From: Consumer advocacy groups Date: January 22, 2010
To: Federal Communications Commission
RE: Comments – NBP Public Notice #29; GN Docket Nos. 09-47, 09-51, and 09-137

---

## Introduction

The American Civil Liberties Union, Center for Digital Democracy, Consumer Action, Consumer Federation of America, Consumer Watchdog, Privacy Lives, Privacy Rights Clearinghouse, Privacy Times, and U.S. PIRG (collectively, "Consumer advocacy groups") submit these comments to the Federal Communications Commission ("FCC") concerning consumer privacy as part of NBP Public Notice #29; GN Docket Nos. 09-47, 09-51, and 09-137.[1] The FCC seeks comment "on the use of personal information, identity management services, and privacy protection against broadband applications."[2]

In these comments we will explain: (1) There are significant problems concerning the collection and use of personal data by companies, especially sensitive data and children's data; (2) The FCC should not rely on industry self-regulatory models because they do not adequately protect consumer privacy; and (3) The principles and standards that should serve as the foundation of consumer privacy protection should be the Fair Information Practices, especially as they are implemented in the OECD Guidelines on data privacy.

The issue of consumer privacy protection is vitally important. The FCC should consider all avenues it may use to protect consumers, including exercising its ancillary jurisdiction to address broadband privacy issues, and working with Congress and the Federal Trade Commission ("FTC"), which has substantial expertise in consumer privacy protection.

## I. There Are Significant Privacy Problems in the Collection and Use of Consumers' Personal Data Through Broadband and Mobile Services

We are encouraged that the FCC has sought to understand how or if consumer privacy is protected while they are using online, including broadband, and mobile services. The FCC has discussed consumer privacy as part of the wireless consumer

---

[1] Fed. Commc'ns Comm'n, *Comments Sought on Privacy Issues Raised by the Center for Democracy and Technology,* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-10-62A1.pdf.
[2] *Id*.

information and disclosure "Truth in Billing" debate[3] and as part of the national broadband plan.[4] There is a need for such scrutiny by the FCC, because consumers remain confused about data collection by companies and privacy risks inherent in such data collection, use and distribution, and there is widespread data collection (especially of children's information) in broadband and mobile industry.[5]

### A. Consumers Remain Confused About Data Collection by Companies and Privacy Risks Inherent in Such Data Collection, Use and Distribution

Studies show that consumers are concerned about online privacy, eschewing intrusive data collection and sharing, and customer-profile creation, when they learn of such practices. However, most consumers do not know about these types of data collection and sharing, nor do they understand the privacy and security risks that are part of online commerce.[6] And young consumers especially have difficulty understanding these risks, as children and adolescents are at a developmental disadvantage to give meaningful and informed consent to collection of their personal data.

A 2008 poll from the Consumer Reports National Research Center found "72 percent are concerned that their online behaviors were being tracked and profiled by companies."[7] The poll also found, "93 percent of Americans think internet companies should always ask for permission before using personal information and 72 percent want

---

[3] Fed. Commc'ns Comm'n, Notice of Inquiry: In the Matter of Consumer Information and Disclosure, Truth-in-Billing and Billing Format, IP-Enabled Services, CG Docket No. 158, CC Docket No. 98-170 and WC Docket 04-36) Aug. 28, 2009, available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-68A1.pdf.

[4] Fed. Commc'ns Comm'n, *Notice of Inquiry: In the Matter of a National Broadband Plan for Our Future, GN Docket No. 09-51,* Apr. 8, 2009, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-31A1.pdf (viewed Jan. 16, 2010).

[5] For detailed information about consumer privacy problems with mobile advertisers, see Ctr. for Digital Democracy and U.S. PIRG, Complaint and Request to the Federal Trade Commission for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Mobile Marketing Practices, Jan. 13, 2009, available at http://democraticmedia.org/files/FTCmobile_complaint0109.pdf (viewed Jan. 16, 2010).

[6] *See also*, Ctr. for the Digital Future, Univ. of S. Cal., *Surveying the Digital Future: Survey Highlights,* Apr. 28, 2009, *available at* http://www.digitalcenter.org/pdf/2009_Digital_Future_Project_Release_Highlights.pdf (viewed Jan. 16, 2010). "Almost all respondents continue to report some level of concern about the privacy of their personal information when or if they buy on the Internet," and 93 percent of respondents "reported some level of concern about the privacy of personal information (somewhat, very, or extremely concerned)."

[7] Consumers Union, *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy*, Sept. 25, 2008 (hereinafter "Consumer Reports Poll 2008"), *available at* http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html (viewed Jan. 16, 2010).

the right to opt out when companies track their online behavior."[8] The survey showed that consumer trust does affect their online behavior. "For example, over one-third (35%) use alternate email addresses to avoid providing real information; over one-quarter (26%) have used software that hides their identity; and one-quarter have provided fake information to access a website (25%)."[9]

A 2008 Harris Interactive poll found that U.S. consumers "are skeptical about the practice of websites using information about a person's online activity to customize website content."[10] For example, "A six in ten majority (59%) are not comfortable when websites like Google, Yahoo! and Microsoft (MSN) use information about a person's online activity to tailor advertisements or content based on a person's hobbies or interests."[11] These respondents said they were uncomfortable even though the question noted these sites "are able to provide free search engines or free e-mail accounts because of the income they receive from advertisers trying to reach users on their websites."[12]

The 2008 Consumer Reports survey also shows that there is confusion among consumers about companies' privacy policies and practices.[13] Consumer Reports found: "61% are confident that what they do online is private and not shared without their permission"; "57% incorrectly believe that companies must identify themselves and indicate why they are collecting data and whether they intend to share it with other organizations"; and, "43% incorrectly believe a court order is required to monitor activities online."[14]

Research by the University of Pennsylvania's Annenberg School of Communication and the University of California at Berkeley Law School's Samuelson Law, Technology & Public Policy Clinic has found confusion about customer data and customer privacy protections offered by businesses. A September 2009 study by the universities revealed consumer confusion about how, when or if their data is protected. "Americans mistakenly believe that current government laws restrict companies from

---

[8] *Id*.
[9] *Id*.
[10] Harris Interactive, *The Harris Poll #40,* Apr. 10, 2008, *available at* http://www.harrisinteractive.com/harris_poll/index.asp?PID=894.
[11] *Id*.
[12] *Id*.
[13] Consumer Reports Poll 2008, *supra* note 7.
[14] *Id*.

selling wide-ranging data about them. When asked true-false questions about companies' rights to share and sell information about their activities online and off, respondents on average answer only 1.5 of 5 online laws and 1.7 of the 4 offline laws correctly because they falsely assume government regulations prohibit the sale of data."[15]

### B. Widespread Personal Data Collection in Broadband and Mobile Industry Underscores Need for Strong Consumer Privacy Protections

The online advertising business has witnessed dramatic consolidation over the last several years; major interactive giants have combined with leading data targeting companies. Google now operates DoubleClick; Yahoo acquired Blue Lithium and Right Media; Microsoft bought aQuantive, Screen Tonic and ADECN; Time Warner's AOL acquired Tacoda and Third Screen Media; and Adobe acquired Omniture. As a consequence of this consolidation, a handful of companies engaged in data collection that track, profile, and target users across Web sites, mobile applications, online games, virtual worlds, and search engines are playing an important role shaping the Internet's future. Given the tremendous data collection capabilities inherent in digital marketing, and the growing concentration of influence by a few companies, there is a strong need for regulatory or legislative action to protect consumer privacy.[16]

For these comments, it is necessary to define the terms we are using concerning the online and mobile advertising industry. "Behavioral targeting" is the practice of collecting and compiling data from and about an individual's activities, interests, preferences, behaviors, or communications for interactive advertising and marketing targeted to the individual, including but not limited to the use of a profile that may be

---

[15] Univ. of Penn., Univ. of Cal. at Berkeley, *Americans Reject Tailored Advertising and Three Activities that Enable It,* 3, Sept. 2009, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214 (viewed Jan. 16, 2010). For more on consumer confusion and attitudes about online privacy, *see* Joseph Turow, Deirdre K. Mulligan & Chris Jay Hoofnagle, Univ. of Pa.'s Annenberg Sch. for Commc'n & U.C.-Berkeley Law's Samuelson Law, Tech. & Pub. Policy Clinic, *Research Report: Consumers Fundamentally Misunderstand The Online Advertising Marketplace*, 1, Oct. 2007, (hereinafter "Annenberg/Samuelson Online Ad Surveys") *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/annenberg_samuelson_advertising.pdf (viewed Jan. 16, 2010).

[16] For more information on threats to consumer privacy from targeted behavioral advertising, *see* Ctr. for Digital Democracy and U.S. PIRG, *Cookie Wars, Real-Time Targeting and Proprietary Self-Learning Algorithms: Why the FTC Must Act Swiftly to Protect Consumer Privacy*, Nov. 4, 2009, *available at* http://www.democraticmedia.org/node/419 (viewed Jan. 16, 2010).

stored or linked to a browser cookie, IP address, or any other persistent user identifiers or tracking methods. Behavioral targeting does not include "contextual advertising," which does not involve the maintenance or storage of information about an individual beyond the current online session with a Web site or series of Web sites.

According to a 2008 *New York Times* report on behavioral targeting, five U.S. companies alone – Yahoo, Google, Microsoft, AOL and MySpace – record at least 336 billion data "events" each month.[17] The personalized targeting that results from this vast stockpile of digital data has become a veritable goldmine.

In the absence of strong consumer privacy regulations, online advertisers will continue to mine consumer data, developing increasingly detailed user profiles and sharing their findings with partners and affiliates. One example of a broadband provider using consumer data for behavioral targeting advertising is Comcast, which uses, Nitro "a proprietary engagement engine" from custom-game designer Bunchball. Bunchball "enables brands to cost-effectively measure and drive consumers' most valuable behaviors," according to the company's Web site.[18]

Nitro claims to "leverage human desires."[19] "People have fundamental needs and desires – for reward, status, achievement, self-expression, competition, and altruism among others. These needs are universal, and cross generations, demographics, cultures and genders," explains Bunchball.[20] "There's a secret, and game designers have known it for years. There are mechanics that you can use to address these needs, and in the process incent, motivate and engage your users. Nitro gives you the power to leverage these mechanics for your brands and online properties."[21]

Bunchball hails its work with the Comcast.net portal site as one of its success stories. Comcast used Nitro "to increase page views and advertising impressions, and to increase the number of Comcast subscribers who were registering and logging in to

---

[17] Louise Story, *To Aim Ads, Web Is Keeping Closer Eye on You,* N.Y. Times, Mar. 10, 2008, *available at* http://www.nytimes.com/2008/03/10/technology/10privacy.html (viewed Jan. 16, 2010).
[18] Bunchball, About Us, http://www.bunchball.com/about/ (viewed Jan. 16, 2010).
[19] Bunchball, How Nitro Works, http://www.bunchball.com/products/nitroworks.shtml (viewed Jan. 16, 2010).
[20] *Id*.
[21] *Id*.

Comcast.net, rather than surfing anonymously."[22] Bunchball says, "the Nitro program on Comcast.net has been successful and can be clearly tied to metrics-driven results, including high member conversion and an increase in page views per unique visitor."[23] These metrics, in turn, are also used to segment users into increasingly detailed consumer niches, which can include children and adolescents.

We must highlight that the concerns about privacy intensify when companies gather data on minors. Children and adolescents have difficulty understanding privacy policies, are at a developmental disadvantage to give meaningful and informed consent to collection of their personal data, and lack the capacity to make informed decisions regarding the trade-offs between privacy and online services.

In an April 2009 article in the Journal of Adolescent Health, Kathryn C. Montgomery and Jeffrey Chester detailed the targeting of behavioral advertising to children and adolescents.[24] "The growth of residential broadband use, the emergence of the 'mobile Web' and wireless networks, and a range of services, such as instant messaging and texting, have created an 'always-on' Internet experience," they wrote. [25] "Marketers are designing campaigns that take advantage of young peoples' constant connectivity to technology, their multi-tasking behaviors, and the fluidity of their media experiences. This '360 strategy' is one of the core principles of contemporary youth marketing, aimed at reaching viewers and users repeatedly wherever they are – in cyberspace, listening to music via a portable player, or watching television."[26]

Problems connected with targeting ads to children and adolescents were detailed in comments to the Federal Trade Commission in April 2008, organizations including the American Academy of Child and Adolescent Psychiatry, the American Academy of Pediatrics, the Center for Digital Democracy and the Institute for Public Representation

---

[22] Bunchball, Comcast Success Story, http://www.bunchball.com/customers/comcast.shtml (viewed Jan. 16, 2010).
[23] *Id*.
[24] Kathryn C. Montgomery and Jeffrey Chester, *Interactive Food and Beverage Marketing: Targeting Adolescents in the Digital Age,* J. of Adolescent Health 45 (2009), *available at* http://digitalads.org/ (viewed Jan. 16, 2010).
[25] *Id*. at S20.
[26] *Id*. For more on the wide range of interactive marketing techniques that target children and adolescents, techniques that are also linked to the U.S. obesity crisis, *see* http://www.digitalads.org/updates.php (viewed Jan. 16, 2010).

at Georgetown University Law Center.[27] The groups explained that the problems would only continue, because "children and adolescents are increasingly attractive demographics for online advertisers. Youth have the highest percentage of internet access: 93 percent of Americans between twelve and seventeen years of age use the internet … Children ages six to twelve spend approximately $40 billion annually and influence $200 billion more of family spending."[28]

"Even when children recognize that they are the target of marketing influence," explains Louis J. Moses, a psychology professor at University of Oregon.[29] "They may nonetheless have difficulty defending against what may be quite powerful marketing tactics. Unlike much of traditional advertising, digital marketing environments tend to be interactive, immersive, alluring, engaging, and motivationally and emotionally rewarding. They also offer the opportunity for individuals to 'play' with products for extended periods of time. Moreover, marketers continue to enhance these characteristics as the capacity grows to tailor marketing to specific demographics and specific individuals."[30]

The FCC has an obligation to protect youth from harmful and unfair marketing practices. The FCC should investigate the data collection and profiling of both children and adolescents, with a particular focus on the role broadcast, cable, phone networks, and major online providers play in the collection and use of data from youth for interactive marketing purposes.

---

[27] Angela J. Campbell and Coriell S. Wright, Inst. for Pub. Representation, Georgetown Univ. Law Ctr., *Online Behavioral Advertising Principles Comment* (Apr. 11, 2008), *available at* http://www.democraticmedia.org/files/Children's%20Advocacy%20Groups%20%20Behavioral%20Advertising%20Comments%20FINAL.pdf (viewed Jan. 16, 2010); *see also* Ctr. for Digital Democracy and U.S. PIRG, *Supplemental Statement to the Federal Trade Commission In Support of Complaint and Request for Inquiry and Injunctive Relief Concerning and Deceptive Online Marketing Practices* (Nov. 1, 2007), *available at* http://www.democraticmedia.org/files/FTCsupplemental_statement1107.pdf (viewed Jan. 16, 2010).

[28] Campbell and Wright, *supra* note 27 at 3.

[29] Louis J. Moses, *Research on Child Development: Implications for How Children Understand and Cope with Digital Marketing* 5, Memo prepared for the Second NPLAN/BMSG Meeting on Digital Media and Marketing to Children for the NPLAN Marketing to Children Learning Community, Berkeley, CA, June 29-30, 2009, *available at* http://www.digitalads.org/documents/Moses_NPLAN_BMSG_memo.pdf (viewed Jan. 16, 2010).

[30] *Id*.

## II. FCC Should Not Use Industry Self-Regulatory Models Because the Online Marketing Industry's Practices Do Not Adequately Protect Consumer Privacy

The U.S. Interactive Advertising Bureau ("IAB"), the online marketing industry's principal trade and lobbying group, has pointed to self-regulatory principles, released in July, which the online marketing industry says shows an effort to improve consumer privacy protection by following the FTC's promulgated self-regulatory principles.[31] However, for several reasons, these industry-imposed self-regulatory principles do little to protect consumer privacy. The Network Advertising Initiative, "a cooperative of online marketing and analytics companies committed to building consumer awareness and establishing responsible business and data management practices and standards," also has developed "actionable self-regulatory standards that establish and reward responsible marketing behavior."[32] Those self-regulatory standards do not adequately protect consumer privacy rights.[33] Also, the marketing industry continues to hide behind the cloak of data "anonymization" or "de-identification," stating that this protects consumer privacy while allowing companies to build profiles on consumers. However, as we explain below, it has proved relatively easy to link anonymized or de-identified data back to personally identifiable information of individuals.

These problems within the industry unfortunately show that the FTC's self-regulatory principles (released last year)[34] have not worked to convince the online marketing industry to improve its consumer protections. The FCC should not use the industry's self-regulatory standards as a model for strong consumer privacy protection.

---

[31] Interactive Adver. Bureau, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009) (hereinafter "IAB Self-Regulatory Principles"), *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf (viewed Jan. 16, 2010).

[32] Network Adver. Initiative, About the NAI, http://www.networkadvertising.org/about/ (viewed Jan. 16, 2010).

[33] For a detailed survey of the failure of the Federal Trade Commission's earlier effort to work with the industry to self-regulate, *see* Pam Dixon, World Privacy Forum, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation* (Nov. 2007), *available at* http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf (viewed Jan. 16, 2010).

[34] FTC, *FTC Staff Report: Self Regulatory Principles for Online Behavioral Advertising* (Feb. 12, 2009) (hereinafter "FTC Report on Self-Regulatory Principles"), *available at* http://www2.ftc.gov/os/2009/02/P085400behavadreport.pdf (viewed Jan. 16, 2010).

### A. Industry's Self-Regulatory Principles Do Not Ensure Proper Protection of Consumer Privacy

The only change of note in the revised IAB self-regulatory principles seems to be an "enhanced notice" proposal. "Links to consumer notices will be clear, prominent, and conveniently located," for any businesses that voluntarily follow these principles.[35] Though we support improved transparency, this is not enough. The online marketing industry is merely providing an easier way for consumers to reach long and difficult-to-understand notices. Unless the notices are easier to understand, it will not matter if there are larger links to them on Web sites. Before any consumer data is collected, the users need to be candidly informed about the process – how their profile is created; how their profile evolves as more personal data is collected; how tracking and data gathering occurs site to site; and what data can be added to their profile from outside databases.

Another failure of the IAB self-regulatory principles is its narrow definitions of "sensitive data" and "personally identifiable data." The principles ask industry members not to collect "sensitive data," which the industry construes as (1) "personal information" of children under age 13 and (2) "financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records about a specific individual."[36] The principles do allow for the collection and use of the second category – health and financial data – if a user consents to the collection and use.[37] This would permit widespread data collection involving personal information regarding our health and financial concerns based on consent that is gathered via complicated privacy notices and the user consent is most likely to be unknowing or confused. The IAB's definition is similar to that of the National Advertising Initiative, which in its 2008 self-regulatory principles, defined "sensitive consumer information" in the narrowest of terms:

SENSITIVE CONSUMER INFORMATION INCLUDES:

- Social Security Numbers or other Government-issued identifiers
- Insurance plan numbers
- Financial account numbers

---

[35] IAB Self-Regulatory Principles at 5, *supra* note 31.
[36] *Id*. at 16-17.
[37] *Id*. at 17.

- Information that describes the precise real-time geographic location of an individual derived through location-based services such as through GPS-enabled devices
- Precise information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history.[38]

There is a substantial need for the FCC and the FTC to define "sensitive information." It should include data about health, finances, ethnicity, race, sexual orientation, personal relationships and political activity. Sensitive information should not be collected or used for behavioral tracking or targeting.

The IAB and NAI also have narrow definitions of "personally identifiable information. From the IAB self-regulatory principles:

> PERSONALLY IDENTIFIABLE INFORMATION "PII"
>
> Personally Identifiable Information is information about a specific individual including name, address, telephone number, and email address -- when used to identify a particular individual.[39]

From the NAI principles:

> PERSONALLY-IDENTIFIABLE INFORMATION ("PII")
>
> PII includes name, address, telephone number, email address, financial account number, government-issued identifier, and any other data used or intended to be used to identify, contact or precisely locate a person.[40]

Both definitions focus on the traditional sense of personally identifiable data – identification numbers or geographic addresses. These narrow definitions of personally identifiable information are in stark contrast to the FTC's vision. The agency has said, "Indeed, in the context of online behavioral advertising, rapidly changing technologies and other factors have made the line between personally identifiable and non-personally identifiable information increasingly unclear."[41] We agree with this assessment. Individuals should be protected even if the information collected about them in behavioral tracking cannot be linked to their names, addresses, or other traditional

---

[38] Network Adver. Initiative, *2008 NAI Principles*, 6 (2008) (hereinafter "NAI Principles"), *available at* http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf (viewed Jan. 16, 2010).
[39] IAB Self-Regulatory Principles at 11, *supra* note 31.
[40] NAI Principles at 5, *supra* note 38.
[41] FTC Report on Self-Regulatory Principles at iii, *supra* note 34.

"personally identifiable information," as long as they can be distinguished as a particular computer user based on their profile.

The final and most important point where the IAB's self-regulatory principles fail is enforcement. Before the latest self-regulatory principles released by the IAB, one of its representatives made clear the lack of meaningful enforcement at the FTC's "Ehavioral Advertising Tracking, Targeting & Technology" workshop in November 2007. In response to the question, "And do you do anything to enforce the standards?" (referring to IAB's best practices on consumer privacy), IAB executive Michael Zaneis said, "It's just best practice, it's not regulatory. We don't kick people out necessarily. We have been looking at the potential for – we certainly have partnered with TRUSTe on a number of their programs. As I said, we support NAI and DMA and OPA, but we've looked at maybe seeing if it's feasible to roll out some sort of privacy compliance program, whether it's a privacy seal or something like that working with – similar to what you see BBB online doing."[42]

There is no enforcement provision in the latest IAB self-regulatory principles. Non-compliance merely results in "public reporting" of non-compliance.[43] Companies could ignore the principles wholesale without facing meaningful penalties. Clearly, the IAB's latest self-regulatory principles are merely for public relations, rather than consumer protection, and the organization does not have meaningful enforcement of the privacy standards they tout.

We continue to urge that enforcement provisions have teeth, that there be meaningful consequences for companies that fail to protect consumer privacy. The FTC agrees with us. It has said, "Self-regulation can work only if concerned industry members actively monitor compliance and ensure that violations have consequences."[44] We firmly believe that the FCC should work with the FTC to create mandatory regulations for the marketing industry, based on the Fair Information Practices, and follow up with meaningful enforcement of these regulations.

---

[42] Fed. Trade Comm'n, *Transcript of Town Hall Record for "Ehavioral Advertising: Tracking, Targeting & Technology"* 157-58 (Nov. 2, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/71102wor.pdf (viewed Jan. 16, 2010).
[43] IAB Self-Regulatory Principles at 18, *supra* note *supra* note 31.
[44] FTC Report on Self-Regulatory Principles at 47, *supra* note 34.

### B. Marketing Industry Hides Behind Cloak of "Anonymization," but "Anonymized" Data Has Been Linked Back to Individuals

As we explained above, the online and mobile advertising industry has narrow definitions of "sensitive data" and "personally identifiable information," which do not adequately encompass the reality of consumer data collection and consumer profile creations. "Personally identifiable information," as defined by the advertising industry, is restricted to names, addresses, ID numbers, or other traditional personally identifiable information.

Online marketers have deployed an elaborate system of digital surveillance on consumers that tracks, compiles, and analyzes our movements across the Internet, from log-on to sign-off. Consumers' online activities and experiences are monitored, with data about our "behaviors" used to compile "profiles" controlled by marketers and third parties. While the rationale for behavioral advertising is that it helps generate more targeted – and supposedly more relevant – ads, it's really a form of uninvited digital intrusion into our lives. Think of all the products, services and information you seek online – such as inquiring about mortgages and credit cards or health remedies. With behavioral targeting, marketers and others stealthily collect and analyze details about your life – and this profile is made available to others, so they can target you with interactive advertising.

The industry definition of behavioral targeting puts marketers' goals in context. Marketers continually argue that behavioral targeting is not really targeted to an individual and is relatively harmless. But, the IAB defines behavioral targeting as, "A technique used by online publishers and advertisers to increase the effectiveness of their campaigns. Behavioral targeting uses information collected on an individual's web browsing behavior such as the pages they have visited or the searches they have made to select which advertisements to be displayed to that individual. Practitioners believe this helps them deliver their online advertisements to the users who are most likely to be influenced by them."[45]

---

[45] Interactive Adver. Bureau, "Glossary of Interactive Advertising Terms v. 2.0," *available at* http://www.iab.net/media/file/GlossaryofInteractivAdvertisingTerms.pdf (viewed Jan. 16, 2010).

The online and mobile advertising industry insists that "anonymized" or "de-identified" data will protect consumer privacy while still allowing the marketers to create user profiles for targeted advertising. On its own Web site, the IAB assures visitors that, "We may collect information from visitors to our Web site and users of our services in an aggregate, anonymous form, which means that the information will not contain nor be linked to any personal information."[46] However, often, data that is believed to have been rendered anonymous can easily be "de-anonymized," and sensitive data would be linked back with the affected individual.

Carnegie Mellon professor Latanya Sweeney has been researching the issue of de-anonymization or re-identification of data for years. In 1998, she explained how a former governor of Massachusetts had his full medical record re-identified by cross-referencing Census information with de-identified health data.[47] Sweeney also found that, with birth date alone, 12 percent of a population of voters can be re-identified. With birth date and gender, that number increases to 29 percent, and with birth date and zip code it increases to 69 percent.[48]

In 2000, Sweeney found that 87 percent of the U.S. population could be identified with birth date, gender and zip code.[49] She used 1990 Census data. In 2006, Philippe Golle at the Palo Alto Research Center revisited her research, using 2000 Census data, and found that "disclosing one's gender, ZIP code and full date of birth allows for unique

---

[46] Interactive Adver. Bureau, Event Privacy Policy, http://www.iab.net/event_privacy_policy (viewed Jan. 16, 2010). Though titled "Event Privacy Policy," IAB states, "Please read this policy to understand how we collect and use information gathered through this Web site, and to understand your rights regarding these practices."

[47] Latanya Sweeney, Lab. for Computer Sci., Mass. Inst. of Tech., *Roundtable Discussion: Identifiability of Data at a Meeting of the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics*, Jan. 28, 1998, *available at* http://www.ncvhs.hhs.gov/980128tr.htm (viewed Jan. 16, 2010).

[48] Latanya Sweeney, Lab. for Computer Sci., Mass. Inst. of Tech., *Weaving Technology and Policy Together to Maintain Confidentiality*, J. Law Med. Ethics, 1997 Summer/Fall.

[49] Latanya Sweeney, Lab. for Int'l Data Privacy, Carnegie Mellon Univ., *Uniqueness of Simple Demographics in the U.S. Population* (2000).

identification" revealed the identity of 63 percent of the U.S. population.[50] (Note that the U.S. population in 1990 was 248.7 million and the 2000 population was 281.4 million.)[51]

In 2006, the publication of search records of 658,000 Americans by AOL demonstrated that the storage of a number as opposed to a name or address does not necessarily mean that search data cannot be linked back to an individual. Though the search logs released by AOL had been "anonymized," identifying the user by only a number, *New York Times* reporters were quickly able to match some user numbers with the correct individuals.[52] User No. 4417749 "conducted hundreds of searches over a three-month period on topics ranging from 'numb fingers' to '60 single men' to 'dog that urinates on everything.'" A short investigation led *Times* reporters to "Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga." and has three dogs. The *Times* also noted that the data associated with Ms. Arnold was misleading. "At first glace, it might appear that Ms. Arnold fears she is suffering from a wide range of ailments. Her search history includes 'hand tremors,' 'nicotine effects on the body,' 'dry mouth' and 'bipolar.' But in an interview, Ms. Arnold said she routinely researched medical conditions for her friends to assuage their anxieties. Explaining her queries about nicotine, for example, she said: 'I have a friend who needs to quit smoking and I want to help her do it.'"[53]

Pace University professor Catherine Dwyer, who published in 2009 a detailed case study of behavioral targeting practices on Levis.com, found that so-called "anonymous" profiling fails to provide the targeted consumer any real privacy protection. "The vast majority of data is collected anonymously, i.e., not linked to a person's name," she said.[54] "However, behavioral targeting does create digital dossiers on consumers with the aim of connecting browsing activity to a tagged individual. This tagging is largely

---

[50] Phillippe Golle, Palo Alto Research Ctr., *Revisiting the Uniqueness of Simple Demographics in the US Population* (2009), *available at* http://www.privacylives.com/wp-content/uploads/2010/01/golle-reidentification-deanonymization-2006.pdf (viewed Jan. 16, 2010).
[51] U.S. Census Bureau, 1990 Census, http://www.census.gov/main/www/cen1990.html (viewed Jan. 16, 2010); U.S. Census Bureau, 2000 Census, http://www.census.gov/main/www/cen2000.html (viewed Jan. 16, 2010).
[52] Michael Barbaro and Tom Zeller, "A Face Is Exposed For AOL Searcher No. 4417749," N.Y. TIMES, Aug. 9, 2006, *available at* http://www.nytimes.com/2006/08/09/technology/09aol.html (viewed Jan. 16, 2010).
[53] *Id*.
[54] Catherine Dwyer, Pace Univ., *Behavioral Targeting: A Case Study of Consumer Tracking on Levis.com* 1 (Aug. 6, 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1508496 (viewed Jan. 16, 2010).

invisible to consumers, who are not asked to explicitly give consent for this practice. By using data collected clandestinely, behavioral targeting undermines the autonomy of consumers in their online shopping and purchase decisions."[55] Such targeting, Dwyer suggested, can also undermine consumer confidence in e-commerce: "Not asking for explicit consent, and using anonymity to sanitize the tagging of individuals are components of behavioral targeting that can destroy trust in e-commerce. Even if consumers are anonymous, … advertising networks are silently collecting data to influence their purchase decisions…. Behavioral targeting without consent threatens the autonomy of consumers, and can undermine the trust and expectations of benevolence that customers associate with a name brand."[56]

Researchers and consumer advocates are not the only ones investigating the efficacy of anonymization or de-identification of data. On Jan. 4, 2010, the federal Department of Health and Human Services ("HHS") posted a notice on Federal Business Opportunities Web site stating it intends to hire a contractor to "demonstrate the ability or inability to re-identify" information that has been "de-identified" under the Health Information Portability and Accountability (HIPAA) Privacy Rule.[57] "Re-identify means to accurately and unambiguously match the de-identified data record to an actual individual."[58]

In August, University of Colorado law professor Paul Ohm discussed "the surprising failure of anonymization," and said, "Data can either be useful or perfectly anonymous but never both."[59] He said anonymization's failure "should trigger a sea change in the law, because nearly every information privacy law or regulation grants a get-out-of-jail-free card to those who anonymize their data."[60]

---

[55] *Id*.
[56] *Id*. at 8-9.
[57] Dept. of Health & Human Serv., *Comprehensive Research on Re-identifying a HIPAA De-Identified Dataset: Solicitation Number: DeidentifiedDataset*, Jan. 4, 2010, https://www.fbo.gov/index?s=opportunity&mode=form&id=bf5b42d4d605295ec2d4bde88078cffa&tab=core&_cview=0&cck=1&au=&ck= (viewed Jan. 16, 2010).
[58] *Id*.
[59] Paul Ohm, Univ. of Colo. Law Sch., *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* 4 (Aug. 13, 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 (viewed Jan. 16, 2010).
[60] *Id*.

We agree. So-called "anonymization" or "de-identification" should not be used as a cloak for data collectors to hide behind. Anonymization should be left behind. Instead, the definition of personally identifiable information of individuals should be changed. We believe that personally identifiable information is data that can be linked to an individual. "An individual" includes any: (a) person identified by name, address, account number, or other identifying particular assigned to the individual; and b) user of any online service or facility who is targeted (1) based on information obtained in more than a single transaction, online encounter, or other online activity; (2) notwithstanding the absence of a name, address, account number, or other identifying particular about the user known to the behavioral targeter; and (3) when the behavioral targeter has any reason to believe that the user being targeted is a particular user about whom the behavioral targeter obtained information in the past or from another source, including the use of IP addresses, browser cookies, and other persistent user identifiers or tracking methods. Consumer privacy will be better protected if the FCC joins the FTC in agreeing that, "in the context of online behavioral advertising, rapidly changing technologies and other factors have made the line between personally identifiable and non-personally identifiable information increasingly unclear."[61]

## III. Fair Information Practices Should Be Foundation of FCC's Standards for Consumer Privacy Protection

Privacy is a fundamental right in the United States. For four decades, the foundation of U.S. privacy policies has been based on the Fair Information Practices promulgated in 1973 by the U.S. Department of Health, Education and Welfare. [62] As applied under the 1980 OECD Guidelines on data privacy, the Fair Information Practices include: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[63]

---

[61] FTC Report on Self-Regulatory Principles at iii, *supra* note 34.
[62] U.S. Dep't. of Health, Educ. & Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (1973), *available at* http://aspe.hhs.gov/datacncl/1973privacy/Summary.htm (viewed Jan. 16, 2010.
[63] Org. for Econ. Cooperation & Dev., *Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data, OECD Doc. 58 final* (Sept. 23, 1980), *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (viewed Jan. 16, 2010).

Congress has reaffirmed its commitment to the Fair Information Practices numerous times. Congress used the Fair Information Practices as the basis of the Privacy Act of 1974, which restricts the amount of personal data that Federal agencies can collect and requires agencies to be transparent in their information practices.[64] When Congress created the Department of Homeland Security's Privacy Office several years ago, Fair Information Practices were included in the establishing legislation. In the Homeland Security Act of 2002, Congress said, "The Secretary shall appoint a senior official in the Department to assume primary responsibility for privacy policy, including … assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974."[65]

The Fair Information Practices ensure that individuals are able to control their personal information, help to protect human dignity, hold accountable organizations that collect personal data, promote good business practices, and limit the risk of identity theft. Developments in the digital age urgently require the application of Fair Information Practices to new business practices. Today, information from consumers is collected, compiled, and sold secretly, all done without reasonable safeguards. We urge the FCC to continue to base consumer privacy standards on this strong foundation.

For a detailed discussion of how the Fair Information Practices can be applied to protect consumer privacy across broadband services, review a legislative primer released last year by a group of consumer advocacy organizations (including some that submit these comments to the FCC).[66] This document was developed with the goal of recommending solutions for and informing the public and government officials of important gaps in consumer privacy protection. While the recommendations are not exhaustive, they do represent areas of consensus among leading organizations concerned with consumer privacy.

---

[64] 5 U.S.C. § 552a (1974); S. Rep. No. 93-1183 at 1 (1974). The U.S. Senate report said the Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the 40 personal information systems and data banks of the Federal Government."

[65] 6 U.S.C.A. § 142 (2003).

[66] Ten Consumer Advocacy Groups, Legislative Primer: Online Behavioral Tracking and Targeting Concerns and Solutions from the Perspective of Consumer Advocacy Groups (Sept. 2009), available at http://www.privacylives.com/wp-content/uploads/2009/09/onlineprivacylegprimer_0909.pdf (viewed Jan. 16, 2010).

## Conclusion

Broadband, mobile and other advertising companies will continue to be part of national and international media, and there are benefits to these businesses. However, as noted above, there can arise substantial threats to our privacy and related consumer protection issues in their business practices and policies. We urge the FCC to consider all avenues it may use to solve important gaps in consumer privacy protection and work with the FTC, which has substantial expertise in consumer privacy protection.

Respectfully submitted:

Chris Calabrese
American Civil Liberties Union

Jeff Chester
Center for Digital Democracy

Linda Sherry
Consumer Action

Susan Grant
Consumer Federation of America

John Simpson
Consumer Watchdog

Melissa Ngo
Privacy Lives

Beth Givens
Privacy Rights Clearinghouse

Evan Hendricks
Privacy Times

Amina Fazlullah
U.S. PIRG

**Contact:**

Jeff Chester
Executive Director

Center for Digital Democracy
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 494-7100
jeff [at] democraticmedia.org

Date filed: January 22, 2010