRACKING ADVERTISERS UNDER THE NATIONAL BROADBAND PLAN

by

Courtney A. Barclay*

The Federal Communications Commission (FCC) has consistently been charged with protecting American consumers from intrusive practices. The FCC has regulated telemarketers and email advertisers, as well as telecommunications carriers. The challenge now faced by the FCC is whether, and how, to regulate advertising via broadband as it develops a National Broadband Plan to expand the adoption of this technology.

In 2009, the FCC issued a Notice of Inquiry on a variety of issues pertaining to the development of the National Broadband Plan.[1] One area in which the FCC asked for public comment was the use of online tracking technologies for commercial purposes.[2] The FCC specifically asked about behavioral targeting and deep packet inspection to provide targeted online advertisements.[3] Behavioral targeting is the technique that advertisers use to analyze a person's web viewing habits "to predict user preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such Web viewing behaviors."[4] These technologies can be used in a pervasive

---

* Dr. Barclay holds a Ph.D. in Mass Communications and J.D. from the University of Florida. She is an Assistant Professor in Communications Law at the S.I. Newhouse School of Public Communications at Syracuse University. Ms. Barclay is grateful to the staff and 2009 Summer IPIOP clerks at the Electronic Privacy Information Center.

[1] In the Matter of a National Broadband Plan for Our Future, GN Docket No. 09-51, FCC 09-31 (Apr. 8, 2009) (hereinafter "FCC NOI"), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-31A1.pdf.

[2] *Id.* at 21-3.

[3] *Id.* at 22-3.

[4] American Association of Advertising Agencies, the Association of National Advertisers, the Better Business Bureau, the Direct Marketing Association, and the

manner to track a user's movements and views not only on one site, but across multiple web sites and for extended lengths of time.

Online, targeted advertising is a growing market that provides many benefits to advertisers and consumers. For example, Google's content network allows advertisers to control the number of times an individual is exposed to a particular ad, as well as to get information on the number of persons viewing an ad and the average number of times those ads are viewed by an individual user. Google's system also provides consumers with the opportunity to opt out of certain types of advertising as well as the tracking technologies Google uses to provide advertisements relevant to the individual user.

Part I of this article discusses the traditions of privacy protection and the existing privacy protection laws in the United States, including past actions by the FCC to protect consumer privacy. Part II discusses online advertising practices and the associated privacy concerns for consumers. Part III examines the Federal Trade Commission's (FTC) recommended principles and the current industry guidelines adopted to protect consumer privacy. Part IV discusses the increased federal efforts to regulate online consumer tracking by the FTC, Congress, and the FCC. This article concludes with a discussion of the need for government regulation of online advertising, with emphasis on potential FCC recommendations as part of the National Broadband Plan.

I
PRIVACY PROTECTION IN THE UNITED STATES

The FCC pointed to consumer privacy as an area of concern in the development of a national broadband play.[5] However, lawmakers, scholars, and citizens have struggled to articulate a comprehensive definition of privacy.[6] The general acceptance of privacy as "right to be let alone," first asserted by Samuel Warren and Louis Brandeis in the late

---

Interactive Advertising Bureau, Self-Regulatory Principles for Online Behavioral Advertising (July 2009) [hereinafter Coop Principles], *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf.

[5] FCC NOI, *supra* note 1 at 21-23.

[6] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 479 (2006).

1800s, is vague and incorporates a wide range of issues from protecting personal property to controlling the collection and dissemination of personal information.[7] In contrast to this sweeping definition, the legal protections for privacy have developed gradually in fragments to address specific issues one at a time. [8]

These piecemeal protections target distinct privacy concerns that can generally be described as either decisional or informational.[9] Decisional privacy refers to an individual's autonomy to make decisions about what to wear on a given day and what religion to practice. Informational privacy refers to use of personal information about an individual that "both expands and limits individual autonomy."[10] This latter category has found limited protection in the federal courts, which grant the government deference in determining when an invasion of informational privacy is necessary.[11] There has been some progress in the federal and state legislatures with varying levels of success.[12]

The long-standing privacy protection principles that have influenced the legislative progress originated in international law. These principles dictate that consumers need to be fully informed about what data is being collected, how the data will be used or shared, and how long the data will be retained. Consumers need to have a choice as to whether to provide this data. This section will explore those principles.

---

[7] *See* Jon L. Mills, Privacy: The Lost Right 14 (2008).

[8] Solove, *supra* note 6. *See also, e.g.,* Health Insurance Portability and Accountability Act of 1996, Pub. Law No. 104-191, 110 Stat. 1936 (1996); Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 15 U.S.C. § 1681 et seq. (2009); Family Educational Rights and Privacy Act of 1974, 20 USCS § 1232g (2009); Cable Communications Policy Act of 1984; Video Privacy Protection Act of 1998; Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003; Telephone Consumer Protection Act of 1991.

[9] Daniel J. Solove, Marc Rotenberg, & Paul M. Schwartz, Information Privacy Law 1 (Aspen 2006).

[10] *Id.*

[11] Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 Berkeley Tech L.J. 283, 288 (2003).

[12] *Id.* at 289-90.

A. Data Privacy Protection

As the electronic collection and transfer of data became more prominent, nations began to adopt data protection laws. In 1980, the Organization of Economic Cooperation and Development (OECD) adopted guidelines for data privacy protection. The OECD is an organization consisting of thirty countries, including the United States, formed to promote economic development and individual liberty.[13] The guidelines adopted by the OECD were intended to serve as a model for legislation in member states.[14] The main principles of the OECD Guidelines are 1) limiting data collection, 2) data quality, 3) purpose specification, 4) limited use of data, 5) security safeguards, 6) openness, 7) individual participation, and 8) accountability.[15]

The OECD principles focus on the collection of data. The collection should be limited to legal means, and should be done with the knowledge and consent of the subject of the information. Collection also should be limited to the data necessary for the stated purpose of collection. The request for consent should include notice of the purpose of the data collection.

Limiting the use of the data is also an important aspect of the OECD principles. Use should be limited to the stated purposes for the collection. Any additional uses should only be made with the consent of the data subject. Data should be protected from unauthorized use or access.

Another key principle is individual control and participation. This principle ensures that individuals have the right to inspect the data a third party maintains on him or her. Individuals also should have the right to challenge any data that may be incorrect for the opportunity to have the data erased or amended.

---

[13] *See generally* Organisation for Economic Co-operation and Development, http://www.oecd.org/ (last visited October 23, 2009).

[14] OECD, Organization for Economic Co-Operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2004), *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[15] *Id.*

Although the OECD principles are not binding on nations supporting them, they formed the basis for laws implementing strong privacy protections.[16] In 1995, the European Union adopted the Data Privacy Protection Directive that provided specific guidance to member nations on minimum standards for the implementation of the OECD principles.[17]

In 2003, the OECD issued a report on privacy online, in which it provided guidance for applying the data privacy protection principles to the online environment.[18] For example, the OECD suggested that using the OECD's Privacy Policy generator would create more consistency in website privacy policies across companies and countries.[19] The report also advocated the development and use of alternative dispute resolution methods for consumers and businesses.[20] Consumer education was an important goal raised by this report – education about privacy concerns online, privacy policies, and Privacy Enhancing Technologies (PETs).[21] To promote these goals – and the OECD Privacy Principles – the report recommended a hybrid of government-enforced legislation and industry-led, self-regulation as the best solution for the online environment.[22]

B. Incorporating OECD Principles

Although the U.S. Congress has not formally adopted these guidelines in a comprehensive piece of privacy legislation, it is evident in privacy laws that address particular issues, such as the Electronic

---

[16] *CDT's Guide to Online Privacy, Chapter Three: Existing Privacy Protections*, CENTER FOR DEMOCRACY & TECHNOLOGY, Oct. 22, 2009, http://www.cdt.org/privacy/guide/protect/.

[17] Council Directive 95/46/EC, 1995 O.J. (L 281) 31.

[18] WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, REPORT ON COMPLIANCE WITH, AND ENFORCEMENT OF, PRIVACY PROTECTIONS ONLINE (OECD 2003), *available at* http://www.olis.oecd.org/olis/2002doc.nsf/LinkTo/NT00000B82/$FILE/JT00139173.PDF.

[19] *Id.* at 8.

[20] *Id.* at 9-11.

[21] *Id.* at 12-3.

[22] *Id.* at 15.

Communications Privacy Act, the Gramm-Leach-Bliley Act, and the Fair Credit Reporting Act.[23]

To protect consumers, Congress has passed a series of laws that restrict the use and dissemination of sensitive financial data. The Gramm-Leach-Bliley Act of 1999 (GLBA),[24] for example, requires financial institutions to offer consumers the opportunity to opt-out of sharing "nonpublic personal information" with third parties.[25] The GBLA places other restrictions on financial institutions regarding privacy policies and limits on disclosures. However, the organization collecting the consumer data must be a "financial institution" before these restrictions apply.[26]

The Fair Credit Reporting Act of 1960,[27] similarly provides privacy protection to consumers, but is limited to "consumer reporting agencies."[28] These agencies must provide consumers with privacy notifications and opportunities to opt-out of disclosures. This law gives consumers the right to inspect their credit reports and challenge any information included in the reports.

Congress also has made efforts to protect consumers' private information held by communications providers. The FCC has been a

---

[23] *A Review of the Fair Information Principles: The Foundation of Privacy Public Policy*, THE PRIVACY RIGHTS CLEARINGHOUSE, Feb. 2004, http://www.privacyrights.org/ar/fairinfo.htm.

[24] 15 U.S.C. §§ 6801-6809 (1999).

[25] 15 U.S.C. § 6802(a) (1999).

[26] "The term "financial institution" means any institution the business of which is engaging in financial activities as described in section 1843(k) of title 12." 15 U.S.C. § 6809 (3)(A) (1999). Factors to be considered in the determination of if an activity is financial in nature are listed at 12 U.S.C. § 1843(k)(3).

[27] 15 U.S.C. §§ 1681 et. seq. (1970).

[28] "The term "consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f) (1999).

primary agency responsible for supporting these efforts.[29] For example, Congress has charged the FCC with regulating telecommunications carriers, telemarketers, and spammers.[30] In 1991, Congress, in an effort to protect consumer information of telephone service subscribers, instructed the FCC to "prescribe regulations to implement methods and procedures for protecting the privacy rights ... in an efficient, effective, and economic manner and without the imposition of any additional charge to telephone subscribers."[31]

The FCC, in tandem with the FTC, adopted the national Do-Not-Call Registry in 2002.[32] The FCC adopted regulations in 2003 that required telemarketers to conform to the new national registry. Congress granted specific authority to the FTC to assess fees for the implementation and operation of the registry. Additionally, Congress directed the FCC and the FTC to work together to enforce the registry. Since 2003, the Do-Not-Call Registry has been jointly operated by both agencies.[33] Similarly, the FCC has regulated spam advertisements sent directly to consumers on their mobile devices and unsolicited, commercial facsimile

---

[29] *See* FTC Privacy Initiatives, http://www.ftc.gov/privacy/ (last visited Oct. 20, 2009). The Federal Trade Commission is the other primary government agency responsible for enforcing consumer privacy protections.

[30] *See, e.g.,* Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (1991), *codified at* 47 U.S.C. § 227; Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) codified at 15 U.S.C. §§ 7701-7713, 18 U.S.C. § 1037, and 28 U.S.C. § 994.

[31] Telephone Consumer Protection Act of 1991 (TCPA), Pub. L. No. 102-243 (1991), which amended Title II of the Communications Act of 1934, 47 U.S.C. Section§ 201 et seq., *amended by* adding a new section, 47 U.S.C. Section 227. Telephone Consumer Protection Act of 1991, Pub. L. No. 102 § 243 (1991) (adding 47 U.S.C. § 227).

[32] "The National Do Not Call Registry gives you a choice about whether to receive telemarketing calls at home." National Do-Not-Call Registry, http://www.donotcall.gov/ (last visited Jan. 19, 2010). "Telephone numbers placed on the National Do Not Call Registry will remain on it permanently due to the Do-Not-Call Improvement Act of 2007, which became law in February 2008." *Do Not Call Registrations Permanent and Fees Telemarketers Pay to Access Registry Set*, FTC, April 10, 2008, http://www.ftc.gov/opa/2008/04/dncfyi.shtm.

[33] GAO, U.S. Gen. Accounting Office, Telemarketing: Implementation of the National Do-Not-Call Registry (Jan. 2005), *available at* www.gao.gov/cgi-bin/getrpt?GAO-05-113.

communications.[34] However, these regulations focus on the delivery of communications.

The collection, dissemination, and use of data create the potential harm associated with behavioral advertising. The FCC also has been directly involved with regulating these issues. In 1984, Congress regulated how cable companies could collect and use consumers' personal information. The Cable Communications Policy Act, implemented and enforced by the FCC, requires that cable providers notify customers of the information collected or to be collected by the provider on an annual basis. Further, providers may collect personally identifiable information only with express consent of the consumer or when "necessary to render a cable service or other service provided by the cable operator to the subscriber" or to "detect unauthorized reception of cable communications."[35]

The FCC also has enforced fair information practices against other telecommunication carriers with respect to consumer data. The Telecommunications Act of 1996 requires carriers to protect consumers' personal information, including: proprietary network information, such as the time, duration, and destination of each telephone call; directory information; and aggregate lists of proprietary network information.[36] The FCC required carriers to obtain express consent before disclosing the proprietary network information to third parties.[37] The regulations expressly included Voice over Internet Protocol providers and other IP-

---

[34] *See* FCC, IN THE MATTER OF RULES AND REGULATIONS IMPLEMENTING THE TELEPHONE CONSUMER PROTECTION ACT OF 1991, RPT. AND ORDER (June, CG Docket No. 02-278, FCC 03-230 (Sept. 26 , 2003).), *available at* http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-03-230A1.pdf.

[35] 47 U.S.C. § 551(a) (2008). *See also* Video Privacy Protection Act, Pub. L. 100-618 (codified at 18 U.S.C. § 2710 (1988)) (Creating a consumer right to opt-out of the disclosure of their personal information by video rental companies, further cementing Congress's commitment to consumer privacy. Video Privacy Protection Act, Pub. L. No. 100-618, codified at 18 U.S.C. § 2710 (1988).

[36] Telecommunications Act of 1996, 47 U.S.C. § 222 (2008).

[37] In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunication Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 61 Fed. Reg. 26,483 (May 28, 1996).

based telephony services to respond to a new technology modeling a traditionally regulated medium.[38]

The FCC also has stated that it will use its jurisdiction to ensure open and neutral access to broadband for consumers.[39] In charging the Commission with the development of a National Broadband Plan, Congress has specifically tasked the FCC with considering the advancement of consumer welfare.[40] The FCC, in a notice of inquiry, identified the tracking of consumers' web behavior as a potential threat to that welfare and to the successful nationwide adoption of broadband access.[41] The agency is currently reviewing comments on possible government regulation of this practice to protect the privacy of broadband subscribers and consumers.

II
ONLINE ADVERTISING PRACTICES RAISE PRIVACY CONCERNS

Online advertising is capturing an increasing market, as opposed to other, more traditional methods, having brought in $8.1 billion in revenue in 2000, and more than $20 billion in 2007.[42] The Internet has allowed advertisers to target individual consumers in ways other media cannot support.[43] Website owners, Internet Service Providers (ISPs), and search engine operators can provide data on individual consumers such

---

[38] *Id.*

[39] FCC, Policy Statement, (FCC Aug. 5, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf.

[40] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 6001 (k)(2)(D), 123 Stat. 516 (2009).

[41] FCC NOI, *supra* note 1.

[42] David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy, Journal of Economic Perspectives* (forthcoming – draft, Apr. 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1376607.

[43] STAFF REPORT: PUBLIC WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL INFORMATION INFRASTRUCTURE 34 (Federal Trade Commission 1996) [hereinafter "FTC Privacy Workshop"], *available at* http://www.ftc.gov/reports/privacy/Privacy1.shtm.

as geographic location, age, gender, salary, and social interests. This information allows the advertisers to deliver highly customized advertisements. However, such a massive collection of information raises significant privacy concerns. This section discusses online advertising practices and the associated privacy concerns.

A. Online Advertising and Consumer Profiles

There are two basic types of online targeting: contextual and behavioral. Contextual advertising is based on instantaneous data from a web page that a consumer is viewing. This data provides an advertisement relevant to the content on that page. Behavioral targeting tracks consumers' online activities to gather information about multiple websites he or she visits. This data is used to deliver advertisements relevant to the individual's predicted interests. Both of these targeting practices hold a large share of the advertising market – more than $13 billion for 2009.[44]

The majority of those advertising dollars – $12 billion – will be used for contextual advertising.[45] This method of online targeting is fairly innocuous from a privacy standpoint; it uses real-time information about the website a consumer is visiting to provide a contextually relevant advertisement based on keywords contained in the website.[46] For example, if a consumer reads a story about snowboarding on an online news site on which contextual advertising is hosted, the consumer will see ads for ski resorts or snowboarding equipment. The automated ad provider had searched the story and found snowboard as a key term, which generated the ads relevant to the story's content.

---

[44] Susan Hall, *Experts: Make the (Transparent) Case for Behavioral Advertising*, IT BUSINESS EDGE, July 28, 2009, http://www.itbusinessedge.com/cm/community/features/articles/blog/experts-make-the-transparent-case-for-behavioral-advertising/?cs=34433. *See also Behavioral Targeting: Secret Weapon in Display Ads Arsenal*, INTERACTIVE ADVERTISING BUREAU, July 2008, http://www.iab.net/insights_research/530422/1675/368205.

[45] Hall, *supra* note 44.

[46] Frederick Marckini, *Contextual Advertising, Part 1 of 2*, CLICKZ, Oct. 6, 2003, http://www.clickz.com/3087311.

Behavioral advertising raises privacy concerns not at issue with contextual advertising. To engage in behavioral advertising, the ad provider needs information about the consumer – not just information about a web page the consumer loaded. Behavioral advertising uses consumer profiles, which contain data collected over time about a particular user: search terms, websites visited, and online commercial transactions.[47] This information is then used to target advertisements based on the consumer, not the page. For example, if a consumer visits Lowes.com and views washers and dryers, that same consumer may see a Maytag advertisement when he visits the Wall Street Journal website to read a story on unemployment rates.

This multi-site approach, which accounts for at least 25 percent of all online campaigns,[48] has been available for five years. In 2004, TACODA Systems unveiled a system of sixty networked websites to provide targeted ads to visitors of those sites.[49] Before TACODA introduced this system, online advertising services were able to track users on individual sites to customize the advertisements users received on each site. The TACODA system expanded this capability by collecting more data on web users as they browsed various sites for news, travel, shopping, and

---

[47] *See* Elyse Tager, *A New Breed of Behavioral Targeting*, CLICKZ, Apr. 16, 2008, http://www.clickz.com/3629139. *See also A Primer on Behavioral Advertising*, CDT, July 31, 2008, http://www.cdt.org/policy/primer-behavioral-advertising.

[48] Rich Karpinski, *Will Using Behavioral Data Lead to Smarter Ad Buys?*, ADVERTISING AGE, Apr. 20, 2009, http://adage.com/adnetworkexchangeguide09/article?article_id=136003. The use of behavioral targeting may be underestimated as many contextually supplied ads still use tracking data on individual viewers to cap the number of times any individual is exposed to a particular advertisement, or to track whether an individual viewer purchases the product advertised from the advertiser. This tracking requires storing and analyzing data on individual consumers in the same way ad networks collect, store, and analyze consumer data to provide behaviorally targeted advertisements.

[49] Kris Oser, *Tacoda Ties Ads to Surfing Behavior; Network Allows Marketers to Extend Reach and Target Individuals Across 60 Sites*, ADVERTISING AGE 44, Nov. 14, 2004, *available at* http://adage.com/abstract.php?article_id=101172 (subscription required).

other activities.[50] Now, advertising networks like TACODA link hundreds of retailers and track more than 140 million Internet users.[51]

Ad networks, like TACODA, analyze this web-behavior data to predict individual users' consumer needs and likely purchasing behavior.[52] Ad networks collect information in a variety of ways, including direct information from content providers, tracking visits to websites over time, and third-party databases, including off-line data collectors.[53] This information could include simple demographics, financial history, hobbies, and interests.[54] This information is compiled and analyzed for behavior predictions.

For example, ValueClick Media introduced a system in 2008 that uses an automated prediction model to categorize website visitors as belonging to one or more category of consumers such as finance, retail/shopper, or travel/air.[55] This model analyzes the behaviors of more than 130 million Internet visitors each month.[56] Acerno uses a similar database of information and then analyzes the data to find out 1) who customers are and 2) what customers will buy next.[57] This analysis

---

[50] *Id.*

[51] *See* Tager, *supra* note 47: *See also* Acerno: the Add Network, http://www.acerno.com/theaddnetwork.html (last visited October 22, 2009).

[52] *See, e.g.,* Tager, *supra* note 47. *See also* Stephanie Oehlert, *Behavioral Targeting*, SALES AND MARKETING MANAGEMENT MAGAZINE, Jan. 20, 2010, http://www.salesandmarketing.com/msg/content_display/publications/e3ia3a7c2e70e62048d6704c96252adfb6c.

[53] Behavioral Advertising: Industry Practices and Consumer Expectations: Joint Hearing Before the H. Subcomm. on Commerce, Trade, and Consumer Protection and the Subcomm. on Communications, Technology and the Internet, 111th Cong. 2 – 4 (2009) (statement of Edward W. Felton, Professor of Computer Science and Public Affairs, Princeton University).

[54] *Id.*

[55] *See* Tager, *supra* note 47.

[56] *Id.*

[57] *See id. See also* Acerno: The Add Network, http://www.acerno.com/wifnetwork.html (last visited Jan. 23, 2010).

identifies Internet visitors that "look" like an individual company's best customers to target to those individuals most likely to act on the advertisement.[58]

B. Benefits of Targeted Advertising

This data profiling provides significant benefits for consumers, advertisers, and online publishers. One benefit for consumers is the reduction of irrelevant and often repeated advertisements.[59] One commentator said that without this tracking and analysis, our Internet experience "would be like having the same conversation--over and over again."[60] Consequently, advertisers benefit because they can target consumers who are more likely to act on the delivered advertisements; advertisers' efforts and money are not wasted on consumers who have no interest in the product or brand.[61]

Additionally, online advertising supports a variety of content that consumers can access free of charge.[62] The advertising revenue from display ads – $7.6 billion in 2008 – supports staff salaries and infrastructure expenses.[63] Advertising networks provide a more efficient and cost-effective means to acquire advertising revenue, especially for smaller website publishers that do not have the resources to devote to advertising sales.[64]

---

[58] *Id.*

[59] Federal Trade Commission, Online Profiling: A Report to Congress 8 (June 2000), *available at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf [hereinafter "FTC 2000 Report"].

[60] Michael Learmonth, *Tracking Makes Life Easier For Consumers; Scrutiny is Needed but Truth is Web Would be Insufferable Without It*, ADVERTISING AGE 44, July 13, 2009, *available at* http://adage.com/abstract.php?article_id=137869 (subscription required).

[61] FTC 2000 Report, *see supra* note 59, at 9.

[62] NAI, Network Advertising Initiative, Comments submitted to the Federal Trade Commission, Privacy Roundtables (Nov. 6, 2009), *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00019.pdf.

[63] *Id.* at 2.

[64] *Id.* at 3-4.

Advertisers using these services are able to better target their efforts to likely purchasers.[65] This reduces wasted spending aimed at reaching uninterested general audiences. This practice also allows advertisers to analyze consumer response to advertisements and evaluate ad effectiveness. Another economic benefit of online advertising is the flexibility in payment structure; advertisers often pay only for ads that produce a desired result, such as a consumer clicking on the ad or a consumer actually making a purchase on the advertiser's website.

Although behavioral targeting supports further expansion of online content and provides economic benefits to advertisers, web publishers, and consumers, this practice requires the collection of consumer information on a scale that raises serious privacy concerns.

C. Consumer Privacy Protection Concerns

When third parties collect personal information, an individual's privacy interests are implicated. As this personal information is collected, stored, and shared, the control and security of that information is taken away from consumers and entrusted to ad networks and other third parties. Additionally, there is concern that this information will be used to discriminate against consumers with certain online behaviors.

Behavioral advertising networks collect a variety of information about Internet users, including search terms entered, commercial transactions, and websites visited. From this information, ad networks can determine a user's age, income level, whether they have children, and if they live in a city.[66] Data collectors maintain that this information is collected, stored, and analyzed anonymously. However, privacy and consumer advocates argue that this information can be used to identify

---

[65] *Id.* at 5-6.

[66] Stephanie Clifford, *Ads Follow Web Users, and Get More Personal*, N.Y. TIMES, July 30, 2009, *available at* http://www.nytimes.com/2009/07/31/business/media/31privacy.html?partner=rss&emc=rss&pagewanted=all.

individuals and should be protected "so long as it can be linked to a particular computer."[67]

American consumers have expressed unease with customized advertisements that are the result of tracking online behavior.[68] Researchers at the Annenberg Public Policy Center, the Annenberg School for Communication, and the Berkeley Center for Law & Technology conducted an independent survey of one thousand Internet users.[69] The researchers reported that 66 percent of respondents did not want advertisements tailored for them at all.[70] When respondents were told the targeted ads were based on tracking users' behavior over multiple websites, the number increased to 84 percent.[71] The promise of anonymity did not lower concern; 87 percent would either "definitely not allow it" or "probably not allow it."[72] The study further reported that 53 percent of Americans believe businesses and laws protect their

---

[67] Privacy Implications of Online Advertising, Hearing Before the Senate Committee on Commerce, Science, and Transportation, 110th Cong. 4 (Statement of Leslie Harris, President and CEO, Center for Democracy & Technology) (July 9th, 2008), *available at* http://commerce.senate.gov/public/_files/LeslieHarrisCDTOnlinePrivacyTestimony.pdf . *See also* John Eggerton, Consumer Groups Want Constraints on Online Behavorial Advertising, BROADCASTING & CABLE, Sept. 1, 2009, http://www.broadcastingcable.com/article/339171-Consumer_Groups_Want_Constraints_on_Online_Behavioral_Advertising.php.

[68] *See* Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessy, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities That Enable It* (2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214. *See Also* Stephanie Clifford, *Many See Privacy on Web as Big Issue, Survey Says*, N.Y. TIMES, Mar. 15, 2009, *available at* http://www.nytimes.com/2009/03/16/technology/internet/16privacy.html?_r=1&partner=rss&emc=rss&pagewanted=all.

[69] *Id.*

[70] *Id.* at 14.

[71] *Id.*

[72] *Id.* at 16.

information.[73] More than 60 percent of respondents believed that the presence of a privacy policy on a website meant that the site cannot share information about its users without their permission.[74]

There is additional concern over the use of "sensitive data" such as health information and financial records.[75] Ad networks collect information from online searches dealing with health issues, such as "abortion" and "AIDS" as well as content viewed on health-related sites. This is an increasing concern, as a majority of Americans turn to the Internet for health information.[76] The collection of this sensitive information has led to concerns about price discrimination and inequality in service. For example, when a firm in the United Kingdom proposed tracking users to provide targeted advertisements, the creator of the Web, Sir Tim Berners-Lee, was concerned about the disparate impact on some consumers.

> I want to know if I look up a whole lot of books about some form of cancer that that's not going to get to my insurance company and I'm going to find my insurance premium is going to go up by 5% because they've figured I'm looking at those books.[77]

III
INDUSTRY SELF-REGULATION

---

[73] *Id.* at 19; *See also* Clifford, *supra* note 68 (Survey by TRUSTe revealed that 75 percent of respondents believed that more regulation of the Internet was necessary to protect "naïve users.").

[74] Turrow et al., *supra* note 68 at 21.

[75] Ryan Singel, *Internet Ad Industry Begs for Regulation*, WIRED, July 8, 2009, http://www.wired.com/epicenter/2009/07/internet-ad-industry-begs-for-regulation/.

[76] PEW INTERNET & AMERICAN LIFE PROJECT, *Press Release: 61% of American Adults Look Online For Health Information* (June 11, 2009) *available at* http://www.pewinternet.org/Press-Releases/2009/The-Social-Life-of-Health-Information.aspx.

[77] Rory Cellan-Jones, *Web Creator Rejects Net Tracking*, BBC News, Mar. 17, 2008 (quoting Tim Berners-Lee), http://news.bbc.co.uk/2/hi/7299875.stm.

The advertising industry has continuously made efforts at self-regulation for nearly a decade. In 2000, a group of online advertising networks announced the formation of the Network Advertising Initiative (NAI) at a FTC workshop.[78] The NAI is a cooperative of online marketing service providers including, among others, Burst Media, Collaborative Media, Google, TACODA, and 24/7 Real Media.[79] The Federal Trade Commission has supported these efforts at self-regulation, offering some guidance to the industry groups through workshops and guiding principles.[80]

The NAI was the primary industry organization leading the efforts for self-regulation and has released guiding principles for member network advertising companies to follow.[81] In 2000, the NAI issued its first set of self-regulatory principles for online networks to abide by when engaging in online profiling of consumers. However, critics noted that these principles were vague and did not adequately address consumer concerns. For example, the Electronic Privacy Information Center (EPIC)[82] criticized the NAI for creating a default opt-out privacy

---

[78] FTC 2000 Report, *supra* note 59 at 22.

[79] *Id; See also* NETWORK ADVERTISING INITIATIVE, Participating Networks, http://www.networkadvertising.org/participating/ (last visited Sept. 1, 2009).

[80] *See e.g.,* FTC Privacy Workshop, *supra* note 43; Protecting Consumers in the Next Tech-ade (Nov. 7, 2006), *available at* http://www.ftc.gov/bcp/workshops/techade/pdfs/transcript_061107.pdf; Federal Trade Commission, Staff Report: Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles (Dec. 20, 2007), *available at* http://www.ftc.gov/opa/2007/12/principles.shtm [hereinafter "FTC Proposed Principles"]; Staff Report: *Self-Regulatory Principles for Online Behavioral Advertising, Behavioral Advertising: Tracking, Targeting, & Technology*, at 13 – 14 (Federal Trade Commission Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf [hereinafter "FTC 2009 Principles"].

[81] EPIC, National NETWORK ADVERTISING INITIATIVE: Principles not Privacy, July 2000, http://epic.org/privacy/internet/NAI_analysis.html. *See also* NAI, Self-Regulatory Principles for Online Preference Marketing by Network Advertisers (2000), *available at* http://www.ftc.gov/os/2000/07/NAI%207-10%20Final.pdf, amended by NETWORK ADVERTISING INITIATIVE, Self-Regulatory Code of Conduct (2008), *available at* http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf.

protection, which requires users to actively opt-out of data collection. [83] EPIC suggested that a more protective guideline would be an opt-in process, by which users would expressly grant ad networks permission to collect information on their web browsing habits.[84]

The NAI Principles, the only formalized self-regulatory mechanism, continued to draw criticism from various organizations during the FTC's decade-long investigation of online advertising practices.[85] In 2007, the FTC proposed guiding principles for the use of behavioral targeting online.[86] These were finalized in 2009. Two major efforts have been undertaken by the industry to respond to these principles. This section will detail the FTC principles, the NAI Code of Conduct, and the Self-Regulatory Principles for Online Behavioral Advertising developed by a cooperative of professional advertising associations.

A. The Federal Trade Commission's Self-Regulatory Principles

The FTC has been monitoring the use of online tracking since the mid-1990s.[87] It recognized that increased capabilities and use of e-commerce raised serious concerns for consumers including loss of privacy, fraud, and deceptive marketing. In an 1996 Report and Workshop, the FTC cited a 1994 Survey that reported a majority of individuals would be "concerned if an interactive service to which they subscribed engaged in subscriber profiling, i.e., the creation of individual profiles based upon subscribers' usage and purchasing patterns, in order

---

[82] "EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values." About EPIC, http://epic.org/epic/about.html (last visited Jan. 23, 2010).

[83] *See* EPIC, *National Advertising Initiative: Principles not Privacy*, July 2000, *available at* http://epic.org/privacy/internet/NAI_analysis.html [hereinafter "EPIC NAI"].

[84] *Id.*

[85] FTC 2009 Principles, *see supra* note 80 at 13-4.

[86] FTC Proposed Principles, *see supra* note 80.

[87] FTC Privacy Workshop, *supra* note 43.

to advertise to subscribers."[88] The FTC staff recommended that the Commission continue to monitor issues of online privacy, but concluded that self-regulation and technological solutions may be sufficient to protect consumers' privacy in the marketplace.[89]

Since this first workshop on consumer online privacy issues, the FTC has continued to issue findings surrounding e-commerce and online advertising. Throughout this process, the FTC has encouraged the industry to issue self-regulation guidelines to ensure privacy protections for consumers. However, in 2000, the FTC reported to Congress on the issue of online profiling and recommended that Congress legislate this practice to mandate compliance with established fair information practices.[90] Although the FTC praised industry efforts at self-regulation, it noted that not all advertisers and website owners were allied with the organizations issuing these guidelines. Proposed federal legislation would mandate compliance for all websites and advertising networks and provide an agency with the authority to enforce privacy protections.[91]

Congress failed to pass legislation following the FTC's recommendations in 2000. Online advertising continued to be governed primarily by self-regulatory guidelines issued by the NAI. However, the FTC continues to note the importance of monitoring online practices and investigating instances of possible deception and unfair practices associated with commercial activities on the Internet.[92]

The FTC featured behavioral targeting at the 2006 Tech-Ade hearings.[93] Industry experts described how new technologies, such as

---

[88] *Id.*

[89] *Id.*

[90] FTC 2000 Report, *supra* note 59.

[91] Federal Trade Commission, Online Profiling: A Report to Congress Part 2 Recommendations (July 2000), *available at* http://www.ftc.gov/os/2000/07/onlineprofiling.htm [hereinafter "FTC 2000 Recommendations"].

[92] FTC 2009 Principles, *supra* note 80.

[93] "On November 6-8, 2006, the FTC [brought] together experts from the business, government, and technology sectors, consumer advocates, academicians, and law

behavioral targeting networks, were developing to allow advertisers to provide consumers with more relevant advertisements.[94] Marcia Hofmann of the Electronic Frontier Foundation questioned whether industry self-regulation would be enough to protect consumer interests. Hofmann noted that it was in the advertisers' interests to create increasingly detailed consumer profiles but that there were few market forces that would promote consumer privacy.[95]

In the months following the Tech-Ade hearings, the FTC worked to gather more information on behavioral targeting. Objections to this practice increased, and the FTC accelerated its investigations in 2007 when Google, the leading online search engine, announced plans to acquire Double-Click, a leader in online marketing technology.[96] Commentators argued that allowing such a merger would result in the "creation of 'super-profiles,' which will make up the world's single largest repository of both personally and non-personally identifiable information."[97] However, after an investigation into the proposed merger, the FTC allowed the acquisition to continue without imposing any privacy regulations on Google's activities.[98]

---

enforcement officials to explore the ways in which convergence and the globalization of commerce impact consumer protection. The hearings [provided] an opportunity to examine changes that have occurred in marketing and technology over the past decade, and to garner experts' views on coming challenges and opportunities for consumers, businesses, and governmental bodies." Protecting Consumers in the Next Tech-Ade, http://www.ftc.gov/bcp/workshops/techade/what.html (last visited Jan. 23, 2010). *See also Id.* at 8; Protecting Consumers in the Next Tech-ade, *supra* note 80.

[94] Protecting Consumers in the Next Tech-ade, *supra* note 80 at 54-9.

[95] *Id.* at 76-7.

[96] FTC 2009 Principles, *supra* note 80 at 9.

[97] Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief, In re: Google, Inc. and Doubleclick, Inc., F.T.C. No. 071-0170, *available at* http://epic.org/privacy/ftc/google/supp_060607.pdf.

[98] Statement Concerning Google/DoubleClick, No. 071-0170 (2008), *available at* http://ftc.gov/os/caselist/0710170/071220statement.pdf.

Since the Google/Double-Click merger, online profiling has continued to be a standard, yet controversial practice.[99] In response to continuing concerns, the FTC released guiding principles for the self-regulation of online behavioral advertising in February 2009.[100] In this statement, the FTC warned the advertising industry that if self-regulation efforts were not effective, the Commission would take steps to regulate online advertising.[101]

In the FTC Principles, behavioral advertising is defined as "the tracking of a consumer's online activities over time – including the searches the consumer has conducted, the web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer's interests."[102] This definition specifically excludes contextual advertising. The guiding principles focused on transparency, data security, changes in privacy policies, and sensitive data. Websites through which data is collected should have a clear, concise, and prominent statement alerting visitors that the information is being collected for advertising purposes and that visitors may opt-out of this data collection. Website operators are directed to include a user-friendly method to opt-out. The FTC also emphasized consent whenever a company changes its privacy after data collection, and before gathering "sensitive data," such as medical information, for advertising purposes.

Additionally, holders of consumer data should develop and use security protocols to protect the data. The FTC also recommends that companies place limits on the retention of consumer data; it should only be stored "as long as is necessary to fulfill a legitimate business or law enforcement need."[103]

B. NAI Code of Conduct

---

[99] *See, e.g.*, *FTC Clears Google-DoubleClick Merger*, PRIVACY REVOLT, Dec. 21, 2007, http://consumercal.blogspot.com/2007/12/ftc-clears-google-doubleclick-merger.html.

[100] FTC 2009 Principles, *supra* note 80.

[101] *Id.* at 47.

[102] *Id.* at 46.

[103] *Id.* at 47.

Following the release of a draft of the FTC's Proposed Principles for Behavioral Advertising,[104] the NAI revised its principles and issued the Self-Regulatory Code of Conduct.[105] The 2008 Code of Conduct requires all NAI members to adhere to ten key principles, including notice, consumer choice, limitation on the use of information, consumer access to the information, data reliability, data security, and data retention. Critics have said that these principles do not go far enough in protecting consumer privacy. The Center for Democracy and Technology (CDT) specifically criticized the NAI's substandard notice requirements, noting that burying these requirements in a privacy policy is not the most effect method of notifying consumers about data collection practices.[106] Additionally, the CDT expressed concern that the NAI's approved opt-out methods were not user friendly enough to be sufficient protections.[107]

The Code of Conduct incorporates many of the OECD principles.[108] For example, the Code of Conduct requires that members of the NAI ensure that consumers are presented with a clear description of the types of data that will be collected, how that data will be used or transferred to third parties, and if that data will be merged with personally identifying information (PII).[109] Notice must also be provided if privacy policies change.[110] Additionally, the Code of Conduct requires "reasonable

---

[104] FTC Proposed Principles, *supra* note 80.

[105] NETWORK ADVERTISING INITIATIVE, Self-Regulatory Code of Conduct (2008), *available at* http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf [hereinafter "Code of Conduct"].

[106] CENTER FOR DEMOCRACY & TECHNOLOGY, Response to the 2008 NAI Principles: The Network Advertising Initiative's Self Regulatory Code of Conduct for Online Behavioral Advertising (Dec. 16, 2008), available at http://www.cdt.org/privacy/20081216_NAIresponse.pdf.

[107] *Id.*

[108] *See supra* text accompanying notes 13-18.

[109] Code of Conduct, *supra* note 105 at 7. This addresses OECD Principle 3: Purpose Specification.

[110] *Id.* at 9.

security" for all data collected.[111] The Code of Conduct does provide guidance and minimum standards for consumers to opt-out, in most instances, or opt-in, as to sensitive information or, after changes in policy, of data collection and use.[112] Consumers are also provided the right to inspect any PII that a NAI member holds.[113] The NAI members must "make reasonable efforts to ensure that they are obtaining data . . . from reliable sources."[114]

The Code of Conduct successfully addresses the accountability principle by setting out a compliance process. The NAI will review a company's compliance with the Code when 1) it is a new company applying for membership; 2) once annually for all member companies; and 3) when needed in response to a credible, unresolved consumer complaint.[115] The NAI will post an annual compliance review relating to all consumer complaints and any NAI enforcement actions.[116] The Code of Conduct does not specify the procedures for the compliance reviews, but suggests that penalties could include referral to the FTC.[117]

The Code of Conduct does fall short of the OECD principles in several facets. First, it fails to limit data collection in any meaningful way, a key principle of the OECD guidelines.[118] Additionally, although the Code does not adequately address data quality, it does require companies to use "reliable sources" and it provides consumers the right to access any PII held about them. However, there is no such right for

---

[111] *Id.* at 10. This addresses OECD Principle 5: Security Safeguards.

[112] *Id.* at 8. This partially addresses OECD Principle 7: Individual Participation.

[113] *Id.* at 9. This partially addresses OECD Principle 7: Individual Participation.

[114] *Id.* at 10. This partially addresses OECD Principle 2: Data Quality.

[115] *Id.* at 11.

[116] *Id.*

[117] *Id.*

[118] OECD, *supra* note 14. "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject." *Id.* at para 7.

non-PII. Nor is there a specified process for challenging or verifying the accuracy of the stored information. Although the Code references consumer complaints in the accountability section, there is no specific right of the consumer to have information erased or amended.[119]

C. Professional Cooperative Self-Regulatory Principles

Another joint effort has been made by several advertising industry organizations to set industry principles for online advertising. The American Association of Advertising Agencies, the Association of National Advertisers, the Better Business Bureau, the Direct Marketing Association, and the Interactive Advertising Bureau (collectively the Coop) worked to respond to the FTC Proposed Principles and accompanying report. The Self-Regulatory Principles for Online Behavioral Advertising, published by the Coop in July 2009, outlines seven principles: education, transparency, consumer control, data security, material changes, sensitive data, and accountability.[120]

These principles address several of the OECD principles, including limiting the collection of data. The Coop principles prohibit the collection and use of financial account numbers, Social Security Numbers, pharmaceutical prescriptions, and medical records, without consent.[121] The principles also prohibit the collection of "personal information" from or the targeted advertising to children under the age of 13, as required the by the Children's Online Privacy Protection Act (COPPA).[122]

The Coop Principles also require service providers, web site publishers, and third-party advertisers to provide "clear, meaningful, and prominent notice on their own Web sites" that details what types of data are collected for behavioral advertising and what that data will be used for, including whether the data will be transferred to other entities for behavioral advertising.[123] This notice must point consumers to a

---

[119] *Id.* at paras 8, 13.

[120] Coop Principles, *supra* note 4.

[121] *Id.* at 16-7.

[122] *Id.*

mechanism that allows them to choose if information is collected, transferred, or used for behavioral advertising.

Additionally, the Coop Principles require "enhanced" notice by third-party advertisers. This requires advertisers to include a link to their privacy notice on the Web page where the data is collected, including in or around the third party's advertisement.[124] A third-party may meet the enhanced notice requirement by listing itself on an industry Web site providing consumer options for controlling data collection and use.[125]

The Coop Principles place stronger restrictions on Service Providers regarding consumer control. "Service Providers" are defined as entities that provide Internet access, an Internet toolbar, a browser, or "comparable desktop application or client software."[126] When a Service Provider collects and uses consumer data for behavioral advertising, it must obtain consumer consent. The Coop's explanation of this indicates that Service Providers must obtain affirmative consent and continue to provide opportunities for customers to withdraw that consent.

> Recognizing the central role they play, this Principle holds Service Providers to a high standard by requiring that customers take action in response to a clear, meaningful, and prominent notice regarding their Service Provider's collection and use of Web surfing data for Online Behavioral Advertising purposes. It prohibits Service Providers from the collection of data through such service and use of such data . .

---

[123] *Id.* at 12.

[124] *Id.* at 13.

[125] *Id.*

[126] *Id.* at 11.

> . absent their customers' Consent for such purposes.[127]

Although there are strong protections in the Coop Principles, there are areas of concern. These principles, while prohibiting the collection and use of financial account numbers, Social Security numbers, and medical records, ignore the vast amount of sensitive data collected through health-related search terms and website visits. The Coop Principles also fail to address data quality or accuracy. There are no consumer rights to inspect or verify the stored information.

D. Additional Industry Solutions

Individual companies have proposed solutions to concerns raised by privacy advocates. For example, Phorm, an online advertising network publicly traded in the UK, proposed that any ISP partnering with Phorm for data collection or online advertising would provide users with notification and clear opt-out procedures.[128] The UK government had approved implementation of Phorm's tracking system only if users gave their consent and Phorm made it easy for users to opt out.[129] Phorm proposed that once its system was deployed users would see a web-entry page the first time they signed online after deployment.[130] The full-page display would include a notification of what information will be collected and how that information will be used. The page would also provide an opt-out tool for users. Additionally, each page the user browses would contain a banner ad telling users that Phorm's tracking program was on and collecting data.[131] The banner ads would also have an opt-out tool for

---

[127] *Id.* at 36.

[128] Darren Waters, *Ad System 'Will Protect Privacy,'* BBC NEWS, Mar. 6, 2008, http://news.bbc.co.uk/2/hi/technology/7280791.stm.

[129] Darren Waters, *EC starts legal action over Phorm*, BBC NEWS, Apr. 14, 2009, *available at* http://news.bbc.co.uk/2/hi/technology/7998009.stm.

[130] Waters, *supra* note 128.

[131] *Id.*

users to access.[132] However, the European Commission questioned whether these practices would equate to sufficient consent.[133]

European Commission's Consumer Affairs Commissioner Maglena Kuneva, in a keynote address at a European Union roundtable event in Brussels, said that current protections for online users were not sufficient.

> Currently, consumers have little awareness of what data is being collected, how and when it is being collected and what it is used for. And they are also not able to control this process. The current opt-out systems are partial, sometimes nowhere to be found, they are difficult or cumbersome and most of all, they are unstable. Avoiding tracking is currently technically difficult if not impossible.[134]

Google and Yahoo! have both set up consumer controls for their respective behavioral advertising services.[135] Google's Ad Preferences Manager provides consumers with explanations as to why they are receiving certain types of advertisements.[136] The consumer then has the

---

[132] *Id.*

[133] Waters, *supra* note 129.

[134] Jack Marshall, *E.U. Hints Strongly at Tighter Regulation of Online Data Collection*, CLICKZ, Apr. 2, 2009, http://www.clickz.com/3633257.

[135] Google, Ads Preferences Manager, http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/details.html. Yahoo, Ad Interest Manager, http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/details.html; *See also* Rebecca Lieb, *Google Raises the Behavioral Bar*, CLICKZ, Mar. 13, 2009, http://www.clickz.com/3633076; Joelle Tessler, *Yahoo Launches Online Consumer-Privacy Tool*, ENTERPRISE SECURITY TODAY, Dec. 9, 2009, http://www.enterprise-security-today.com/news/Yahoo-Debuts-Consumer-Privacy-Tool/story.xhtml?story_id=033002FCYKH3.

[136] *See* Google Ads Preferences Manager, *supra* note 135.

option to control the categories of advertisements he or she receives, such as business, entertainment, investing, and current events.[137] Google also provides on this page the opportunity to opt-out of cookie-based tracking.[138] Yahoo's Ad Interest Manager works in a similar way.[139]

These preference manager tools provide consumers with some control over whether information is collected and how it is used. However, they do not allow consumers to see the total online profile created by Google or Yahoo!. Consumers see the end result – that, based on tracking data, Google has decided if he or she is interested in Business News or Entertainment-Movies. The tool does not allow a consumer to inspect the underlying data used for that analysis for accuracy, or the opportunity to challenge the accuracy of that information.

IV
INCREASED FEDERAL EFFORTS AND THE NATIONAL BROADBAND PLAN

Immediately following the release of the FTC Self-Regulatory Principles, Rep. Rick Boucher stated that self-regulation "is not sufficient."[140] Rep. Boucher said that national privacy protections are "fundamental" to the expansion of broadband technologies.[141] He has since led the efforts in Congress for hearings and legislation on this issue. The House Committee on Energy and Commerce Subcommittees on Communications, Technology and the Internet and on Commerce, Trade, and Consumer Protection held a joint hearing in June 2009 discussing the practice and privacy implications of behavioral targeting.[142]

---

[137] *See id.*

[138] *See id.*

[139] *See* Yahoo Ad Interest Manager, *supra* note 135.

[140] Emily Steel, *Rep. Boucher Calls for Internet Ad Regulation,* WSJ.COM, Feb. 13, 2009, http://blogs.wsj.com/digits/2009/02/13/rep-boucher-calls-for-internet-ad-regulation/.

[141] *See id.*

[142] 155 CONG. REC. D718 (daily ed. June 18, 2009) (hearing before the H. Subcommittee on Commerce, Trade and Consumer Protection and the H. Subcommittee

Several members of Congress have asked for input on a bill to protect online privacy.[143] Although hearings have been held on the issues of online privacy and behavioral advertising, no bill had been introduced at the time of this writing. Rep. Boucher has reported that he is drafting legislation to address these issues.[144]

The FTC has supported industry self regulation, although statements from Chairman Jon Leibowitz and David Vladeck, the head of the FTC Bureau of Consumer Protection, signal a more aggressive, regulatory approach.[145] The FTC held the first of three roundtable events on Internet privacy issues, including behavioral targeting, on Dec. 7, 2009, to further explore these issues.[146]

During the development of the National Broadband Plan, the FCC had an opportunity to address this issue as part of a comprehensive protection plan for online consumers. Congress has charged the FCC with developing a National Broadband Plan for "use of broadband infrastructure and services in advancing consumer welfare, civic participation, public safety and homeland security, community development, health care delivery, energy independence and efficiency, education, worker training, private sector investment, entrepreneurial

---

on Communications, Technology and the Internet: Behavioral Advertising: Industry Practices and Consumers' Expectations).

[143] John Eggerton, Broadcasting & Cable, Sept. 1, 2009, http://www.broadcastingcable.com/article/339171-*Consumer_ Groups_ Want_ Constraints_ on_ Online_ Behavioral_ Advertising*.php., BROADCASTING & CABLE, Sept. 1, 2009, *available at* http://www.broadcastingcable.com/article/339171-Consumer_Groups_Want_Constraints_on_Online_Behavioral_Advertising.php.

[144] Rick Boucher, Behavioral Advertising: The Need for Privacy Protection, Sept. 23, 2009, http://www.boucher.house.gov/index.php?option=com_content&task=view&id=1833&Itemid=38&layout=default&view=article&date=2010-01-01.

[145] *See, e.g.,* Douglas MacMillan, *The FTC Takes on Targeted Web Ads*, BUSINESSWEEK, Aug. 2, 2009; Stephanie Clifford, *Fresh Views at Agency Overseeing Online Ads*, N.Y. TIMES, Aug. 5, 2009.

[146] Federal Trade Commission, *Exploring Privacy: A Roundtable Series*, http://www.ftc.gov/bcp/workshops/privacyroundtables/ (last visited Dec. 9, 2009).

activity, job creation and economic growth, and other national purposes."[147] In promotion of this effort, the FCC issued the Notice of Inquiry in which the Commission has asked for input on each of those goals, as well as the affordability, efficacy and efficiency, and status of broadband deployment.[148]

Consumer privacy is an issue that the Commission raised in several areas of the NOI. In one instance, the FCC specifically noted the concerns that have been raised regarding behavioral advertising and other web tracking practices. The FTC submitted comments to the FCC in response to the NOI.[149] The FTC emphasized the importance of privacy protections and noted the industry guidelines it had promulgated.[150] The FTC statement urged the FCC to "incorporate sound . . . consumer protection principles as the foundation for the Broadband Plan."[151]

Consumer advocacy organizations submitted comments that urged the FCC to regulate behavioral advertising. The Electronic Privacy Information Center[152] submitted comments that focused on the need for more effective notice of data collection, citing a Consumer Reports poll that reported 61 percent of Internet users "are confident that what they do online is private and not shared without their permission."[153] EPIC argued that because users are unaware their information is collected and shared, traditional opt-out protections supported by industry guidelines

---

[147] American Recovery and Reinvestment Act of 2009, *supra* note 40.

[148] FCC NOI, *supra* note 1.

[149] Federal Trade Commission, FTC, Comments of the FTC, Sept. 4, 2009 (In Response to FCC NOI, GN Docket 09-51, April 8, 2009) *available at* http://www.ftc.gov/os/2009/09/090904fccnbp.pdf.

[150] *Id.* at 14-5.

[151] *Id.* at 17.

[152] EPIC, *Supra*, note 82.

[153] EPIC, Comments of the Electronic Privacy Information Center at 10, June 6th 2009, (In Reponse to FCC NOI, GN Docket 09-51, April 8, 2009) *available at* http://epic.org/privacy/pdf/fcc_broadband_6-8-09.pdf.

are not sufficient. EPIC urged the FCC to "exercise greater oversight of practices in the online advertising" industry.[154]

The Center for Digital Democracy, Privacy Rights Clearinghouse, and U.S. PIRG, collectively commented that FCC intervention is necessary to "alleviate consumer confusion and ensure adequate privacy and security protection of consumer data."[155] These organizations argued that industry self-regulation has been "totally inadequate" because privacy policies are long and ineffective.[156] The consumer groups cited a 2008 study that reported that "if all American Internet users were to annually read the online privacy policies word-for-word each time they visited a new site" users would spend "33 minutes a day … approximately 46% of the estimated 72 minutes a day people spend using the Internet."[157] The consumer groups urged the FCC to "step in" and address broadband privacy issues.[158]

V
DISCUSSION AND CONCLUSIONS

Although the advertising industry has responded to calls from consumers and the FTC for more effective self-regulation, some government regulation of data collection and use is needed. The 2003 OECD report on online privacy, stated that a hybrid of government-enforced legislation and industry-led self regulation is the best solution for protecting privacy in the online environment.[159] In the absence of comprehensive privacy legislation, the FCC should take this opportunity

---

[154] *Id.*

[155] CENTER FOR DIGITAL DEMOCRACY, PRIVACY RIGHTS CLEARINGHOUSE, & U.S. PIRG, Comments of the Center For Digital Democracy, et. al. at 6, June 8 2009 (In Response to FCC NOI, GN Docket 09-51, April 8, 2009) *available at* http://www.democraticmedia.org/files/privacy-fcc-060809.pdf.

[156] *Id.* at 1-2.

[157] *Id.* at 11.

[158] *Id.* at 13.

[159] OECD, *Report on Compliance With, and Enforcement of, Privacy Protection Online*, *supra* note 18.

to include recommendations for consumer privacy protections in the broadband plan that conform to OECD Guidelines.

Protections should provide specific guidance to entities that collect data from online consumers. These should include prescribed methods for effective notice to consumers, specific limitations on data retention, and an effective means for consumers to control what, if any, data is collected.

Policies should place reasonable limits on the personal data collected. Most data aggregators currently store and analyze this data anonymously. Federal policy should mandate this as a continued practice. However, it should also restrict the collection of sensitive data, including medical and financial information. Collection also should be limited to data collected with the consent of the user. Traditional notice and consent schemes have not been effective on the Internet. Privacy policies that comply with current industry standards are difficult to understand, and often difficult to find. David Vladeck, head of the Bureau of Consumer Protection at the FTC, doesn't "believe that most consumers either read them, or if they read them, really understand it."[160] The FCC should work with the FTC, industry representatives, consumer and privacy advocates to develop a framework for more practicable notification schemes to ensure consumers are fully informed.

Another key concern is the opt-out policy. Privacy advocates have argued that opt-in schemes are the only adequate approach to protecting consumer privacy. Industry representatives argue that this will disrupt the business model of online communications. One problem with privacy policies and opt-out tools is that they are diversified across sites. Some commentators have suggested that the FTC or the FCC institute a Do-Not- Track List, operating similarly to the Do-Not-Call Registry for telemarketing. In 2007, the Center for Democracy and Technology and other consumer and privacy groups wrote in a letter to the FTC that creating and maintaining this list would allow consumers to effectively block in one action the behavioral tracking activities of advertisers.[161]

---

[160] Clifford, *supra* note 68.

[161] Ari Schwartz, et. al., In advance of the FTC Town Hall, "Ehavioral Advertising: Tracking, Targeting, and Technology," to be held November 1-2, 2007 in Washington, D.C., *available at*

Another solution may be to make the Internet Service Providers that participate in ad networks responsible for this. This was the model proposed by Phorm in the United Kingdom that privacy advocates said would provide users with an unavoidable notice page and easy-access opt-out tools. This approach is also evident in the stringent consent requirement for Service Providers in the Coop Principles. However, the FCC and the FTC should investigate the viability of these options, as well as an opt-in approach, with respect to the goal promoting of competition and innovation.

Another issue that current self-regulatory guidelines, including the FTC's principles, do not address is the inspection and correction of data. Policies should guarantee that consumers have the right to receive copies of data held specifically relating to them, and to have any inaccurate data erased or amended to accurately reflect the individual. Consumers already have this right for data maintained by credit reporting agencies. This inclusion would further the principles of individual participation set out in the OECD guidelines.

The FCC should take this opportunity to recommend legislation that would grant the FTC and the FCC specific authority to implement and enforce these consumer privacy principles. Any such legislation or agency regulation should continue to incorporate self-regulation as a continued resource for privacy protection. While it should not be the only protection available to consumers, self-regulation is an important element. The FCC should continue to consult with the FTC in the development of these regulations to provide consumers and the industry a consistent framework for enforcing privacy rights online.

---

http://www.worldprivacyforum.org/pdf/ConsumerProtections_FTC_ConsensusDoc_Final_s.pdf.