CENTER FOR
DIGITAL
DEMOCRACY

Marlene Dortch, Secretary
Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20554

June 27, 2016

Re: WC Docket No. 16-106
Reply Comments in the matter of protecting the privacy of customers of broadband and other telecommunications services

Dear Ms. Dortch:

The Center for Digital Democracy (CDD), a nonprofit organization representing the interests of consumers in the digital marketplace, is submitting reply comments to address and rebut some of the arguments submitted in the Commission's Notice of Proposed Rulemaking[1] (NPRM) regarding proposed rules to protect the privacy of customers of broadband and other telecommunications services.

First, we like to disagree with some of the commenters, including those from AT&T Services Inc. (AT&T), Comcast, National Cable & Telecommunications Association (NCTA), and Verizon that the NPRM would cause significant consumer confusion. On the contrary, we believe that the absence of any FCC rulemaking to protect the privacy of broadband customers would significantly add to the already prevalent sense of confusion and sense of loss of control among broadband internet customers under the existing FTC regime. Instead, the proposed rules will give ISP customers much needed control over their data and are much more likely to increase consumer confidence.

Second, we would like to emphasize that current BIAS provider data practices already undermine the privacy of their customers and that they are in the process of further building out their powerful data management capabilities. Due to these practices and their significant position in the data eco system, BIAS providers are a growing and significant marketplace force in digital advertising. Contrary to companies' and trade associations' claims, we see no evidence that giving BIAS providers' customers effective privacy choices will limit the online advertising industry to flourish. The American public wants to see its privacy protected and

[1] 47 U.S.C. § 222(h); Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Notice of Proposed Rulemaking, 31 FCC Rcd. 2500, 2519 ¶ 57 (proposed Apr. 1, 2016) (hereinafter "NPRM").

needs the safeguards proposed by the Commission. Nothing less will limit the expansion of an unprecedented intrusion of BIAS providers into the most private aspects of American consumers' lives. The Commissions' proposed rules are needed to protect individual autonomy and the fundamental right to privacy and self-determination.

CDD would like to address some of the issues and claims raised by several commenters in detail:

Companies Raise Unsupported and Surprising Concern About Future Increased Consumer Confusion

Several of the submitted comments raise the specter of consumer confusion due to the fact that the proposed rules are 'different' from existing FTC rules (Comcast) or because there would be 'multiple privacy regimes' (Verizon). It is suggested by some petitioners that this confusion would lead to misinformed customers who would assume that the FCC rules would not only apply to ISPs but also to 'use of consumer data elsewhere in the Internet ecosystem' (Comcast, AT&T). Moreover, NCTA argues that customer confusion would *increase* (emphasis added) confusion arising from 'asymmetric regulation'. NCTA goes so far to predict that this confusion 'will lead to less use of the Internet, not more' (NCTA).

CDD strongly disagrees with these unfounded claims. Commenters present no evidence that ISPs customers would experience any additional confusion due to the proposed rules or that an awareness of different regulatory regimes would lead to additional consumer confusion.

Ample Evidence Points to Consumer Confusion under the Current Regulatory Opt-Out Regime

To the contrary, there is ample evidence that the existing regulatory regime prior to this NPRM has produced severe frustration and a sense of lack of control among consumers. Multiple studies have been referenced by others in this proceeding[2] that document consumers' pervasive sense of resignation and loss of control over the uses of their data. More than half of Americans do not want to lose control but believe that this loss of control has already happened[3].

These sentiments are not surprising as the burden to the average consumer to assess and manager her privacy risks are in practice not manageable. In order to self-manager her privacy risks, the average consumer has to be constantly vigilant due to the prevailing opt-out regime: one study has estimated that the number of unique websites the average Internet user visits annually with a lower bound of 119 sites. And the average consumer would need to spend

---

[2] See for example, Rainie, Lee, Duggan, M., *Privacy and Information Sharing,* Pew Research Center, December 2015 Available at: http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf;

[3] Joseph Turow, Michael Hennessy & Nora Draper, *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation*, Univ. of Penn. Annenberg School of Comm'n 3 (June 2015), available at https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

between 181 and 304 hours each year reading these web sites' privacy policies to be able to understand how her information is being used.[4] Consider further that websites are just one aspect of managing ones privacy risks. The number of digital devices and platforms available to today's consumers has exploded in recent years. It has been estimated already in 2014 that Americans own four digital devices on average.[5] In addition, most consumers lack knowledge and understanding how to manage their privacy risks[6] and consumers' knowledge seems dangerously inadequate for dealing with the ever-growing complexity of the digital data ecosystem (and it is particularly concerning that young adults from a low income background displayed particularly alarming low levels of knowledge in a 2014 study[7]). Even when companies make extra efforts to educate consumers on their opt-out choices, the results are often more than disappointing, as was the case with the Digital Advertising Alliance's AdChoices icon campaign[8].

In other words, under the existing FTC opt –out regime today's every day consumer experience is already confusing. Still, consumers know that every website, connected device and Internet provider has its own privacy policy that the consumer herself has to seek out, review, comprehend, evaluate and where they ultimately have to assert their privacy interests and arrive at a privacy choice via the privacy settings. It is the current FTC opt-out regime that assumes the consumer's acquiescence to an invasion of her privacy. It is due to an impossible task of privacy self-management that the current opt-out regime confuses and overwhelms the average consumer.[9]

As mentioned above, some commenters in the rule making went so far to suggest that the proposed rules may possibly lead to 'less use of the Internet, not more' (see NCTA filing). Alas, US Internet users curtail their Internet use under the current opt-out regime already significantly: A recent study by the National Telecommunications and Information Administration found that nearly half of Internet users in the US refrained from online activities due to privacy and security concerns[10]. Whether customers would further restrict their Internet

---

[4] Aleecia McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 J. of L. & Pol'y for the Info. Society (I/S) 540, 560 (2008), authors' draft available at http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

[5] See http://www.nielsen.com/us/en/insights/reports/2014/the-us-digital-consumer-report.html, accessed 6-17-2016

[6] Turow, Hennessy, Draper

[7] Y.J. Park, S. Mo Jang, *Understanding privacy knowledge and skill in mobile communication*, Computers in Human Behavior 38 (2014) 296–303

[8] Kate Kaye, *Study: Consumers Don't Know What AdChoices Privacy Icon Is*, Advertising Age, 1-29-2014, http://adage.com/article/privacy-and-regulation/study-consumers-adchoices-privacy-icon/291374/ accessed 6-17-2016

[9] Solove, Daniel J., *Privacy Self-Management and the Consent Dilemma* (November 4, 2012). 126 Harvard Law Review 1880 (2013); GWU Legal Studies Research Paper No. 2012-141; GWU Law School Public Law Research Paper No. 2012-141. Available at SSRN: http://ssrn.com/abstract=2171018

[10] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, Nat'l Telecomm's & Info. Admin., NTIA Blog (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-andsecurity-may-deter-economic-and-other-online-activities

use or be further confused under stronger FCC privacy safeguards seems highly unlikely.

Proposed Rules Will Give ISP Customers much needed Control over their Data and Are Much More Likely to Increase Consumer Confidence in their Internet Service Provider

Instead of confusing anyone, the proposed rule will provide consumers with stronger privacy protections for secondary uses of their network data under the FCC's mandate and oversight authority. Internet service providers have a special relationship with their customers as they have large amounts of very detailed and sensitive data about their customers, which makes consumers' affirmative consent essential. ISPs will have to prompt customers and obtain affirmative consent for the use and sharing of customer data for services unrelated to the service a customer has purchased. Giving users the opportunity to affirmatively consent to unrelated uses, prompting them to do so, rather than assuming they do not object (as is assumed under an opt-out regime), will give consumer a sense of much needed control. ISP customers' inactivity will not be punished with further loss of privacy and loss of control; instead of being overwhelmed, if the rules will be implemented as proposed, customers will be able to make deliberate decisions as to the trade-offs they wish to engage in. Affording consumers this heightened sense of control is appropriate for the networked uses of the Internet, given that it is the most fundamental communications network of our times.

BIAS Providers are a growing marketplace force using BIAS customer data together with cable TV customer data and it is time to effectively regulate the use of BIAS customer data

BIAS providers are growing as a significant marketplace force in digital advertising, positioned to become key gatekeepers for the collection and cross-device use of consumer information: Verizon, for example, is working closely with new subsidiary AOL (and its new subsidiary app and geo-location data collection company Millennial Media) to develop and deploy "data products for the advertising market," including "data targeting, and measurement." They are also working together on "location based services." They are designing their services to "enable brands to better understand, engage and transact with consumers,"—in another words, to better profile and target their customers. Verizon and AOL are integrating their "video and advertising" products, including "inventory, platforms, targeting data and measurement." This includes the role of real-time programmatic and algorithmic-based decision-making on their customers.[11] AT&T recently told a meeting sponsored by the IAB that its AT&T AdWorks, which includes the "largest addressable TV platform in the industry," is now connected to a "Video Inventory Platform" that includes a "premium programmatic portal," as well as "proprietary first-party data across *online*, mobile and TV. " [emphasis added] Data providers include both Experian and Acxiom, which is mixed with "brand" and "client" data for customer targeting—

[11] See, for example: "Project Manager - Mobile Advertising Data Solutions" and "Project Manager - Mobile Advertising Video Solutions." http://www.verizon.com/about/work/jobs/4918913-digital-advertising-manager-data-solutions; http://www.verizon.com/about/work/jobs/5230077-commercial-integration-lead-video-products

which is also measured for its impact. AT&T also has the "leading mobile and settop box linking to achieve cross-screen addressable targeting; [can] "reach the same users on TV and mobile across tens of billions of ad impressions;" [and generate] "cross-screen reporting insights." [12] In its report on Big Data and ISP practices, CDD described the growth of BIAS-based cross-device targeting, including the role of settop boxes.[13] BIAS companies, despite claims of some commentators, have unique first-party data that comes from settop boxes, video subscriptions, monitoring of device use and provision of broadband and mobile communications services. They have growing visibility into the personal lives of their customers (just a cursory examination of the Comcast's work with Adobe underscores this point alone). Critically, they provide a growing range of cross-platform interactive content along with a sophisticated platform for delivering residential service, that enables them to gather even more information on customers, a key necessity for the digital advertising industry.

We see no evidence that giving BIAS providers' customers effective privacy choices will limit the online advertising industry to flourish

The Association of National Advertisers (ANA) claims that there is evidence that opt-in consent "would curtail the effectiveness of online advertising." There is no legitimate evidence supporting such a claim, on the contrary, there is evidence that suggests that opt-in regimes do not limit the online advertising industry to flourish. Despite having the strongest privacy laws, requiring affirmative consent, online advertising revenues in the European Union are surging, growing 13% in 2015 from the previous year (and surpassing spending for television)[14]. Indeed, a cursory examination of the EU market—which just finalized its General Data Protection Regulation giving the public even more privacy controls—will show significant growth in the

[12] See AT&T presentation. "TV 2020: Clear Vision of the Future of TV Advertising. IAB. June 15, 2016. http://www.iab.com/events/tv-2020-clear-vision-future-tv-advertising/

[13] "Big Data is Watching: Growing Digital Data Surveillance of Consumers by ISPs and Other Leading Video Providers." March 2016. https://www.democraticmedia.org/article/big-data-watching-growing-digital-data-surveillance-consumers-isps-and-other-leading-video

[14] See for example: "Digital overtakes TV advertising revenues across Europe." Irish Times. 12 May 2016: http://www.irishtimes.com/business/media-and-marketing/digital-overtakes-tv-advertising-revenues-across-europe-1.2645463 ; "Europe's Programmatic Video Ad Revenues Will Near €2 Billion in 2020." October 2015: http://www.emarketer.com/Article/Europes-Programmatic-Video-Ad-Revenues-Will-Near-2-Billion-2020/1013055#sthash.vRLYCd5F.dpuf

data driven digital ad business, including programmatic and mobile video advertising. [15] ANA comments claim that publishers and bloggers would move behind paywalls or face threats from ad blocking. ANA failed to inform the commission that there is a growing consensus in the digital ad industry that how it conducts digital advertising must change and provide—in the words of the Internet Advertising Bureau's new guide to address ad blocking— "a better user experience," and "**…explain** the value exchange that advertising enables." [their emphasis]. [16]

Indeed, there is ample evidence conducted by leading scholars that undeniably demonstrate that Americans are growing desperate about their loss of their privacy today.[17]

ANA's claim that the FCC's proposal for opt-in will "diminish access to vast amounts of non-sensitive information" is unfounded

This assertion doesn't hold up to scrutiny. First, asking a consumer for permission before a BIAS provider can engage in data-driven marketing practices does not, on its face, diminish access to data. The Commission's proposals are reasonable in that they do not prohibit the use of customer data for any purpose, but the proposed rules would simply give customers a choice in how they want their data used. Today, there is, as ANA says, a "vast" (and growing) amount of information available to marketers. For example, as ANA demonstrates in some of its own recent seminars for its members, consumer data are available outside the BIAS provider-customer relationship via ad exchanges, offline and online data onboarding, geolocation from

[15]; "European Online Advertising surpasses TV to record annual spend of €36.2bn." May 11, 2016. http://www.iabeurope.eu/research-thought-leadership/press-release-european-online-advertising-surpasses-tv-to-record-annual-spend-of-e36-2bn

[16] IAB Releases Ad Blocking Primer That Recommends a New 'DEAL' Between Publishers and Consumers." March 7, 2016: http://www.iab.com/news/new-iab-tech-lab-ad-blocking-primer/; "IAB Creates Guide for Publishers to Combat Ad Blocking." Advertising Age. May 7, 2016: http://adage.com/article/digital/iab-creates-guide-publishers-combat-ad-blocking/302953/

[17] "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation." Joseph Turow, Ph.D., Nora Draper, Ph.D. and Michael Hennessey, Ph.D. Annenberg School of Communication. University of Penn. 2015. https://www.asc.upenn.edu/news-events/publications/tradeoff-fallacy-how-marketers-are-misrepresenting-american-consumers-and

mobile devices and apps, and more.[18] BIAS companies are closely working with leading marketing and data "cloud" providers, for example, giving them ongoing access to an array of data on an individual. [19]

Furthermore, ANA and others opposed to consumer privacy choice fail to be candid with the Commission on the role of today's so-called "non-sensitive information." As one can see by examining, for example, the services provided by Acxiom and the Oracle Marketing Cloud, what the industry calls 'non-sensitive' involves information on a consumer's health status, financial status, buying habits, online behaviors, loyalty program use, presence of children, race and ethnicity and much more. Today, digital marketers are able to "mix and match" a digital avalanche of information about a person, where traditional categories of sensitive and non-sensitive are meaningless and no longer reflect marketplace realities. The analytical power of data management platforms provides powerful analytics to Comcast and others which are used to analyze all this "non-sensitive " information to reveal deep and highly sensitive personal insights and allow for inferences that are used for marketing (and eligibility) decisioning. Once again, it's a person that should decide whether such data on them is accessed and analyzed—not her ISP.[20]

The industry's distinction between sensitive and non-sensitive information is increasingly meaningless and thus we agree with the proposed rule to require affirmative consent for the use and sharing of customer data for services unrelated to the service a customer has purchased

Current digital marketing practices create a person's profile used for targeting that is composed of a ever-increasing set of data attributes, gathered from both online and offline sources. The dynamic creation of an individual profile, developed in part through deep analysis of their behavior, relationships, actions and more, illustrate that the former distinctions between sensitive and non-sensitive no longer apply. For example, in a recent presentation at the Adobe

---

[18] For example, see: "New Study Shows Huge Increase in Programmatic Ad Buying Among Top Marketers." ANA. March 3, 2016: https://www.ana.net/content/show/id/38895; "Mobile ROI Data and Insights from Walmart and MasterCard." ANA. June 3, 2015. Available via: http://www.ana.net/miccontent/showvideo/id/v-comww-0603; see too the partners that work together with Acxiom to gather and merge consumer offline and online data. http://liveramp.com/partners/

[19] For example, Verizon works with Oracle's marketing Cloud. See: https://www.oracle.com/marketingcloud/customers/success-stories/verizon.html; Comcast is a client of Adobe data profiling and targeting system. http://success.adobe.com/en/na/programs/products/digitalmarketing/migration12/1208_21408_comcast.html

[20] See, for example, Acxiom's Liveramp data partners for so-called "People-based marketing" (where they even have more information on a consumer because they are authenticated in some way on social networks, for example. It includes Facebook, Twitter, cross-device tracking company Drawbridge, programmatic data targeting company Mediamath, Adobe, etc. http://liveramp.com/partners/; CDD urges the commission to review the data available from Oracle's Marketing Cloud partners: http://www.oracle.com/partners/en/partner-with-oracle/get-started/join-opn/index.html

Summit by Comcast, three of its digital marketing team members described all the data they now have available today. That includes "first-party" data, such as "website, mobile web, or mobile app behaviors on operated and owned properties; CRM/Data Warehouse; Transaction and Point-of-Sale; Call Center [and from] Media Performance." Then they point to "second-party" information, which is "a partner's 1st party data (such as a co-brand partner);" and 'Third-party" information, including from "Datalogix" (Oracle), eXelate (Nielsen) or Acxiom; demographic data, spend-pattern data and geographic data." With all the data and technology today, according to the Comcast representatives, a marketer can "use data to manage the [consumer] journey," giving them a "360 degree view of [a] Customer, Panoramic Messaging Whenever and Wherever." Comcast explains that this provides them with "unified user profiles" that are used for "more accurate targeting, including suppressing unqualified prospects…" The technology Comcast uses also allows them to engage in "prospecting" as well as "test and learn" helping to track consumers across the Internet, engage in "cross" and "up" selling, and identify other consumers to target based on the data gathered from customers, so-called "look-alike" modeling.[21] Comcast is typical of how digital marketers work today—continually gathering and making "actionable" (in their words) a wide range of information about a person. Contemporary data analytics, measurement, and ad creation practices (such as creative versioning to personalize marketing content and change campaigns "inflight," make the non-sensitive and sensitive data distinctions no longer seriously operational.

CDD respectfully urges the commission to swiftly act to protect the privacy of Americans who subscribe and use BIAS provider services.

Submitted by Center for Digital Democracy
Jeff Chester,
Executive Director

[21] "DMP 101: Basics for brands, publishers and agencies. Krista Vezain, Doug Moore and Becky Thomas. Comcast. Presented at the Adobe Summit. 2016.
https://adobesummit.lanyonevents.com/2016/connect/sessionDetail.ww?SESSION_ID=1428