Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	
	)	

Reply Comments of Tech Knowledge

Unlike the "telecommunications" traffic carried by the plain old telephone network, internet traffic is valued by advertisers.[1] The data generated by internet traffic is so valuable that at least half of the internet's economic value is based on the collection of individual user data (primarily for advertising) and most commercial content on the Internet relies on advertising to some extent.[2] "Advertising lessens the cost that each user must pay to receive the benefits of the Internet, and expands the size of the system that society can afford to have."[3] To put this in perspective, the market for digital advertising ($59.6 billion) is now three times larger than the market for broadcast television advertising ($18.6 billion), and digital advertising is still growing at double-digit rates (20.4% in 2015) while broadcast television advertising is stagnant or declining.[4] Just as watching ads is part of the price consumers pay for free broadcast television, providing access to user data is part of the price consumers pay for the internet as we know it today. Whatever benefits consumers might derive from more stringent regulation of internet data practices will necessarily involve a tradeoff in terms

---

[1] *See* John Deighton and Leora D. Kornfeld, "Economic Value of the Advertising-Supported Internet Ecosystem" at p. 5 (Sep. 2012), http://www.iab.com/wp-content/uploads/2015/07/iab_Report_September-24-2012_4clr_v1.pdf.

[2] *See id.*

[3] *Id.* at p. 6.

[4] *See* Pew Research Center, "State of the News Media 2016" (broadcast TV ad revenue), http://www.journalism.org/files/2016/06/State-of-the-News-Media-Report-2016-FINAL.pdf; IAB internet advertising revenue report, 2015 full year results (Apr. 2016) (digital ad revenue), http://www.iab.com/wp-content/uploads/2016/04/IAB-Internet-Advertising-Revenue-Report-FY-2015.pdf.

of higher costs — like the premium consumers pay for video services that do not sell advertising (e.g., HBO Now at $14.99 per month[5]).

The FCC's decision to regulate the usage of internet data for marketing purposes thus raises a central question: When and under what circumstances are the costs imposed on consumers by particular ex ante prohibitions on internet marketing (including costs to market competition) fully offset by the benefits consumers would derive from preventing such use of their data in those circumstances?

According to a recent study by Pew Research Center, consumers view the answer to this question as contingent and context-dependent.[6] "People's views on the key tradeoff of the modern, digital economy – namely, that consumers offer information about themselves in exchange for something of value – are shaped by both the conditions of the deal and the circumstances of their lives."[7]

Rather than conduct an analysis of this central question in the appropriate context, however, the FCC assumes the answer can be found (1) in a statutory provision (section 222) adopted in the pre-broadband era for the purpose of regulating a service (telephony) with an entirely different set of consumer expectations and competitive tradeoffs; and (2) a reclassification decision (the 2015 Open Internet Order[8]) that was aimed primarily at protecting the interests of internet "edge" companies (not consumers' personal interests in privacy).[9] As a result, the Marketing NPRM has failed to consider important aspects of the problem of how to empower consumer choice regarding the use of data on the broadband internet for marketing purposes without unnecessarily increasing consumer costs or creating competitive distortions in the marketplace for internet advertising and other "big data" services.

---

[5] See https://order.hbonow.com.

[6] See http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.

[7] *Id.*

[8] Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601 (2015)[hereinafter "Open Internet Order"].

[9] *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, FCC 16-39 at ¶ 3 (2016) [hereinafter "Marketing NPRM"] ("Privacy protects important personal interests.").

A rational approach to the problem would not seek guidance for regulating consumer privacy in the broadband era in an outdated statutory provision or a largely unrelated "net neutrality" decision. A rational approach would require the FCC to consider the consumer privacy problem in its current context — *a broadband internet context* — which involves different economic tradeoffs (including consumer costs and competitive considerations) and consumer expectations than those envisioned when section 222 was adopted or those that underlay the FCC's Open Internet Order. If the FCC were to consider all of the important aspects of the problem, it would forbear from applying section 222 to broadband internet access service (BIAS), at least to the extent that section 222 conflicts with the FTC's fair and comprehensive privacy framework.

BIAS Is Not a Unique Threat to Consumer Privacy

The FCC's proposed justification for the application of discriminatory marketing rules to BIAS — that "broadband networks are not, in fact, the same as edge providers in all relevant respects"[10] — merely begs the question. Even assuming that statement is true, the Marketing NPRM does not offer any analysis regarding (1) how or the extent to which BIAS and on-BIAS services differ or (2) how any such differences relate to consumer privacy issues online.

The Marketing NPRM's lack of analysis on this point is highlighted by the fact that the FCC's discussion of the "differences" between BIAS and non-BIAS providers with respect to consumer data appears in its introductory section (paragraph 4) rather than in its more substantive text. The only "evidence" offered by the Marketing NPRM to support its (implied) conclusion that BIAS presents a unique threat to consumer privacy consists of conclusory, out-of-context, incomplete, and/or irrelevant statements. The evidentiary and/or analytical problems with each of these FCC statements — all of which appear in paragraph 4 of the Marketing NPRM — are discussed in detail below.

[10] Marketing NPRM at ¶ 4.

FCC statement. "ISPs are 'in a position to develop highly detailed and comprehensive profiles of their customers – and to do so in a manner that may be completely invisible.'"[11]

Analysis. This statement, which consists almost entirely of an out-of-context quote from the 2012 FTC Privacy Report,[12] tells us nothing about whether BIAS providers are in a unique (or better) position to develop such profiles than non-BIAS providers. Contrary to the implication created by the FCC's out-of-context quotation, the 2012 FTC Privacy Report (on which the Marketing NPRM frequently relies) concludes that BIAS providers are ***not unique*** in their ability to develop such profiles: "ISPs are just one type of large platform provider that may have access to all or nearly all of a consumer's online activity. Like ISPs, operating systems and browsers may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles."[13] The FTC also recognized that the ability of some web companies (e.g., Google and Facebook) to track consumers across different websites could create similar privacy issues, but at the time its report was issued in 2012, the FTC concluded this capability was not yet widespread.[14] Consistent with its general lack of analysis, the Marketing NPRM did not consider whether such capabilities have since become more widespread.

FCC statement. "This [ability of BIAS providers to collect consumer data] is particularly true because a consumer, once signed up for a broadband service, simply cannot avoid that network in the same manner as a consumer can instantaneously (and without penalty) switch search engines

---

[11] Marketing NPRM at ¶ 4. *See also id*. at ¶ 265 (citing the 2012 FTC Privacy Report for the same proposition). Though the FCC used the acronym for "internet service providers" in this sentence, it presumably meant BIAS providers.

[12] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers at p. 56 (2012) [hereinafter "2012 FTC Privacy Report"], https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[13] *Id*. The FTC's findings in this respect were recently confirmed by research from the Institute for Information Security & Privacy at Georgia Tech University. *See* Peter Swire, Justin Hemmings, Alan Kirkland, "Online Privacy and ISPs: ISP Access to Consumer Data Is Limited and Often Less than Access by Others" (Feb. 29, 2016) (filed in this docket on May 24, 2016) [hereinafter "Swire"], https://www.fcc.gov/ecfs/filing/60001926727/document/60002031928.

[14] *See* 2012 FTC Privacy Report at p. 56.

(including to ones that provide extra privacy protections), surf among competing websites, and select among diverse applications."[15]

Analysis. *First*, this sentence is entirely conclusory. The FCC provided no citation to any evidentiary source to support its conclusion that there are no costs (either in terms of the time involved or a "penalty") associated with switching among internet search engines, competing websites, or applications;[16] and the Marketing NPRM does not elsewhere consider the switching costs associated with such services. The few, scattered references to switching costs in the remainder of the marketing NPRM are limited to the costs of switching among BIAS providers and generally cite the 2015 Open Internet Order for support.[17]

Second, this sentence disregards entirely the two internet platforms the 2012 FTC Privacy Report concluded already had "access to all or nearly all of a consumer's online activity" in 2012[18] — i.e., operating systems and browsers — and the Marketing NPRM does not elsewhere consider the switching costs associated with these two platforms.[19] The 2015 Open Internet Order likewise did not consider the costs of switching operating systems or browsers, despite record evidence indicating that switching costs for mobile operating systems (and applications) are at least as high as the costs of switching mobile BIAS providers.[20]

Third, there is substantial evidence that consumers ***cannot*** switch between internet search engines, competing websites, applications, operating systems, or browsers "instantaneously" or with-

---

[15] Marketing NPRM at ¶ 4.

[16] *See id.* (containing no footnote or other reference to evidence supporting the FCC's conclusion with respect to the relative costs of switching among BIAS and other types of internet services that are capable of collecting and using consumer information to the same or similar extent as BIAS).

[17] *See, e.g.*, Marketing NPRM at ¶ 128, n. 223 (citing 2015 Open Internet Order, 30 FCC Rcd. at 5631, ¶ 81).

[18] 2012 FTC Privacy Report at p. 56.

[19] The FTC implied that there are switching costs associated with operating systems and browsers, but did not analyze the issue in the 2012 FTC Privacy Report. *See id*. ("Consumers, moreover, might have limited ability to block or control such tracking except by changing their operating system or browser.").

[20] *See, e.g.*, Protecting & Promoting the Open Internet, Reply Comments of the Center for Boundless Innovation, GN Docket No. 14-28, at 27–33 (Sept. 15, 2014) (noting, among other things, that Apple uses its exclusive control over its mobile operating system to decide which applications it will allow iPhone and iPad users to access over the Internet).

out any costs. For example, the European Commission (EC) has opened formal investigations and issued statements of objections regarding Google's abuse of its dominant position in the Internet software markets for general internet search services, licensable smart mobile operating systems, and app stores for the Android mobile operating system.[21] In each case, the alleged abuse has been based on Google's desire to exploit switching costs with respect to search engines and browsers.

In April 2015, the EC issued a statement of objection alleging Google "has abused its dominant position in the markets for general internet search services in the European Economic Area (EEA) by systematically favouring its own comparison shopping product in its general search results pages."[22] The EC is concerned that Google's practice of showing Google Shopping more prominently in its search results may "artificially divert traffic from rival comparison shopping services" and harm consumers by preventing them from seeing "the most relevant results" in response to their search queries.[23] The lack of transparency in Google's search results is a form of "switching cost"[24] within the meaning of the 2015 Open Internet Order — in the words of the D.C. Circuit Court of Appeal's opinion addressing the relevance of switching costs in the BIAS context, consumers cannot be "fully responsive" to manipulated search results if consumers are unaware of the practice or its extent.[25]

In April 2016, the EC issued a statement of objection alleging that Google violated antitrust laws by (1) "requiring manufacturers to pre-install Google Search and Google's Chrome browser and requiring them to set Google Search as default search service on their devices, as a condition to

---

[21] European Union, Press Release, Antitrust: Commission sends Statement of Objections to Google on Android operating system and applications (Apr. 20, 2016) [hereinafter "2016 Statement of Objections"], http://europa.eu/rapid/press-release_IP-16-1492_en.htm.

[22] European Union, Press Release, Antitrust: Commission sends Statement of Objections to Google on comparison shopping service; opens separate formal investigation on Android (Apr. 15, 2015), http://europa.eu/rapid/press-release_IP-15-4780_en.htm.

[23] *Id.*

[24] Even if a transparency issue of this type were not considered a form of "switching cost" in the antitrust context, such costs are considered in antitrust analyses. *See* Chris Wilson, "Markets with Search and Switching Costs" (May 6, 2006), https://mpra.ub.uni-muenchen.de/131/1/MPRA_paper_131.pdf.

[25] *See* Verizon v. FCC, 740 F.3d 623, 648 (D.C. Cir. 2014).

license certain Google proprietary apps"; (2) "preventing manufacturers from selling smart mobile devices running on competing operating systems based on the Android open source code"; and (3) "giving financial incentives to manufacturers and mobile network operators on condition that they exclusively pre-install Google Search on their devices."[26] The European "Commission's investigation showed that it is commercially important for manufacturers of devices using the Android operating system to pre-install on those devices the Play Store, Google's app store for Android"[27] (the "choice of the default option" in terms of behavioral economics). According to the EC, because Google has made licensing the Play Store conditional on Google Search being pre-installed and set as default search service on Android devices, rival search engines are not able to become the default search service on the significant majority of Android devices sold in Europe. Google has similarly made licensing the Play Store a condition on pre-installation of its Chrome browser, another "important entry point for search queries on mobile devices."[28]

The EU thus found that the choice of the default option is a significant barrier to switching between internet search engines and browsers — i.e., consumers cannot (and do not) instantaneously switch from the search engines and browsers that are offered on their mobile devices by default. In other words, when a particular device ships with only one default search engine and/or browser, a consumer must, at a minimum, absorb the cost of searching for and downloading a rival search engine and/or browser before switching,[29] and the EU found that this cost is competitively significant.

---

[26] 2016 Statement of Objections.

[27] *Id.*

[28] *Id.*

[29] Switching costs include "the value of users' time." Aaron Edlin and Robert Harris, "The Role of Switching Costs in Antitrust Analysis: A Comparison of Microsoft and Google," 15 YALE J. L. & TECH. 169 at p. 9 (quoting Joseph Farrell & Paul Klemperer, "Coordination and Lock-in: Competition With Switching Costs and Network Effects," in 3 HANDBOOK OF INDUS. ORG. 1967, 1971 (M. Armstrong & R. Porter eds., 2007)), https://works.bepress.com/aaron_edlin/82/download/. Switching default search engines involves other barriers as well, including learning costs. *See, e.g.*, J.D. Biersdorfer, "Changing the Search Engine in Microsoft Edge," NEW YORK TIMES (Sep. 25, 2015) (addressing a user's difficulty in figuring out how to switch the default search engine in Microsoft's Edge browser).

Indeed, according to a paper sponsored by Google, "In many cases, the value of users' time is the most important component of switching costs."[30]

Antitrust precedent also recognizes that switching costs are particularly high with respect to operating systems — one of the categories of internet platform the FTC found has the same or similar ability to collect consumer information as BIAS. In *United States v. Microsoft Corp.*,[31] the cost of switching operating systems was instrumental to the government's case that Microsoft had monopoly power.[32] The Apple Macintosh operating system was excluded from the relevant market because "customers would not switch from Windows to a Mac OS in response to a substantial price increase because of the costs of acquiring the new hardware needed to run Mac OS (an Apple computer and peripherals) and compatible software applications, as well as because of the effort involved to learning the new system and transferring files to its format."[33]

FCC statement. "Providers of BIAS ('broadband providers') thus have the ability to capture a breadth of data that an individual streaming video provider, search engine or even e-commerce site simply does not."[34]

Analysis. *First*, the Marketing NPRM acknowledges that a BIAS provider cannot, as a technical matter, monitor traffic transmitted between a consumer and a destination when that traffic is encrypted,[35] but makes no effort to consider the extent to which internet traffic is encrypted or the effect that encryption has on the breadth of data that can be collected by BIAS providers versus non-BIAS providers. Given the apparent consensus among the FCC and outside experts that a BIAS provider's ability to collect and use consumer data is "comprehensive" only to the extent "users interact with websites or use apps or devices that do not support encryption or do not enable it by

---

[30] *Id.* at p. 9, n. 17.

[31] 253 F.3d 34 (D.C. Cir. 2001).

[32] *See* Edlin, *supra* note 27, at p. 19.

[33] *Microsoft Corp.*, 253 F.3d at 52.

[34] Marketing NPRM at ¶ 4.

[35] *See id.* (noting that BIAS providers can monitor traffic only "absent use of encryption").

default,"[36] any rational analysis of the difference between BIAS and non-BIAS providers with respect to data collection must consider the extent to which encryption is available, the extent to which it is actually used, and the specific limitations that encryption places on BIAS providers' collection of data versus non-BIAS providers' collection of data.

Second, this FCC statement is irrelevant to consumer privacy to the extent it compares the ability of BIAS providers' to collect data, singly or in the aggregate,[37] with the ability of a single non-BIAS provider to collect data. Consumers' interest in avoiding invasions of their privacy do not differ depending on the identity or affiliation of the invaders. A person who has chosen to keep particular information private suffers the same indignation whenever the information is revealed; the damage to a person's dignity does not depend on whether the revelation is made by one or more BIAS providers, one or more non-BIAS providers, or even an ordinary peeping Tom. If a group of unaffiliated non-BIAS providers has the same or substantially similar ability as one or more BIAS providers to collect and combine consumer information — as factual experts in this proceeding have demonstrated[38] — then the group of non-BIAS providers presents just as great a threat to consumer privacy as BIAS providers.

FCC Statement. "But this NPRM looks to learnings from the FTC and other privacy regimes to provide complementary guidance."[39]

Analysis. The FCC's attempt to rely on the FTC's privacy framework as a reason for imposing discriminatory privacy obligations on BIAS providers is irrational, because the FCC's conclusion that BIAS providers are different from non-BIAS providers with respect to consumer privacy

---

[36] *See, e.g.*, FCC Overreach: Examining the Proposed Privacy Rules: Hearing Before the Subcomm. on Commc'ns and Tech. of the H. Comm. on Energy and Commerce, 114th Cong. 3 (2016) (statement of Paul Ohm, Prof., Georgetown University Law Center) ("When users interact with websites or use apps or devices that do not support encryption or do not enable it by default, a BIAS provider's ability to spy is complete and comprehensive."), https://energy-commerce.house.gov/hearings-and-votes/hearings/fcc-overreach-examining-proposed-privacy-rules.

[37] It is unclear from the Marketing NPRM whether the FCC was comparing (1) a single BIAS provider to a single non-BIAS provider, or (2) all BIAS providers to a single non-BIAS provider.

[38] *See* Swire, *supra* note 12.

[39] Marketing NPRM at ¶ 4.

issues directly contradicts the FTC's own findings on the matter.[40] The FTC applied its framework to "all commercial entities," including both online and offline collection of consumer data, because, "Whether such collection occurs online or offline does not alter the consumer's privacy interest in his or her data."[41] The privacy framework adopted in the 2012 FTC Privacy Report on which the FCC so heavily relies thus does not have any potential to harm competition, cause consumer confusion, or distort the market for internet services like the FCC's proposal does.

Section 222 Does Not Require Discriminatory Privacy Regulation

The fact that BIAS providers do not present a greater threat to consumer privacy online than non-BIAS providers means the FCC's proposal to apply unusually strict privacy rules only to BIAS providers will not actually protect consumers privacy online. It also means the FCC's proposal is unreasonably discriminatory, and like all unreasonably discriminatory regulatory provisions, has the potential to adversely affect online competition and distort the markets for online advertising, "big data," and the "internet of things." It will not serve the public interest to apply one set of privacy rules to non-BIAS providers (the FTC's rules) and another set of privacy rules to BIAS providers (the FCC's rules) when the disparity ***will*** harm competition ***without*** protect consumers' privacy.

But the Marketing NPRM does not frame the issue in terms of the public interest or competition, and it does not consider the extent to which the FCC's propose rules would or would not enhance consumer privacy. It instead attempts to justify its discriminatory proposal through a two-step, "legal" sleight of hand: (1) The FCC notes that it classified BIAS as a "telecommunications service" in the 2015 Open Internet Order, and (2) then notes that section 222 requires the FCC to apply certain privacy obligations to telecommunications services and not to other services.[42] The FCC thus implies that, in order to comply with the will of Congress, the agency has no choice but

---

[40] *See* 2012 FTC Privacy Report at p. 56 ("ISPs are just one type of large platform provider that may have access to all or nearly all of a consumer's online activity. Like ISPs, operating systems and browsers may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles.").

[41] *Id.* at p. 18.

[42] Marketing NPRM at ¶ 13.

to apply section 222 to BIAS providers (including a host of new privacy protections that have never been applied to plain old telephone service under that same statutory provision).

As the FCC demonstrated in the 2015 Open Internet Order (in which the FCC chose to forbear from applying a host of statutory provisions in Title II of the Communications Act), however, the FCC has enormous discretion to determine whether or not it should apply a particular statutory provision.[43] Although the FCC previously decided it should apply section 222 to BIAS, that decision is no more sacrosanct than the FCC's initial classification of BIAS as an "information service" in 2002 — the FCC still can (and should) forbear from applying section 222 to BIAS.

Even if it does not reconsider its forbearance decision, the FCC can still use its forbearance authority selectively to apply section 222 to BIAS providers in a manner that is fully consistent with the FTC's privacy framework and avoid the discriminatory regulation of BIAS and non-BIAS providers with respect to privacy. In the latter case, the only difference between the FCC's and the FTC's privacy frameworks would be the identity of the enforcing agency.

The Proposed Privacy Regulations Would Be Unlawful

For the reasons noted above, the FCC's proposal does not satisfy the applicable standards of review under the Administrative Procedure Act (APA) or the First Amendment. Because a court would apply either strict scrutiny or the "intermediate" *Central Hudson*[44] standard to a First Amendment analysis, both of which are more demanding than the arbitrary and capricious standard under the APA, this section applies the APA standard for the sake of brevity.

Under the APA, "Normally, an agency rule would be arbitrary and capricious if the agency has relied on factors which Congress has not intended it to consider, entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or

---

[43] *See* 2015 Open Internet Order at ¶¶ 434-532.

[44] *See* Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 564-66 (1980).

the product of agency expertise."[45] As described above, the FCC entirely failed to consider important aspects of the online privacy problem and, to the extent the FCC concluded that BIAS providers are a greater threat to online privacy than non-BIAS providers, the FCCs' decision runs counter to the evidence. It is simply irrational for the FCC to conclude that imposing discriminatory privacy rules on BIAS providers will protect consumer privacy when half of the world's most valuable companies are internet "edge" providers who have built their empires on the collection and exploitation of consumers' online data.[46]

Conclusion

The public interest would be best served if the FCC were to exercise its authority to forbear from applying section 222 to BIAS providers and leave internet privacy matters to the FTC, or alternatively, to adopt rules that are fully consistent with the FTC's current privacy framework. The FTC's current privacy framework has proven successful in allowing the internet to flourish, and to the extent additional privacy protections might be warranted in the future, the FTC is more than competent enough to implement them to BIAS and non-BIAS providers alike in a fair and non-discriminatory manner.

Respectfully submitted,

TECH KNOWLEDGE

By: /s/ FBCJR

Fred B. Campbell, Jr.
Director
14925 Doe Ridge Road
Haymarket, VA 20169
703-470-4145

July 6, 2016

[45] Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983).

[46] See https://en.wikipedia.org/wiki/List_of_public_corporations_by_market_capitalization#2016 (listing Apple, Alphabet (Google), Microsoft, Facebook, and Amazon in the top ten largest public corporations by market capitalization.