From: Consumer advocacy groups Date: June 8, 2009
To: Federal Communications Commission
RE: In the Matter of a National Broadband Plan for Our Future, GN Docket No. 09-51

Introduction

The Center for Digital Democracy, Privacy Rights Clearinghouse, and U.S. PIRG ("Consumer advocacy groups") submit these comments concerning consumer privacy as part of the national broadband plan to the Federal Communications Commission ("FCC").[1] The FCC has a vital role to play in protecting privacy online. Any broadband policy must address privacy in order to protect online consumers. Not only should consumer data be secured (and data collection minimized), but the FCC must analyze how online data is used to structure the commercial and other transactions that have become a part of the broadband marketplace.

We support the FCC's consideration of a wide range of questions in its development of a national broadband plan, and we are especially encouraged that the FCC is focusing on consumer privacy protections from the beginning of the process, instead of trying to haphazardly plug privacy protections in near the end.

Here are the questions detailed by the FCC that we seek to answer in our comments:

1. What are consumer expectations of privacy when using broadband services or technology?[2]
2. We seek comment on how the Commission should treat issues such as deep packet inspection and behavioral advertising in developing a national broadband plan and whether there are issues related to other types of information connected with the provision of broadband services that the Commission should consider. If consumers view this negatively, is it something that Congress or government agencies should address, or can

---

[1] 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, (hereinafter "FCC Broadband Plan Notice of Inquiry") *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-31A1.pdf.

[2] *Id*. at 22.

privacy protections be achieved through industry self-regulation, such as industry best practices?[3] Should the Commission consider as part of its plan whether to exercise its ancillary jurisdiction to address broadband privacy issues, or are other approaches available?[4]

3. We also seek comment on whether the Commission should address novel issues unique to the Internet, like the potential privacy, economic, homeland security, and other issues associated with cloud computing.[5]

Studies show that consumers are concerned about online 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 online commerce. 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 in to protect consumer privacy rights from exploitation.

I. 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.

---

[3] *Id*. at 23.

[4] *Id*. at 23.

[5] *Id*. at 35.

A. Consumers Are Concerned About Online Privacy

The 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."[6] Ninety-three percent of respondents "reported some level of concern about the privacy of personal information (somewhat, very, or extremely concerned)."[7]

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."[8] 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."[9] 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%)."[10]

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.[11]

---

[6] 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.

[7] *Id*.

[8] 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.

[9] *Id*.

[10] *Id*.

[11] *Id*.

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."[12]

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 also 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 ecommerce. Consumers do not understand the nature and legality of information-collection techniques that form the core of online advertising business models."[13]

Some highlights from the surveys by Annenberg and Samuelson:

- "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."[14]
- "55% (of respondents) either don't know or falsely believe that privacy policies prohibit affiliate sharing."[15]
- "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.'"[16]

---

[12] *Id*.

[13] 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.

[14] *Id*. at 2.

[15] *Id*.

[16] *Id*.

- 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"[17]

It is important to note that the Annenberg/Samuelson 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."[18]

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

Such problems 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 at Georgetown University Law Center.[19] 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."[20]

---

[17] *Id*.

[18] Annenberg/Samuelson Online Ad Surveys, *supra* note 13 at 1.

[19] 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; *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.

[20] Campbell and Wright, *supra* note 19 at 3.

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.

II. The FCC Needs to Regulate Deep Packet Inspection and 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 deep packet inspection ("DPI") and targeted behavioral advertising as practices that should be regulated; (2) We believe consumers mistrust data-gathering and consumer profiling practices such as deep packet inspection and targeted behavioral advertising; (3) Consumers do view DPI and targeted behavioral advertising negatively and industry self-regulations practices have failed, so Congress and agencies such as the FCC need to regulate deep packet inspection and targeted behavioral advertising; and (4) The Commission should consider all avenues it may use to protect consumers, including exercising its ancillary jurisdiction to address broadband privacy issues.

A. The FCC Should Treat DPI and Targeted Behavioral Advertising as Practices That Should Be Regulated

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

1. Consumers Are Confused About Deep Packet Inspection

Few people understand what deep packet inspection actually is, and that causes confusion about the issue.[21] Here is a very simplified explanation of how the Internet works: Whenever you send an e-mail or visit a Web site, your data is broken into packets of information and directed toward the destination requested. Internet Service Providers ("ISPs") have traditionally only done deep packet inspection (where you can read the contents of an e-mail or figure out what Web site a customer is visiting) in order to do systems testing (for example, identifying computer viruses).

Advances in technology have made deep packet inspection easier, and it can be done in almost real-time. Now, some ISPs are proposing to use deep packet inspection of their customers' data as an advertising tool (targeted behavioral advertising), to enforce copyright law, and more. And it's unclear if individuals can opt-out or if individuals must suffer this privacy invasion if they wish to use these ISPs. Deep packet inspection also enables non-ISP service providers, such as search engines or webmail companies, to build user profiles.

The situation is untenable: The substantial privacy invasion made possible by DPI 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 DPI in order to alleviate consumer confusion and ensure adequate privacy and security protection of consumer data.

2. 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

---

[21] *Ars Technica* has a good, simple explanation of deep packet inspection and last year's controversy when cable operator Charter Communications was revealed to be quietly using the technology on its customers. Nate Anderson, *Charter "enhances" Internet service with targeted ads*, Ars Technica, May 13, 2008, http://arstechnica.com/old/content/2008/05/charter-enhances-internet-service-with-targeted-ads.ars.

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.[22] 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."[23]

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 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

---

[22] 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.

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

appearance"); and "extroversion" ("recharged by being alone/with others, orientation of thought process/internal vs. external").[24]

As with DPI, 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, as well as DPI, 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 Deep Packet Inspection and Targeted Behavioral Advertising

Surveys from reputable organizations show that consumers distrust data-gathering and -sharing to create consumer profiles, which can include deep packet inspection and 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."[25] 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."[26] 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."[27]

In sections above, we cited surveys by the University of Pennsylvania's Annenberg School of Communication and the University of California at Berkeley Law

---

[24] *Id*.

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

[26] *Id*.

[27] *Id*.

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.

> 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.[28]

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

We believe consumers view DPI and targeted behavioral advertising negatively and industry self-regulations practices have failed so, Congress and agencies such as the FCC need to regulate deep packet inspection and 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.[29] The groups explained the problems with industry self-regulation of data-gathering practices used to build consumer profiles:

> 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

---

[28] Annenberg/Samuelson Online Ad Surveys, *supra* note 13 at 3.

[29] 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.

> 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.[30]

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 Annenberg/Samuelson 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.'"[31]

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.[32]

> 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 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%).[33]

---

[30] *Id*. at 3.

[31] Annenberg/Samuelson Online Ad Surveys, *supra* note 13 at 2.

[32] 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.

[33] *Id*. at 12.

Other problems with privacy policies are detailed in a study released last week 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.[34]

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."[35]

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.

In February 2009, the Federal Trade Commission ("FTC") released a report outlining a set of self-regulatory guidelines specifically for online behavioral advertising practices.[36] However, there needs to be more analysis of the current state of interactive

---

[34] Joshua Gomez, Travis Pinnick, and Ashkan Soltani, *KnowPrivacy*, 4, June 1, 2009, *available at* http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf.

[35] *Id*. at 11-12.

[36] Fed. Trade Comm'n, *Self-Regulatory Principles For Online Behavioral Advertising*, Feb. 2009, *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

marketing and data collection in creating these self-regulatory guidelines. More analysis could have led to a better definition of behavioral targeting that would illustrate why legislative safeguards are now required. The FTC should not have exempted "First Party" sites from the Principles. "First party" behavioral advertising is advertising by a single Web site. The FTC said "first party" ads are "more likely to be consistent with consumer expectations, and less likely to lead to consumer harm, than other forms of behavioral advertising."[37]. We disagree. Users need to know and approve what kinds of data collection for targeting are being done at that specific online location.

The FTC should have created specific policies for sensitive data, especially in the financial, health, and children/adolescent area. By urging a conversation between industry and consumer groups to "develop more specific standards," the FTC effectively and needlessly delayed the enactment of meaningful safeguards.

The situation is such that Congress and agencies such as the FCC need to step in and protect consumers by regulating deep packet inspection and targeted behavioral advertising. In fact, the FCC should consider all avenues it may use to protect consumers, including exercising its ancillary jurisdiction to address broadband privacy issues.

III. The FCC Needs to Address Privacy and Security Issues Associated with Cloud Computing

Everyone has heard the term, but what is cloud computing? We have two similar definitions from a federal agency and a consumer advocacy organization. The National Institute of Standards and Technology released this month a draft document with a definition of cloud computing.[38] "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[39]

In a February 2009 report, the World Privacy Forum defined cloud computing as

---

[37] *Id*. at iii.

[38] Peter Mell & Tim Grance, Nat'l Inst. of Standards &Tech., *Draft NIST Working Definition of Cloud Computing*, June 2009, *available at* http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v14.doc.

[39] *Id*. at 1.

"involv[ing] the sharing or storage by users of their own information on remote servers owned or operated by others and accessed through the Internet or other connections. Cloud computing services exist in many variations, including data storage sites, video sites, tax preparation sites, personal health record websites, photography websites, social networking sites, and many more."[40]

As more individuals use cloud computing services, it becomes more important to understand the substantial privacy and security issues associated with cloud computing that directly affect consumers. We urge the FCC to investigate and address these issues independently and also in tandem with Congress and other federal agencies.

A. Consumers Have Concerns About Privacy of Cloud Computing Services

Millions of consumers use cloud computing services such as Web-based e-mail, online photo or video databases, or calendar services. The use of these services is growing, and consumers have expressed concerns about the privacy of cloud computing services.

In a September 2008 report, the Pew Internet and American Life Project detailed results from a survey about cloud computing.[41] Consumers reported that they: (1) Use webmail services such as Hotmail, Gmail or Yahoo mail; (2) Store personal photos online; (3) Use online applications, such as Google Documents or Adobe Photoshop Express; (4) Store personal videos online; (5) Pay to store computer files online; and (6) Back up hard drives to an online site.[42] "Overall, 69% of online users have done at least one of these six activities, with 40% of internet users having done at least two of them."[43]

Consumers cite convenience and flexibility as reasons to use cloud computing services, but the Pew study reported, "At the same time, users report high levels of

---

[40] Robert Gellman for the World Privacy Forum, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, 4, Feb. 2009, *available at* http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

[41] John B. Horrigan, Pew Internet & Am. Life Project, *Cloud Computing Gains in Currency*, (Sept. 12, 2008), *available at* http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency.

[42] *Id*.

[43] *Id*.

concern when presented with scenarios in which companies may put their data to uses of which they may not be aware."[44] Pew found:

- 90% of cloud application users say they would be very concerned if the company at which their data were stored sold it to another party.
- 80% say they would be very concerned if companies used their photos or other data in marketing campaigns.
- 68% of users of at least one of the six cloud applications say they would be very concerned if companies who provided these services analyzed their information and then displayed ads to them based on their actions.[45]

B. Consumers Do Not Understand Privacy and Security Risks Involved in Cloud Computing

Experts have detailed substantial privacy and security problems with cloud computing services. Yet most consumers do not understand the risks of using these services. The FCC needs to address these problems.

In a May 2009 essay, security expert Bruce Schneier summarized the problems with cloud computing: "For the most part, your online data is not under your control. Cloud computing and software as a service exacerbate this problem even more. Your webmail is less under your control than it would be if you downloaded your mail to your computer. If you use Salesforce.com, you're relying on that company to keep your data private. If you use Google Docs, you're relying on Google."[46] And there already have been high-profile examples of privacy and security problems with cloud computing service provider Google. In March 2009, media reports found, "Google discovered a privacy glitch that inappropriately shared access to a small fraction of word-processing

---

[44] *Id*.

[45] *Id*.

[46] Bruce Schneier, *Should We Have an Expectation of Online Privacy?*, Information Security, May 2009, *available at* http://searchsecurity.techtarget.com/magazinePrintFriendly/0,296905,sid14_gci1354832,00.html.

and presentation documents stored on the company's online Google Docs service."[47] The technical problem was fixed, but sensitive data was exposed, and consumers had no control over the situation.

In its February 2009 report, the World Privacy Forum also detailed substantial privacy and security problems with cloud computing services. Notable issues include:

- "A user's privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the cloud provider";
- "For some types of information and some categories of cloud computing users, privacy and confidentiality rights, obligations, and status may change when a user discloses information to a cloud provider";
- "Disclosure and remote storage may have adverse consequences for the legal status of or protections for personal or business information";
- "Legal uncertainties make it difficult to assess the status of information in the cloud as well as the privacy and confidentiality protections available to users."[48]

The World Privacy Forum highlighted how the privacy risks can substantially change depending on the terms of service of the particular cloud provider:

> Those risks may be magnified when the cloud provider has reserved the right to change its terms and policies at will. The secondary use of a cloud computing user's information by the cloud provider may violate laws under which the information was collected or are otherwise applicable to the original user. A cloud provider will also acquire transactional and relationship information that may itself be revealing or commercially valuable. For example, the sharing of information by two companies may signal a merger is under consideration. In some instances, only the provider's policy will limit use of that information.[49]

As we have detailed above, few consumers know of the data collection and sharing that is conducted by businesses online. In fact, the Federal Trade Commission has noted, "while behavioral advertising provides benefits to consumers in the form of free

---

[47] Stephen Shankland, *Google Docs suffers privacy glitch*, CNet News, Mar. 9, 2009, http://news.cnet.com/google-docs-suffers-privacy-glitch/; see also, Jason Kincaid, *Google Privacy Blunder Shares Your Docs Without Permission*, TechCrunch, Mar. 7, 2009, http://www.techcrunch.com/2009/03/07/huge-google-privacy-blunder-shares-your-docs-without-permission/.

[48] World Privacy Forum Report on Cloud Computing, *supra* note 40 at 6.7.

[49] Id. at 6.

web content and personalized ads that many consumers value, the practice itself is largely invisible and unknown to consumers."[50] We have explained that consumers do not typically read or understand online privacy policies or terms of service agreements.

Consequently, we argue that most consumers do not understand the privacy and security problems that can arise with cloud computing services, and especially consumers might not understand the importance of terms of service agreements. The FCC should establish binding regulations concerning consumer privacy in cloud computing services, so that consumers can be informed of their privacy rights and the privacy risks involved in using the services of each cloud computing service provider. The consumer should be informed in simple to understand language that is prominently displayed, not buried in the fine print. The cloud computing service provider should not be allowed to change its terms of service provisions arbitrarily or without appropriate notice to consumers.

Conclusion

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 online. The FCC has a vital role; it needs to ensure consumers better understand what data is being collected and how it can be used and also to protect consumer rights. The FCC also has an obligation 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.

As it develops a national broadband plan, we urge the FCC to: (1) Work with Congress and other federal agencies to regulate deep packet inspection and targeted behavioral advertising; (2) 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

---

[50] Fed. Trade Comm'n, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles*, 2, Dec. 2007, *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf.

marketing purposes; (3) Establish binding regulations concerning consumer privacy in cloud computing services, so that consumers can be informed of their privacy rights and the privacy risks involved in using the services of each cloud computing service provider; and (4) Consider all avenues it may use to protect consumers, including exercising its ancillary jurisdiction to address broadband privacy issues.

Respectfully submitted:

Jeff Chester
Executive Director
Center for Digital Democracy

Beth Givens
Director
Privacy Rights Clearinghouse

Amina Fazlullah
Staff Attorney
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: June 8, 2009