From: Consumer advocacy groups Date: October 13, 2009

To: Federal Communications Commission

RE: In the Matter of Consumer Information and Disclosure, Truth-in-Billing and Billing Format, IP-Enabled Services, CG Docket No. 09-158, CC Docket No. 98-170 and WC Docket 04-36)

Introduction

The Center for Digital Democracy, Consumer Action, Consumer Federation of America, Consumer Watchdog, Privacy Rights Clearinghouse, and US PIRG (collectively, "Consumer advocacy groups") submit these comments to the Federal Communications Commission ("FCC") concerning consumer privacy as part of the wireless consumer information and disclosure "Truth in Billing" discussion.[1] The FCC has a vital role to play in protecting privacy in the wireless industry. Any wireless policy must address privacy in order to protect consumers. Not only should consumer data be secured (and data collection minimized), but the FCC must analyze how wireless data is used to structure the commercial and other transactions that have become a part of the mobile device marketplace.

In its Notice of Inquiry, the FCC explained that it sought "comment on whether there are opportunities to protect and empower American consumers by ensuring sufficient access to relevant information about communications services" and data "that can shed light on the general state of consumer awareness about the purchase of communications services."[2] The FCC said it is seeking to ensure consumers receive accurate data about terms of service, which we believe means consumers should be fully aware of the surreptitious data collection that is being conducted by mobile service providers, why it is being collected, and how they can opt-out of this data collection and retention.

The mobile industry has already developed extensive plans and techniques to help determine what it calls the "user journey" through the "mobile Internet." Many mobile

---

[1] 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, (hereinafter "FCC Truth in Billing Notice of Inquiry") *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-68A1.pdf.

[2] *Id*. at 2, 4.

marketers are eager to exploit what they correctly perceive as a unique opportunity to target consumers by taking advantage of our highly personal relationships with these extremely pervasive devices to provoke an immediate consumer response.[3]

Mobile marketers in the U.S. are already deploying a dizzying array of targeted marketing applications, involving so-called rich media, mobile video, branded portals, integrated avatars that offer "viral marketing" opportunities, interactive and "personalized wallpapers," "direct-response" micro-sites, and a variety of social media tracking and data analysis tools. Technologies have also matured to the point where they now permit "the targeted and device-optimized insertion of any type of advertising (images, videos, logos, watermarks) on any type of mobile media consumer application (mobile TV, **web browsing,** MMS)" (emphasis ours).[4]

Studies show that consumers are concerned about their privacy, eschewing intrusive data collection and sharing 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 the wireless industry. 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. We urge the FCC to take the steps detailed below to protect consumer privacy rights from exploitation.

I. Consumers Are Increasingly Using Mobile Devices to Access the Internet, Creating a Growing Market for Advertisers

With an estimated $1 billion in advertising dollars being spent in North America in 2008 – a figure that is expected to increase to $3 billion by 2011 – companies are rushing headlong to develop new capabilities to target more effectively the growing

---

[3] As mobile marketer Amobee describes its various non-voice related applications and service offerings (including Web browsing, online games, and SMS and MMS messaging) to mobile operators, "Our unified solution allows the operator to manage user journeys across all these services in real time," http://www.amobee.com/main/operators.htm (viewed Oct. 9, 2009).

[4] *See*, for example, "Mobile Rich Media Campaigns – A Quick Guideline," http://www.itsmy.biz/social; "Vantrix Ad Booster," http://www.vantrix.com/products/Vantrix-Ad-Booster/ (both viewed Oct. 9, 2009).

number of mobile device users. This audience now numbers more than 267 million in the U.S. alone (up from 251 million in Q4 of 2007).[5]

According to a recent study, "[m]ore people in the United States (and indeed globally) have a mobile phone than an Internet-connected PC. Consumers are quickly emigrating away from pay-per-use mobile services and are heading toward free-to-end-user services that are supported by advertising."[6] In the process, these consumers are becoming increasingly familiar with mobile advertising: "In Q3 of 2008, 39% of mobile phone users (104 million) remembered advertising of some format on their phone. This was the first time the number of Americans aware of mobile advertising has exceeded 100 million in a 3-month period."[7]

II. Consumers Highly Value Data Privacy, But Are Confused About Privacy Protections Provided by Businesses

Surveys conducted by reputable organizations have highlighted two important findings: Consumers highly value data privacy, and consumers are confused about company protections of customer privacy. Few consumers really understand the data collection system and targeting advertising environment online. The FCC has an important role to play – ensuring consumers better understand what data is being collected and how it is used and protecting consumers' rights.

A. Consumers Are Concerned About Data Privacy

In September, researchers at the University of Pennsylvania and the University of California-Berkeley released a study that found, "Contrary to what many marketers claim, most adult Americans (66%) do not want marketers to tailor advertisements to their interests. Moreover, when Americans are informed of three common ways that

---

[5] Action Engine Corp., *The Emerging On-Device Portal Opportunity*, 5; Courtney Acuff, *Mobile Marketers Should Show by Example*, CLICKZ NETWORK, Feb. 7 2008, *available at* http://www.clickz.com/showPage.html?page=3628344 (viewed Oct. 9, 2009); *U.S. Mobile User Numbers, Ad Recall Climbing Steadily*, MEDIABUYERPLANNER, Aug. 22, 2008; Mobile Marketing Ass'n, *Mobile Advertising Report (US) 3rd Quarter 2008*, Nov. 19, 2008 (hereinafter "MMA 2008 Q3 Ad Report," *available at* http://www.mmaglobal.com/research/mobile-advertising-report-us-3rd-quarter-2008 (viewed Oct. 9, 2009).

[6] MMA 2008 Q3 Ad Report, *supra* note 5.

[7] *Id*.

marketers gather data about people in order to tailor ads, even higher percentages — between 73% and 86% — say they would not want such advertising."[8]

The study also found:

- Even when they are told that the act of following them on websites will take place anonymously, Americans' aversion to it remains: 68% "definitely" would not allow it, and 19% would "probably" not allow it.

- 69% of American adults feel there should be a law that gives people the right to know everything that a website knows about them.

- 92% agree there should be a law that requires "websites and advertising companies to delete all stored information about an individual, if requested to do so."[9]

In April, University of Southern California's Center for the Digital Future found in its eighth annual "Surveying the Digital Future" project that "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."[10] Ninety-three percent of respondents "reported some level of concern about the privacy of personal information (somewhat, very, or extremely concerned)."[11]

A poll from the Consumer Reports National Research Center found "72 percent are concerned that their online behaviors were being tracked and profiled by companies."[12] The poll also found, "93 percent of Americans think internet companies should always ask for permission before using personal information and 72 percent want the right to opt out when companies track their online behavior."[13] The survey showed that consumer trust does affect their online behavior. "For example, over one-third (35%)

---

[8] Univ. of Penn., Univ. of Cal. at Berkeley, *Americans Reject Tailored Advertising and Three Activities that Enable It,* 3, Sept. 2009 (hereinafter "Penn-Berkeley Study"), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214 (viewed Oct. 9, 2009).
[9] *Id*. at 3-4.
[10] Ctr. for the Digital Future, Univ. of S. Cal., *Surveying the Digital Future: Survey Highlights,* 6, Apr. 28, 2009, *available at* http://www.digitalcenter.org/pdf/2009_Digital_Future_Project_Release_Highlights.pdf (viewed Oct. 9, 2009).
[11] *Id*.
[12] Consumers Union, *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy*, Sept. 25, 2008, (hereinafter "Consumer Reports Poll") *available at* http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html (viewed Oct. 9, 2009).
[13] *Id*.

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%)."[14]

B. Consumers Are Confused About Companies' Policies Regarding and Protections of Customer Data and Privacy

In the above section, we noted that a 2008 survey from Consumer Reports showed that consumers are cautious about online privacy. However, this survey also shows that there is confusion among consumers about companies' privacy policies and practices.[15] 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."[16]

Also in the above section, we highlighted results from a September study from the University of Pennsylvania and University of California at Berkeley that showed consumers are protective of their data. This study also revealed consumer confusion about how, when or if their data is protected. "Americans mistakenly believe that current government laws restrict companies from 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."[17]

This 2009 study follows surveys by the same universities conducted in 2007 that found confusion about customer data and customer privacy protections offered by businesses. The surveys "indicate that when consumers see the term 'privacy policy,' they assume the website cannot engage in many practices that, in reality, are common in

---

[14] *Id*.
[15] *Id*.
[16] *Id*.
[17] Penn-Berkeley Study, *supra* note 8 at 2.

ecommerce. Consumers do not understand the nature and legality of information-collection techniques that form the core of online advertising business models."[18]

Some highlights from the 2007 surveys:

- "37% of online shoppers falsely believe that a privacy policy prohibits a website from using information to analyze individuals' activities online – a practice essential to most online advertising efforts."[19]

- "55% (of respondents) either don't know or falsely believe that privacy policies prohibit affiliate sharing."[20]

- "55.4% agreed with the false statement that, 'If a website has a privacy policy, it means that the site cannot sell information about your address and purchase information to other companies.'"[21]

- 39.8% believed that "If a website has a privacy policy, it means that the site cannot buy information about you from other sources to analyze your online activities"[22]

It is important to note that the 2007 report found, "When these techniques and the business model of online advertising are explained to them, [consumers] reject the privacy tradeoff made for access to content."[23] The 2009 report found, "when Americans are informed of three common ways that marketers gather data about people in order to tailor ads … between 73% and 86% say they would not want such advertising."[24]

Also, we must highlight that the concerns about privacy and security issues intensify when advertisers 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

---

[18] 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 Oct. 9, 2009).
[19] *Id*. at 2.
[20] *Id*.
[21] *Id*.
[22] *Id*.
[23] Annenberg/Samuelson Online Ad Surveys, *supra* note 18 at 1.
[24] Penn-Berkeley Study, *supra* note 8 at 2.

capacity to make informed decisions regarding the trade-offs between privacy and online services.

Google Mobile Product Manager Sumit Agarwal called the mobile phone "the ultimate ad vehicle. It's the first one ever in the history of the planet that people go to bed with."[25] He noted, "It's ubiquitous across the world, across demographics, across age groups. People are giving these things to ever-younger children for safety and communication."[26]

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 mobile providers and advertisers play in the collection and use of data from youth for interactive marketing purposes.

III. Mobile Marketers Are Embracing Targeted Behavioral Advertising of Mobile Users

Despite all of the concerns it has raised in the personal computer and broadband markets, behavioral targeting is swiftly migrating to the mobile world.[27] Mobile devices, which know our location and other intimate details of our lives, are being turned into portable behavioral tracking and targeting tools that consumers unwittingly take with them wherever they go. The question is whether any mobile user is even aware that behavioral profiling is occurring, let alone cognizant of the many data collection and analysis techniques we describe here.

A. Marketers Are Targeting Mobile Users Even When They're Not Using Mobile Devices

Commenting on the enormous marketing opportunities of the mobile market, Amobee Mobile Systems' Web site states, "mobile phones are the most widely held

---

[25] Quoted in Abbey Klassen, "Why Google Sees Cellphones as the 'Ultimate Ad Vehicle,'" ADVERTISING AGE, Sept. 8, 2008.
[26] *Id*.
[27] 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 Oct. 9, 2009).

media device in the world."[28] "With more than 3 billion subscribers, the mobile phone dwarfs every other media platform. The reach is greater than TV, the effectiveness is stronger than print, and the ability to deliver 'relevancy' is greater than the web."[29]

Amobee has developed an ad-serving platform that enables mobile operators to insert mobile advertising into a wide range of content, including music, video and games, and claims it "enables the delivery of relevant impressions across all users on all handsets for all non-voice related applications and services."[30]

Mobile marketers are even attempting to target users when they aren't using their mobile devices. AdiTon is a mobile advertising platform that allows advertisers to push targeted information, entertainment, advertising, and promotions to their customers via the idle screen on a mobile device. AdiTon shows advertisements and contents on a phone's idle screen while a "carousel of content cycles through each ad or content piece…. As the consumer chooses content, the selections are recorded, forming a personal profile and allowing a more accurate personalization of the content for the consumer. The advertisements the consumer receives are targeted by their interest groups, recorded calls to action and other details such as age and gender."[31]

B. Marketers Are Merging Online and Offline Consumer Data To Create Detailed Consumer Profiles

The merging of offline and online data sources to target the mobile consumer is a serious privacy threat. For example, in May 2007, Acuity Mobile and Acxiom Corporation announced that they had partnered to create "a powerful new mobile marketing solution that integrates world-class consumer data and behavioral analytics with the industry's leading real-time mobile content delivery platform."[32] The new mobile marketing solution married "Acxiom's data and analytical capabilities with Acuity Mobile's location-based technology and Spot Relevance offering – the ability to

---

[28] Amobee Media Systems, Agencies and Advertisers, http://www.amobee.com/main/agencies.htm (viewed Oct. 9, 2009).
[29] *Id*.
[30] Amobee Media Systems, Mobile Operators, http://www.amobee.com/main/operators.htm (viewed Oct. 9, 2009).
[31] AditOn, How We Work, http://www.aditon.com/ourBusiness.html (viewed Oct. 9, 2009).
[32] Press Release, Acuity Mobile, "Acxiom Corporation and Acuity Mobile Partner to Power Targeted Mobile Marketing Solution," May 21, 2007, *available at* http://www.acuitymobile.com/docs/Press05212007.php (viewed Oct. 9, 2009).

deliver mobile content to the right user based on time, context, location and user preferences."[33]

By incorporating customer information data from Acxiom into Acuity's targeting engine, "the technology platform will facilitate relevant content delivery to a specific person based on preferences, time, context and location," ensuring "real-time, location-aware, user-targeted mobile marketing"[34] In addition to the data gleaned from mobile devices, Acuity's eMAP (Embedded Mobile Advertising Platform) Preference Engine "can mine multiple data sources to access any consumer information available," ensuring that all available data, even from "third party databases of consumer data" are utilized.[35]

IV. The FCC Needs to Regulate the Mobile Industry's Targeted Behavioral Advertising, Because Consumers Mistrust the Practices and Industry Self-Regulation Has Failed

For a variety of reasons explained below: (1) We urge the FCC to treat targeted behavioral advertising as a practice that should be regulated; (2) We believe consumers mistrust data-gathering and consumer profiling practices such as targeted behavioral advertising; (3) Consumers do view targeted behavioral advertising negatively and industry self-regulation practices have failed, so Congress and agencies such as the FCC need to regulate targeted behavioral advertising; and (4) The Commission should consider all avenues it may use to protect consumers, including exercising its ancillary jurisdiction to address privacy issues.

A. The FCC Should Treat Targeted Behavioral Advertising as a Practice That Should Be Regulated

Increasingly, mobile service companies are using targeted behavioral advertising to create detailed profiles on individual consumers that are then used by companies in attempts to manipulate users' actions. It is necessary for the FCC to step in and regulate companies' use of targeted behavioral profiling, in order to alleviate consumer confusion and ensure adequate privacy and security protection of consumer data.

---

[33] *Id*.
[34] *Id*.
[35] Acuity Mobile, Technology and Innovation, http://www.acuitymobile.com/company/technology.php (viewed Oct. 9, 2009).

1. Consumers Consider Behavioral Advertising To Be Uninvited Digital Intrusion

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.

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.[36] The personalized targeting that results from this vast stockpile of digital data has become a veritable goldmine.

In a February 2009 article, Center for Digital Democracy Executive Director Jeff Chester explained, "In a 2007 presentation to advertisers in the U.K., Yahoo touted its behavioral targeting as a form of 'intelligent user profiling.' Explaining that it captures user 'DNA' from 'registration and behaviors' (including online activities such as page views, ads clicked, search queries, and search clicks), Yahoo uses this information to fuel its BT targeting."[37]

Chester highlighted that the ability of behavioral targeting to lock in individual users is being fueled through connections to offline databases and other profiling technologies.

> For example, Mindset Media "lets advertisers define their targets on 21 standard elements of personality and then reach those targets on a mass scale in simple

---

[36] 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.
[37] Jeff Chester, *Inside the Digital 'Arms Race' Called BT*, Privacy Journal, Feb. 2009.

> online media buys. . . . Study after study, on large, representative samples, shows statistically significant correlations between Mindsets and buyer behavior. . . . A MindsetProfile will identify the psychographics that drive your brand, your category, and even your competitors." Such targeting is available over one ad network that reaches "150 million unique viewers each month across more than 1500 sites globally." The personality elements that can be targeted include "modesty" (defined as "self-centeredness, desire for recognition, importance of equality"); "perfectionism" ("fear of rejection, need for control, importance of appearance"); and "extroversion" ("recharged by being alone/with others, orientation of thought process/internal vs. external").[38]

The targeted behavioral profiling situation is untenable: The substantial privacy invasion made possible by the profiling is combined with weak consumer understanding about the technology and the fact that consumers seldom have knowledge of the technology's use by companies. It is necessary for the FCC to step in and regulate companies' use of targeted behavioral profiling in order to alleviate consumer confusion and ensure adequate privacy and security protection of consumer data.

B. Consumers Mistrust Data-Gathering and Consumer Profiling Practices Such as Targeted Behavioral Advertising

Surveys from reputable organizations show that consumers distrust data-gathering and -sharing to create consumer profiles, which can include targeted behavioral advertising.

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."[39] 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."[40] 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."[41]

---

[38] *Id*.
[39] Harris Interactive, *The Harris Poll #40,* Apr. 10, 2008, *available at* http://www.harrisinteractive.com/harris_poll/index.asp?PID=894.
[40] *Id*.
[41] *Id*.

In sections above, we cited 2007 and 2009 surveys 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. These surveys found confusion about customer data and customer privacy protections offered by businesses. The surveys also found that consumers would change their online behavior if they were aware of businesses using common advertising data-gathering and -sharing practices. In the 2007 survey:

> The survey's interviewers asked respondents to name a site they valued and then went on to ask their reaction to what is actually a common scenario of the way sites track, extract and share information to make money from advertising. 85% of the surveyed adults who go online at home did not agree that a "valued" site should be allowed to serve clickstream advertising to them based on data from their visits to various websites that marketers collected and aggregated. When offered a choice to get content from a valued site with such a policy or pay for the site and not have it collect information, 54% of adults who go online at home said that they would rather find the information offline than exercise either option presented.[42]

C. Congress and Agencies Such as the FCC Need to Address Targeted Behavioral Advertising, Because Industry Self-Regulation Practices Have Failed

We believe consumers view targeted behavioral advertising negatively and industry self-regulations practices have failed so, Congress and agencies such as the FCC need to regulate targeted behavioral advertising.

In November 2006, the Center for Digital Democracy and U.S. Public Interest Research Group ("U.S. PIRG") filed a complaint and request for inquiry and injunctive relief with the Federal Trade Commission concerning unfair and deceptive online marketing practices, specifically targeted behavioral advertising.[43] The groups explained the problems with industry self-regulation of data-gathering practices used to build consumer profiles:

---

[42] Annenberg/Samuelson Online Ad Surveys, *supra* note 18 at 3.

[43] 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 Online Marketing Practices,* Nov. 1, 2006, (hereinafter "CDD/U.S. PIRG Complaint") *available at* http://democraticmedia.org/files/FTCadprivacy_0.pdf.

> Consumers entering this new online world are neither informed of nor prepared for these technologies and techniques – including data gathering and mining, audience targeting and tracking – that render users all but defenseless before the sophisticated assault of new-media marketing. It is evident that attempts at self-regulation by the industry, such as the Network Advertising Initiative "principles," have failed to protect the public. Current privacy disclosure policies are totally inadequate, failing to effectively inform users how and what data are being collected and used. While many companies claim they collect only "non-personally identifiable" information, they fail to acknowledge the tremendous amounts of data compiled and associated with each unique visitor who visits their website. Thus even if these companies don't know our names, through online tracking and analysis they literally know every move we make.[44]

The surveys detailed above explain how consumers are confused about businesses' privacy policies and practices, and the protections that are in place to safeguard consumers' data. Notably, the 2009 study by the University of Pennsylvania and University of California at Berkeley found, "Americans mistakenly believe that current government laws restrict companies from selling wide-ranging data about them,"[45] while the universities' 2007 survey found that "55.4% [of respondents] agreed with the false statement that, 'If a website has a privacy policy, it means that the site cannot sell information about your address and purchase information to other companies.'"[46]

The time needed to read privacy policies is enormous; a 2008 study estimated it would take about eight to 10 minutes to read one average privacy policy on the most popular sites.[47]

> We estimate that if all American Internet users were to annually read the online privacy policies word-for-word each time they visited a new site, the nation would spend about 44.3 billion hours reading privacy policies.
>
> To put this in perspective, using the point estimate of 201 hours / year to read privacy policies means an average of 33 minutes a day. This is approximately 46% of the estimated 72 minutes a day people spend using the Internet (Nie, 2005). This exceeds the combined percentage of Internet time devoted to

---

[44] *Id*. at 3.
[45] Penn-Berkeley Study, *supra* note 8 at 4.
[46] Annenberg/Samuelson Online Ad Surveys, *supra* note 18 at 2.
[47] McDonald, Aleecia and Cranor, Lorrie Faith, CyLab at Carnegie Mellon University, *The Cost of Reading Privacy Policies*, 7, 2008, *available at* http://www.cylab.cmu.edu/news_events/cylab_news/privacy_policy.html.

> shopping (1.9%) dealing with spam (6.2%) and playing games (13%) in 2005 (Nie, 2005). The estimated time to read privacy policies is on par with the percentage of time people currently spend surfing the web (45.3%).[48]

Other problems with privacy policies are detailed in a study released in June from the University of Berkeley School of Information:

> Our survey of privacy policies revealed that most of the top 50 websites collect information about users and use it for customized advertising. Beyond that, however, most contained unclear statements (or lacked any statement) about data retention, purchase of data about users from other sources, or the fate of user data in the event of a company merger or bankruptcy.
>
> Sharing of information presents particular problems. While most policies stated that information would not be shared with third parties, many of these sites allowed third-party tracking through web bugs. We believe that this practice contravenes users' expectations; it makes little sense to disclaim formal information sharing, but allow functionally equivalent tracking with third parties.[49]

The report also listed several reasons that privacy policies are ineffective: (1) They are difficult to read; (2) They lead consumers to believe that their privacy is protected; (3) The amount of time required to read privacy policies is too high; (4) There is not enough market differentiation in the policies for users to make informed choices; and (5) Even if there were enough market differentiation, "it is not clear that users would protect themselves. **The potential dangers are not salient** to most users. And even when they are salient, **they are difficult to evaluate** against the benefits of using a particular website."[50]

It is clear that industry self-regulation has failed to adequately inform consumers about data-gathering and -sharing practices. Also, as explained previously, consumers are not comfortable with these data-gathering and -sharing practices when they learn businesses are using them.

---

[48] *Id*. at 12.
[49] Joshua Gomez, Travis Pinnick, and Ashkan Soltani, *KnowPrivacy*, 4, June 1, 2009, *available at* http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf.
[50] *Id*. at 11-12.

The situation is such that Congress and agencies such as the FCC need to step in and protect consumers by regulating targeted behavioral advertising. In fact, the FCC should consider all avenues it may use to protect consumers.

Conclusion

In its Notice of Inquiry, the FCC said it is seeking to ensure consumers receive accurate data about terms of service. We believe this means the FCC should ensure consumers are fully aware of the surreptitious data collection that is being conducted by mobile service providers and mobile advertisers, why it is being collected, and how they can opt-out of this data collection and retention. The FCC also should seek to protect youth from harmful and unfair marketing practices, especially as children and adolescents are prime targets for behavioral advertising, even though they lack the capacity to make informed decisions regarding data collection. The potential dangers to consumers' privacy rights are enormous, yet few consumers understand the intrusive and all too common data collection and sharing that occurs with mobile devices.

We urge the FCC to: (1) Work with Congress and other federal agencies to regulate targeted behavioral advertising; (2) Investigate the data collection and profiling of both children and adolescents, with a particular focus on the role mobile service providers and mobile advertisers play in the collection and use of data from youth for interactive marketing purposes; (3) Establish binding regulations concerning consumer privacy in mobile services, so that consumers can be informed of their privacy rights and the privacy risks involved in using the services of each mobile service provider; and (4) Consider all avenues it may use to protect consumers.

Respectfully submitted:

Jeff Chester
Center for Digital Democracy

Ruth Susswein
Consumer Action

Susan Grant
Consumer Federation of America

John Simpson
Consumer Watchdog

Beth Givens
Privacy Rights Clearinghouse

Ed Mierzwinski
US 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: October 13, 2009