

**BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION**

In the Matter of:
Protecting the Privacy of Customers of
Broadband and Other
Telecommunications Services

WC Docket No. 16-106

**COMMENTS OF PUBLIC KNOWLEDGE, THE BENTON FOUNDATION,
CONSUMER ACTION, CONSUMER FEDERATION OF AMERICA, AND
NATIONAL CONSUMERS LEAGUE**

Meredith F. Rose, Harold Feld, Dallas
Harris, and Mojdeh Bowers¹
Public Knowledge
1818 N Street NW, Suite 410
Washington, DC 20036

May 27, 2016

¹Special thanks to Tennyson Holloway, former Mozilla Fellow at Public Knowledge, for his research and technical expertise.

**COMMENTS OF PUBLIC KNOWLEDGE, THE BENTON FOUNDATION,
CONSUMER ACTION, CONSUMER FEDERATION OF AMERICA, AND
NATIONAL CONSUMERS LEAGUE**

Contents

- I. Broadband Internet Access Service Providers Occupy A Unique Gatekeeper Position In The Internet Ecosystem. 3
 - A. The Value And Power Of User Data 4
 - 1. The Increasing Importance Of Predictive Analysis Creates A Market For Broadband Providers’ Uniquely Granular Data 6
 - 2. The Real Value Of BIAS Data 12
 - B. Broadband Networks Experience Systemic Issues That Are Not Easily Resolved 17
 - 1. Multiple Device Usage Increases, Not Decreases, The Granularity Of Data That A BIAS Provider Can Collect On Its Users. 17
 - 2. Traffic Remains Largely Unencrypted. 19
 - 3. VPNs And Other Technical Methods Available To Consumers Do Not Resolve The Problem 22
 - C. The Burden Of Protecting A User’s Information Must Fall On The Provider, Not The Consumer. 24
 - 1. All Information Must Be Treated As Sensitive Information 24
 - 2. Consumers Must Not Be Expected To Adopt Expensive “Self-Help” Measures In Order To Protect Their Statutory Rights 26
- II. The Customer Must Be Queen Of Her Information 27
 - A. Privacy Rules Must Offer A Meaningful Scope Of Protection 27
 - B. The User’s Control Over Her Information Must Be Meaningful 28
 - 1. An Opt-In Framework Would Be More Appropriate For Affiliate And “Related Telecommunications Services” Marketing 31
 - 2. “Pay for Privacy” Regimes May Deprive Users Of Meaningful Choice Regarding Management Of Their Private Data 32
 - 3. The User Must Be Given Meaningful Opportunities To Exercise Control Over Their Data 32
 - C. Other Issues 33
 - 1. Mandatory Arbitration Contracts In Title II Services Have Been Found Violative of §208 And Thus Should Be Prohibited In BIAS Contracts 33
 - 2. Competitive Concerns Underlying The Role Of Section 222(b) Require A Similarly Updated Framework 34
 - 3. The Current Proceeding Fulfills The Commercial Speech Test 35
- III. Conclusion 39

I. Broadband Internet Access Service Providers Occupy A Unique Gatekeeper Position In The Internet Ecosystem.

BIAS providers are gatekeepers to the Internet. This position is unique to BIAS providers, and carries substantial implications for consumers, as the Commission has previously recognized.² While traffic splinters among providers at the edge, *all* data — sensitive, non-sensitive, and everything in between — must pass through the hands of an ISP.

When data is commodified, this is a very lucrative position to occupy — and the economic reality of the American broadband market, with its market concentrations that tend toward monopoly, means that there has been zero competition (meaningful or otherwise) on the privacy axis. Barring a radical reorganizing of the broadband market as it exists, consumers have no means of exercising control over their information or preventing it from being collected, packaged, and monetized by their broadband providers. No ISP enjoys an unfettered right to abuse its market position in one line of business (broadband provision) to gain a competitive advantage in a separate line of business (predictive advertising) — and it most certainly does not enjoy the right to do so without regard to the wishes of those customers whose personal data is being leveraged.

The different ways that broadband providers can exploit the information that consumers must expose as part of receiving service — as well as the certainty that the most sensitive information will flow over the network — justify Congress' decision to design unique privacy protections for common carriers. As Senator Leahy recently noted in a letter to the

²See *In re* Protecting & Promoting the Open Internet (“*Open Internet Order*”), 30 F.C.C. Rcd. 5601 (2015) [hereinafter *Open Internet Order*] (Report and Order on Remand, Declaratory Ruling, and Order), available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1_Rcd.pdf.

Commission, “[t]he patchwork of state privacy laws and Federal Trade Commission enforcement are not adequate protections” for consumers.³ This is doubly true when dealing with network gatekeepers. The FTC’s privacy approach — that consumer privacy is best served by holding companies to their promises — is rooted in a model that fundamentally assumes a competitive market and robust consumer choice. Broadband is not, however, a freely competitive market, as the Commission has already found.⁴ This difference in approach between the FCC and FTC is one of design, not accident; suggestions, therefore, that the FCC should abandon the role given it by Congress are contrary to the entire purpose of the statute and the specific statutory framework created by Congress in the FTC Act and the Communications Act.

A. The Value And Power Of User Data

A BIAS provider can paint a detailed composite portrait of a user’s life solely from basic header information such as IP addresses, ports, and timing. As Professor Nick Feamster of Princeton University recently explained in a letter to FCC Chairman Wheeler, “[w]e can learn so much from this traffic that we’ve written papers with conclusions about human behavior solely based on our analysis of the traffic that ISPs can see.”⁵

The IP address of a packet’s intended recipient can reveal a great deal about its sender: sustained visits to the Disney website, job search sites, or domestic violence support fo-

³Letter from Senator Patrick Leahy, to Tom Wheeler, Chairman, Federal Communications Commission (May 26, 2016).

⁴*In re* Deployment of Advanced Telecomms. Capability to All Americans in a Reasonable & Timely Fashion, GN Docket No. 15-191 (Jan. 29, 2016) (2016 Broadband Progress Report).

⁵Letter from Nick Feamster, to Tom Wheeler, Chairman, Federal Communications Commission 1 (Mar. 3, 2016), *available at* <http://ftt-uploads.s3.amazonaws.com/fcc-cpni-nprm.pdf>.

rum paint very different (and deeply private) images of a customer's life.⁶ IP addresses are also easily geographically locatable, and thus generate location data for both the subscriber and the service being accessed.⁷ And while it is true that the physical location of most Internet services is relatively uninteresting from a privacy perspective — everyone knows where Amazon is located — peer-to-peer or direct-connection services such as Skype route directly from individual-to-individual.⁸ Thus, IP address information could potentially not only reveal the subscriber's location, but also the locations of their friends, relations, and associates.

Port numbers often reveal the exact nature of the communication, even without deep packet inspection. Web page requests route through port 80,⁹ emails through port number 25,¹⁰ and Spotify peer-to-peer distribution through port 4070.¹¹ A pattern of port number usage can thus reliably reveal the types of services that the subscriber uses, and, by extension, the subscriber's interests or line of work. If, for example, a BIAS provider notices a subscriber frequently using port number 22, then the provider could easily infer that the

⁶See, e.g., Tech. Analysis Branch, Office of the Privacy Comm'r of Can., *What an IP Address Can Reveal About You* (2013), https://www.priv.gc.ca/information/research-recherche/2013/ip_201305_e.pdf (noting wide range of information that may be discerned from an IP address).

⁷See Dan Jerker B. Svantenson, *Geo-Location Technologies and Other Means of Placing Borders on the "Borderless" Internet*, 23 J. Marshall J. Computer & Info. L. 101, 109–11 (2004).

⁸Cf. Brian Krebs, *Privacy 101: Skype Leaks Your Location*, Krebs on Security (Mar. 13, 2013), <http://krebsonsecurity.com/2013/03/privacy-101-skype-leaks-your-location/>.

⁹See J. Reynolds & J. Postel, RFC 1700, *Assigned Numbers 19* (1994), <https://www.ietf.org/rfc/rfc1700.txt>.

¹⁰See *id.* at 16; Jonathan B. Postel, RFC 821, *Simple Mail Transfer Protocol 44* (1982), <https://www.ietf.org/rfc/rfc821.txt>. Some Internet service providers already inspect subscriber data for port 25 traffic, primarily to block spam. See Chris Wilson, *What's "Port 25," and What Does It Have to Do with E-mail Spam?*, Slate Mag. (July 1, 2008), http://www.slate.com/articles/news_and_politics/explainer/2008/07/the_spam_superhighway.html.

¹¹See *How Do I Configure My Router for Spotify?*, Spotify Support (last visited Feb. 12, 2016), <https://support.spotify.com/us/problems/#!/article/how-do-i-configure-my-router-for-spotify>.

subscriber is likely a computer software developer or system administrator, since traffic over port 22 generally relates to command-prompt logins to remote servers.¹²

At an even more basic level, the timing of packet traffic can reveal data about a subscriber. Indeed, time of activity can be a matter of great personal privacy, such as when Justice Scalia contemplated “at what hour each night the lady of the house takes her daily sauna and bath — a detail that many would consider ‘intimate.’”¹³ Researchers have found timing so informative that they can decode a person’s password merely by the spacing of keystrokes.¹⁴ Traffic timing can reveal the hours when a subscriber is awake, asleep, or at work. It can reveal a person’s religious beliefs (as with observance of the Sabbath), or unexpected changes in lifestyle, such as holidays, new relationships, or lost jobs — all without the need for deep packet inspection.

1. The Increasing Importance Of Predictive Analysis Creates A Market For Broadband Providers’ Uniquely Granular Data

Before addressing the specifics of the NPRM, it is important to lay out the role that the rise of predictive advertising has had in the explosion of the data commodity market in recent years.

The description of online advertising put forward by opponents of the current rule-

¹²Specifically, port 22 is used for the Secure Shell (SSH) protocol. See T. Ylonen & C. Lonvick, RFC 4253, The Secure Shell (SSH) Transport Layer Protocol 4 (2006), <https://www.ietf.org/rfc/rfc4253.txt>.

¹³*Kyllo v. United States*, 533 U.S. 27, 38 (2001).

¹⁴See Dawn Xiaodong Song, David Wagner & Xuqing Tian, *Timing Analysis of Keystrokes and Timing Attacks on SSH*, 10 Proc. Conf. on USENIX Security Symp. No. 25 (2001), available at https://www.usenix.org/legacy/events/sec01/full_papers/song/song.pdf.

making¹⁵ fails to address the area's most significant trend since 2014: programmatic ad buying.¹⁶ Also called “predictive marketing” or “predictive analytics” (which refers to the broader field of using amassed data on individuals to make accurate predictive judgments as to what they are doing and how they will respond), this approach to targeted marketing uses the numerous data points associated with an individual's online (and offline) behavior to predict with precision when, how, and on what device to deliver an advertisement so as to maximize the likelihood of success.¹⁷

Anthony Iacovone, an early developer of predictive marketing technology, explained the dramatic way this approach differs from traditional behavioral marketing:

Though behavioral targeting may have been considered effective enough in the past, there are inherent limitations that are too fundamental to ignore any longer:

- Targeting individuals who have done something that reveals their interests is not the whole story.
- This data used to target your customer is narrow and often fragmented, which offers limited real advertising value.
- Little or no correlation is made between the behavioral data collected and other conditions (i.e. location, time of day, weather, etc.).

The amount of wasted impressions and missed opportunities using current targeting methods is astounding. Why would you ignore millions of mobile users who haven't yet visited your site or displayed a specific behavior? Many of them may actually be prime for your campaign. Predictive targeting offers a way to find them, and you can't afford to ignore it.¹⁸

¹⁵See, e.g., Peter Swire et al., *The Inst. for Info. Sec. & Privacy at Ga. Tech, Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* (Feb. 29, 2016) (white paper), available at http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf.

¹⁶See Alex Kantrowitz, *10 Things You Need to Know About Programmatic Buying*, AdvertisingAge (June 1, 2015), <http://adage.com/article/print-edition/10-things-programmatic-buying/298811/>. (noting that spending on programmatic ad buying increased from \$9 billion to \$14 billion from 2014 to 2015).

¹⁷Anthony Iacovone, *The Death of Behavioral Targeting*, Huffington Post (Sept. 26, 2013), http://www.huffingtonpost.com/anthony-iacovone/the-death-of-behavioral-t_b_3990465.html.

¹⁸*Id.*

What makes predictive marketing work is the broad net it casts both in terms of what behavior is considered valuable. No fact is considered too trivial or too far afield. Any digital activity, especially when collected over time and across multiple devices, enriches the profile. “The more that is known about buyers, the more the message and communication can be tailored to meeting pain points and activating them. By coupling what is already known about buyers with predictive analytics, the right patterns or traits can be uncovered.”¹⁹ One analyst points to “IP logs” as precisely the kind of granular information that particularly enhances the predictive power of marketing analytics.²⁰ Increasingly, advertisers prize the power of predictive advertising because it massively improves results over behavioral advertising. According to Direct Marketing News, advertisers using predictive analytics experienced a 25% rise in their return on investment.²¹

Cable operators, with access to both set-top box information and broadband information, are positioned to reap the greatest benefits of this shift from behavioral advertising to the new world of predictive marketing. “Indeed, in television’s most disrupted hour, pay-TV operators are in a prime position to not only control the broadband infrastructure that will transport the video of the future, but also to facilitate the advanced advertising schemes that will support it.”²²

¹⁹Mary Wallace, *Exploring the Cutting Edge: Predictive Marketing Analytics*, Marketing Land (Feb. 3, 2015), <http://marketingland.com/another-prediction-this-one-is-85-accurate-114919>.

²⁰*Id.* (also noting that effective use of predictive analytics increases accuracy by up to 85%).

²¹Al Urbanski, Senior Editor, *Predictive Analytics Is Paying Off for Marketers*, Direct Marketing (Nov. 2, 2015), <http://www.dmnews.com/dataanalytics/predictive-analytics-is-paying-off-for-marketers/article/450692/>.

²²Daniel Frankel, *From DAI to programmatic: Why advanced advertising is giving pay-TV operators a reason to stay in the video biz*, FierceCable (Dec. 1, 2015), <http://www.fiercecable.com/special-reports/dai-programmatic-why-advanced-advertising-giving-pay-tv-operators-reason-st>.

BIAS providers are significant participants in the cross-platform advertising business. In response to the demand for the kind of granular data that only ISPs can provide, the largest providers have invested enormous amounts of money in the technical capacity to harvest subscriber information, analyze it, and monetize it.²³ This, in turn, has resulted in significantly enhanced revenue for BIAS providers.

Opponents of the rulemaking, ignoring the reality of the predictive advertising industry, have publicly relied on claims made in a February 2016 report by Professor Peter Swire and colleagues at The Institute for Information Security and Privacy at Georgia Tech. Swire's report was, in its own words, "intended to provide a factual and descriptive foundation for making public policy decisions about the privacy framework that should apply to ISPs and other companies that collect and use consumers' online data."²⁴ However, while the report claims to give "an up-to-date and accurate understanding of [the broadband] ecosystem,"²⁵ it ignores the explosion of predictive analysis and its increasing importance in online advertising and product development.

This failure to account for the rise of predictive analysis in marketing fatally undermines the central thesis of Swire's argument. Opponents of the current rulemaking cite the Swire Report to argue that the rise of encryption — either through websites encrypting their traffic or through services such as virtual private networks (VPNs) — sharply reduces

²³See, e.g., Anthony Crupi, *Cablevision 'TAPPS' Into the Power of Addressable Advertising*, AdvertisingAge (Apr. 30, 2015), <http://adage.com/article/media/cablevision-tapps-power-addressable-advertising/298339/>. ; Oracle, *Verizon Personalizes Marketing Communication with Oracle* (Video), <https://www.oracle.com/marketingcloud/customers/success-stories/verizon.html>.

²⁴Swire et al., *supra* note 15, at 6.

²⁵*Id.* at 3.

the value of the information uniquely available to BIAS providers.²⁶ But predictive analysis depends much more on data related to patterns or use than it does on actual content to build individual profiles. Put more simply, whereas the old behavioral advertising discussed in the Swire report relied chiefly on knowing what movies you streamed, modern predictive analysis places a higher value on knowing details such as the time of day you stream, how long you watch, and what device you use to watch it. To advertisers trying to build an effective commercial, these details are far more valuable than the gross data on whether prefer rom coms or spy thrillers.

By updating our understanding of the modern Internet marketplace to include the dramatic rise of predictive marketing over the last two years, we observe that:

1. ISPs do have a unique perspective on consumer online activity that is different from that of other providers in the ecosystem;
2. This unique perspective confers enormous financial and anti-competitive benefits to BIAS providers in the manner Congress intended to prohibit; and,
3. It does so because predictive analytics works by accumulating as many data points over time about the target.

This last point is extremely important, as it addresses a key fallacy that runs throughout the opposition's logic. Swire and others argue that it is search engines and social networks,

²⁶It is worth noting that, in response to Feamster's letter, Swire fully embraced — in direct contradiction of his earlier paper — Feamster's conclusions on the visibility of traffic to ISPs and the ability to use this information for predictive purposes. Swire's sole objection to Feamster's critique was that he believed his conclusions were not "*technically* inaccurate" (emphasis added). Letter from Peter Swire, to Professor Nick Feamster, Acting Director, Center for Information Technology Policy, Princeton University (Mar. 6, 2016), available at <http://peterswire.net/wp-content/uploads/feamster-swire-final.pdf>.

rather than ISPs, that are the “greater” danger to consumer privacy, and that adopting the proposed rules will somehow either fail to have positive benefits, or will actively make things worse for consumers. But this principle of *argumentum ad Google* is not merely wrong on the law (as the FCC is obligated by Congress to protect consumer privacy in telecommunications, while the FTC is prohibited from doing so); nor is it merely an example of the fallacy of “making the perfect the enemy of the good.” As discussed below, when incorporating the importance of predictive analytics, it is also false to fact.

None of this engenders confidence in the conclusions contained in the Swire report. As Professor Feamster noted, “[t]he technical inaccuracies concerning ISP capabilities in [the Swire Report] reflect some basic misunderstandings of Internet protocols, as well as the current Internet ecosystem.”²⁷ In response, Professor Swire does not dispute the statements made by Professor Feamster that ISPs can see many details about online usage patterns even when traffic is encrypted through VPNs or other means.²⁸ Nevertheless, Swire has not retreated from his core claim that — despite the unique availability of this detailed information to broadband providers — nothing in the way BIAS providers handle this information raises unique concerns in light of the information already collected by Google and others. Even disregarding its potential technical shortcomings, the Swire report is — by its author’s own concession²⁹ — out of date, and intentionally lacking relevant context.

²⁷Feamster, *supra* note 5, at 3.

²⁸Swire, *supra* note 26.

²⁹*Id.*

2. The Real Value Of BIAS Data

The data collected by BIAS providers is enormously commercially valuable in and of itself. BIAS providers, however, use their position to enhance the value of the data in two unique ways. First, BIAS providers blend this information with unique information obtained from non-Internet services, particularly cable set-top box (STB) information. Second, BIAS providers have unique information on the use of devices in the home that are inaccessible to individual edge providers such as Google or Facebook.

Consider the following example of a single adult individual subscribing to a cable broadband provider for video and broadband. Let us assume that Comcast subscriber Jane Doe decides to start working out. Investigating online (using Google), Jane decides that she will get a FitBit so that she can measure her progress. Jane flushes her cookies and uses encryption like a good, technologically savvy, privacy conscious consumer. She then goes to Amazon and buys a FitBit.

Google, of course, knows the nature of the searches and may deduce by the pattern that Jane was interested in buying a FitBit, possibly for herself and possibly for someone else. Because Jane is using encryption and following best practices, Google should not be able to track her next activity. Even if Google does track her to Amazon, it may guess, but cannot be sure, that Jane bought a FitBit. At this point, Google can collect no more information about this particular search/transaction.

Amazon, for its part, knows that Jane bought a FitBit; that it is not a gift (or at least was not ordered as a gift); and that it arrived at her house at such-and-such a date at such-and-so a time. If Jane decides to come back and write a review of the FitBit, Amazon will

know that as well. But otherwise, Amazon is likewise finished with studying Jane and her FitBit.

Comcast, on the other hand, is only just getting started on what it knows about Jane and her FitBit.

Comcast, of course, knows everything that Google knows (it knows Jane went to Google, it knows what IP addresses she clicked on in response to the search, how long she stayed at each page, and lots of other information that allows Comcast to know Jane's search pattern). Comcast knows Jane went to Amazon, and can guess from the pattern of internal URLs returned to Jane that she purchased a FitBit.

But Comcast also knows when Jane activates her FitBit. The FitBit app opens on her computer and immediately communicates to an IP address associated with FitBit's servers. Comcast also knows every other time Jane synchs her FitBit and how long the device is in communication with the FitBit server. Is Jane synching it every day? Every few days? Did she start strong, then gradually lose interest? Comcast knows based on the pattern of synching her home device with FitBit's server.

Amazon and Google can never know this information. Jane's FitBit does not communicate with Google or Amazon. If Jane is deleting tracking software and using encryption, then Google and Amazon will never know the behavior pattern of Jane's FitBit, and whether she has other associated behavior patterns.

Comcast, on the other hand, must know all this information in order to function as an ISP. Mind you, Comcast does not have to use this information in any way once it has completed the FitBit synching. Further, under the Commission's proposed rules, Comcast could not collect such personal information about Jane and her fitness program (or lack

of fitness program over time) to exploit for purposes that Jane cannot even imagine.

But let us pretend that somehow Google and Amazon were able to know everything Comcast knows. This would not diminish the value of Comcast's information. Not only would it spare Comcast the expense of buying the information from someone else so that it could insert its own advertising, but the Comcast information would still retain independent value to third party data brokers. Remember, the value of predictive marketing comes in the volume of information. Having multiple confirmations from multiple sources, e.g., Google, Amazon and Comcast, enhances the ability to predict Jane's behavior.

It is important to stress this is but one, simplified example. The FitBit is only one piece of Jane's online information footprint, which is combined with thousands of other data points. Does Jane's use of FitBit, for example, increase after Jane joins an online dating site? In response to online travel plans? In response to impending dates such as birthdays or high school reunions? These correlations are trivially easy for an ISP under the existing regulatory regime.

Nor are broadband providers shy about how they scrape such data. As Jeffrey Chester discusses at great length,³⁰ major BIAS providers regularly highlight the invasiveness and ubiquity of their tracking schemes. AT&T's Vice President of Marketing and Ad Sales, Maria Mandel Dunsche, boasted that "[AdWorks'] value proposition is to find and target audiences based on the data we have that nobody else has access to."³¹ This data includes "what wireless device they are using, what operating system they are using for their device,

³⁰Jeffrey Chester, Ctr. for Digital Democracy, *Big Data is Watching: Growing Digital Data Surveillance of Consumers by ISPs and Other Leading Video Providers* (Mar. 2016) (white paper), available at <https://www.democraticmedia.org/sites/default/files/field/public-files/2016/ispbigdatamarch2016.pdf>.

³¹eMarketer, *An Interview with Maria Mandel Dunsche* (last visited May 12, 2016), <http://www.emarketer.com/corporate/clients/att>.

how large a data plan they have, and when their contract expires,”³² as well as “single-person household viewer data derived from 15 million AT&T U-Verse set-top boxes.”³³ The company’s Every Addressable TV campaign “is fueled by proprietary insights aggregated from over 12 million households, yielding invaluable information about an advertiser’s true target.”³⁴ The company also offers services including “In-Store Boost,” a hyper-local geo-location tracking function that monitors the “path to purchase” from the moment a consumer receives a television ad to the moment she makes a retail transaction for the advertised good.³⁵ And Cablevision, in an ad for its “Total Audience Application” marketing suite, showcases the ability for marketers to target audiences by ethnic group, income, and presence of children.³⁶

Finally, it is also worth noting that those advancing the *argumentum ad Google* appear to imagine that there is no harm in allowing the ISP itself to have the information. As a recent news story about Cable One proves, however, ISPs may use information collected for one reason (in this case, billing) to perform predictive analytic analysis to discriminate against customers in impermissible ways.

As reported in Fierce Cable, Cable One CEO Thomas Might described at an investor

³²FierceCable, *AT&T AdWorks Adds Anonymous Wireless Customer Data to TV Ad Targeting Platform*, FierceCable, July 29, 2014, <http://www.fiercewireless.com/story/att-adworks-adds-anonymous-wireless-customer-data-tv-ad-targeting-platform/2014-07-29>.

³³Kelly Liyakasa, *AT&T AdWorks Officiates Marriage Between Mobile Data And TV Audience*, AdExchanger, July 30, 2014, <http://adexchanger.com/digital-tv/att-adworks-officiates-marriage-between-mobile-data-and-tv-audiences/>.

³⁴Press Release, *AT&T AdWorks: Leading the Charge in Addressable TV Advertising* (Nov. 29, 2015), available at <http://www.adweek.com/sa-article/att-adworks-leading-charge-addressable-tv-advertising-168311>.

³⁵AT&T AdWorks, *Research* (last visited May 12, 2016), <http://adworks.att.com/research.html>.

³⁶Namakula Mu, *Cablevision ‘Tapp’*, Vimeo, <https://vimeo.com/144146415>.

conference how Cable One had reduced the cost of maintaining “hollow value” customers, *i.e.* customers who provide much lower, or even negative, return on investment.³⁷ Cable One collected the billing information of all hollow value subscribers, then combined it with third party data to determine if there were any predictors they could use to screen customers before their billing history identified them as hollow value customers. Cable One discovered that customers with low credit scores were much more likely to become hollow value subscribers, and that knowledge of a subscribers credit score at the point of sale predicted the customer’s future payment patterns and purchase of additional services with reasonable accuracy.

As a consequence, Cable One instituted of a policy of collecting customer subscriber information, using the information to check the customer’s credit score, and then determining the level of customer service they would provide to a new customer based on credit score. “We don’t turn people away,” Might said, but the cable company’s technicians aren’t going to “spend 15 minutes setting up an iPhone app” for a customer who has a low FICO score.

It does not matter in the slightest who else can obtain the subscriber’s credit score. The harm occurs to this customer because Cable One uses information collected for one purpose (billing information) and then combines it with third party data to use for another purpose (deciding whether or not to provide a customer with standard or sub-standard service).

The Commission’s proposed rule would quite obviously protect Cable One’s customers

³⁷Daniel Frankel, *Cable One using FICO scores to qualify video customers, Might says*, Fierce Cable (May 23, 2016), <http://www.fiercecable.com/story/cable-one-using-fico-scores-qualify-video-customers-might-says/2016-05-23>.

from this kind of secret and undiscoverable discrimination. This benefit would be instantly realized by all Cable One customers (or subscribers to any other ISP that engages in similar practices), even if Google, FaceBook, Twitter, Amazon, McDonalds and every other edge provider is not so regulated. By contrast, waiting until Congress creates a new statute that would regulate everyone will leave broadband subscribers to this kind of discrimination for the foreseeable future.

B. Broadband Networks Experience Systemic Issues That Are Not Easily Resolved

1. Multiple Device Usage Increases, Not Decreases, The Granularity Of Data That A BIAS Provider Can Collect On Its Users.

The proliferation of connected devices, combined with modern app design and data practices, has exponentially multiplied consumer data footprints over the past several years. Rather than fragmenting user data in such a way as to obfuscate it from any given carrier, the current app and device ecosystem creates a “duplicate footprint” that is pushed across all connected providers at once in order to reach all of a consumer’s devices.

This is due in large part to the common practice of multi-platform apps and “push alert” systems. A customer using one app across multiple devices will receive data transferred to that app not only on the device she is currently using, but also on any others on which she has installed the same app. This redundancy (designed to ensure a seamless transition between devices) translates into simultaneous, duplicate traffic over all networks connected to the affected devices. Messaging applications, email, document storage

systems, music libraries, and photo libraries commonly implement such systems to allow total synchronization across all devices — itself no mean feat, given that the average North American Internet user had 6.1 connected devices in 2014.³⁸ But rather than resulting in a clean fracture of a user’s traffic across multiple carriers (as Swire implies),³⁹ data redundancy across devices results in redundancy across networks, giving all providers access to a given communication. Standard operating procedure for multi-platform apps and services is for files, settings, and requests to sync between devices, across all ISPs utilized. An app installed on both a phone and desktop receives the same data over both the phone’s mobile network and the desktop’s home network. As such, valuable traffic remains visible to all ISPs regardless of which network a user is currently activating. In practice, this means that having just one device at home (such as a tablet or desktop) enables your home broadband provider to handle the same push updates you are receiving on your mobile devices, through your mobile provider.

Moreover, any discussion of multiple-device connectivity must take into account the enormous volume of highly granular data provided by Internet of Things-enabled devices. “Smart” devices (such as refrigerators, televisions, or thermostats) are frequently designed as stationary fixtures within a home. In order to function, they must reveal their nature, relative location, and use patterns to the BIAS provider. Even if these devices practice good encryption techniques — which evidence suggests they do not⁴⁰ — BIAS providers

³⁸Cisco, *The Zettabyte Era—Trends and Analysis* (last visited May 13, 2016), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html.

³⁹Swire et al., *supra* note 15, at 7.

⁴⁰Nick Feamster, *Who Will Secure the Internet of Things?*, Freedom to Tinker (Jan. 19, 2016), <https://freedom-to-tinker.com/blog/feamster/who-will-secure-the-internet-of-things/>.

can ascertain a home’s IoT devices by observing unique DNS queries that only IoT devices will make (e.g. to `fridge-software-update.samsung.com`); destination traffic (e.g. constant upstream data to an IP associated with a home-security company); or, if the BIAS provider controls the router, the device name at the router level (e.g. “Tennyson’s Chromecast”). Rather than obfuscating an provider’s view of consumer behavior, IoT devices provide even more detailed and valuable data on a household and its habits than a provider could garner in the absence of such devices.

Critically, IoT devices provide extremely robust and valuable marketing data. If an ISP knows you are transitioning to smart devices, it is a simple matter to target you with advertising for affiliated products. The sudden emergence of regular traffic from a new smart device to an IP address pushing firmware updates for a smart baby monitor immediately flags the subscribers as new parents — prime targets for hawking home alarm systems, CO₂ monitors, children’s programming cable packages, and more.

2. Traffic Remains Largely Unencrypted.

According to a recent report on the state of encryption, few sites provide full, modern HTTPS encryption by default, and many sites still do not support it at all.⁴¹ Additionally, analysis by Upturn shows that of the top 50 sites in the “Health” category, only 86% support encryption by default; in “News,” 90%; and in “Shopping,” 86%.⁴² Moreover, only considering top-site traffic paints a false picture of a user’s behavior, as it neglects to con-

⁴¹Google, *Google Transparency Report: HTTPS on Top Sites* (last visited May 12, 2016), <https://www.google.com/transparencyreport/https/grid/?hl=en>.

⁴²Upturn, *What ISPs Can See: Clarifying the technical landscape of the broadband privacy debate* (Mar. 2016), <https://www.teamupturn.com/static/reports/2016/what-isps-can-see/files/Upturn%20-%20What%20ISPs%20Can%20See%20v.1.0.pdf>.

sider low-volume but high-sensitivity sites such as your child’s school website, or your doctor’s appointment booking system. These sites, while not top-50 websites, may handle critically sensitive information.⁴³

Despite being major generators of behavioral and financial data, e-commerce sites are (contrary to Swire’s claims)⁴⁴ notoriously unencrypted. As of March 3, 2016, the majority of the world’s largest e-commerce sites — including Amazon, eBay, Walmart, Target, Costco, Overstock, Newegg, Apple, Alibaba, and others — do not encrypt connections by default. Most of these sites further “downgrade” encrypted requests, forcing users’ requests for encrypted content to be delivered over a nonsecure (HTTP) method.⁴⁵ The mere fact that a site encrypts its log-in and payment requests — the bare minimum required by common sense — does not render that site “encrypted.” If you’ve ever browsed, searched, or purchased from these websites, then the “growing prevalence of HTTPS”⁴⁶ has not removed visibility of your activities and searches from your ISP. This poor encryption discipline is an advertiser’s dream, leaving everything from Amazon search queries, eBay bid information, and the contents of digital shopping carts visible to BIAS providers at any given moment.

Nor do HTTPS requests remove all valuable information from a provider’s sight. When

⁴³Swire claims that new evidence produced shows that 42 of the 50 top sites by traffic use encryption, accounting for nearly 50% of total traffic. Swire et al., *supra* note 15.. Closer examination of the data reveals that Swire is actually counting sites which encrypt their *login form* — and not necessarily anything else. Of the 50 sites Swire surveys, only 24 of them actually support full HTTPS encryption.

⁴⁴*Id.* at 28.

⁴⁵To determine if a site “downgrades” encrypted requests, a connection request is made via a browser to “https://example.com”, then the resulting connection’s encryption status is observed. If the encrypted request has been downgraded, the resulting webpage will not have “https” in the URL, or will provide an insecure security certificate.

⁴⁶Swire et al., *supra* note 15, at 38.

observing an encrypted connection, the ISP can still see the IP address, the time the request was made, and the amount of information sent between the destination and origin server — all of which is itself deeply descriptive.⁴⁷

Moreover, encrypted connections are rarely made in isolation. Beyond the tangible data about any given request, the ISP has a full record of other encrypted requests made in the same period, and the data about those requests. In the aggregate, this information can reveal what a consumer is doing even *with* encryption turned on. While it is true that encryption deters the most trivial form of traffic analysis (plain-text analysis), network security research has definitively shown that monitoring encrypted connections is more than feasible, and can provide near plain-text results. As one team of researchers noted,

Specifically, we found that surprisingly detailed sensitive information is being leaked out from a number of high-profile, top-of-the-line web applications in healthcare, taxation, investment and web search: an eavesdropper can infer the illnesses/medications/surgeries of the user, her family income and investment secrets, despite HTTPS protection; a stranger on the street can glean enterprise employees' web search queries, despite WPA/WPA2 Wi-Fi encryption. More importantly, the root causes of the problem are some fundamental characteristics of web applications: stateful communication, low entropy input for better interaction, and significant traffic distinctions. As a result, the scope of the problem seems industry-wide.⁴⁸

Even without the researchers' active monitoring techniques, BIAS providers still have access to the “meta-data” associated with encrypted communications. A visit to a modern, encrypted webpage (Gmail, for example) is made up of 100+ initial requests, and depend-

⁴⁷See Upturn, *supra* note 42. While Swire mentions this flow of data, he fails to account for it in his summary, instead asserting (falsely) that “the ISP thus sees, at most, the IP address to which the user originally connected, such as the web server for ExampleShows.com.” Swire et al., *supra* note 15, at 27.

⁴⁸Shuo Chen et al., *Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow*, Proceedings 2010 IEEE Symp. on Security & Privacy 191 (2010), <http://research.microsoft.com/pubs/119060/WebAppSideChannel-final.pdf>.

ing on the nature of the website, additional requests every n seconds or minutes. The ISP can not only see the origin of these requests, but also the “length” of the requests (how many bytes). By taking into account the number of requests, their origin, their frequency, and the size of each request, the ISP, or another middleman, can determine with a high probability what website you visited and what kinds of interactions you had with it.

Again, it is undoubtedly true that, if we are comparing the 90s and early 2000s to today, “ISPs see less because encryption is becoming pervasive.”⁴⁹ However, as long as industry groups like e-commerce continue to hold out with unencrypted connections, and as the feasibility of monitoring encrypted connections rises, the potential for any given ISP to see more of its users’ Internet activity rises correspondingly.

3. VPNs And Other Technical Methods Available To Consumers Do Not Resolve The Problem

VPN and DNS technologies, while important, are not “silver bullets” for BIAS privacy, and it is patently absurd to assume that “these technical blockages mean that ISPs do not and will not have ‘comprehensive’ visibility into user Internet activity.”⁵⁰ First, VPNs do not in all (or even many) cases prevent an ISP from seeing the domain name traffic of their users. Although some VPNs are, in fact, configured to route DNS requests through their encrypted tunnel, this is not a required (or even standard) configuration. Many VPNs suffer from “DNS leak,” in which DNS traffic is not sent over the VPN’s encrypted tunnel. As Upturn notes, “it would be quite difficult for non-experts to tell whether their configura-

⁴⁹Swire et al., *supra* note 15, at 25.

⁵⁰*Id.* at 35.

tion is properly tunneling their DNS queries, let alone to know that this is a question that needs to be asked.”⁵¹

Additionally, VPN access is typically limited to workstations. Laptop and desktop computers have the most advanced support for VPNs, while VPN settings for phones are often complex and difficult to manage. Outside of these devices, VPNs are rare and often poorly supported. IoT devices, for example, have little to no support for proxy or VPN usage. When considered in light of their continued proliferation, more of users’ traffic in the “connected home” will be unencrypted not by choice, but by technical necessity.

The efficacy of VPNs and proxies has long been a topic of debate in the privacy and engineering communities, with its own set of security concerns. The very nature of VPNs requires a user to transfer complete trust of communications from their ISP to the VPN provider. Providers will often advertise free services, such as free proxies or free VPNs, and will monetize them by injecting ads, monitoring traffic, and selling data to advertisers. Outside of corporate-managed VPNs, the marketplace is vast, and finding a reputable company to trust with your internet traffic is a challenging task. Even a cursory examination of popular resources bely the fact that correctly selecting a VPN provider takes extensive research.⁵² VPNs also dampen performance, as they by nature add (at minimum) an extra two hops to a connection (one outgoing to the VPN server and one incoming from the VPN server). These hops can add seconds to every internet connection, and depending on the bandwidth available on the VPN server, can also throttle a user’s connection.

⁵¹Upturn, *supra* note 42.

⁵²“That One Privacy Guy”, *That One Privacy Guy’s VPN Chart* (last visited May 12, 2016), <https://docs.google.com/spreadsheets/d/1FJTvWT5RHFSYuEoFVpAeQjuQPU4BVzbOigToxebxTOW/htmlview?sle>.

C. The Burden Of Protecting A User’s Information Must Fall On The Provider, Not The Consumer.

The mere availability of specialized privacy tools in a highly technical market does not obviate a carrier’s statutory duty to protect its customers’ data under 47 U.S.C. § 222. The position that a customer should exhaust all available avenues of self-help before expecting her BIAS provider to meaningfully protect her data is little more than an attempt to override the will of Congress and, in the end, blame the victim of providers’ opaque practices.

1. All Information Must Be Treated As Sensitive Information

Industry’s repeated insistence that the FCC should abandon its current rulemaking in favor of an “FTC-style” approach to data privacy is patently absurd, and deliberately ignores the outcomes of such an approach in favor of convenient rhetoric.

Under the FTC’s “by type” privacy classification regime, only information deemed especially sensitive (e.g., financial and health information) are subject to unique handling and collection restrictions. Industry representatives have repeatedly demanded that the FCC take a similar approach to privacy in the broadband context. However, implementing this in the broadband context is not feasible, as it would necessarily require ISPs to first determine whether sensitive information is present in any given communication — a task necessarily requiring *manual inspection of each packet — before* applying the appropriate amount of protection.

DPI is not only impractical, but contrary to both the letter and spirit of privacy regulation. Placing a requirement on broadband providers that would result in them view-

ing more details about a customer's communications in the name of privacy is, to put it mildly, self-contradictory. In addition, there is no way that DPI could be implemented with any meaningful consent regime. Because all communications concern at least two parties, there are only a limited number of ways that ISPs could conduct DPI, all of which are untenable:

- *No consent from either party:* As discussed above, DPI without the consent of either party is contrary to the ideas and goals of privacy regulation. ISPs cannot and should not be allowed to view the details of the packets traveling over their network, especially without the consent of the customer.
- *Single party consent:* Assuming one party has consented to DPI and the other party to the communication has not, ISPs would have to either forgo the DPI, risking that the information in that communication does not receive the proper level of protection, or conduct the DPI against the wishes, and likely without the knowledge, of the non-consenting party.
- *Consent from all parties:* Conducting DPI only when all parties to the communication consent would place an undue regulatory burden on ISPs. ISPs would first have to verify how many parties there are to each communication, verify that every party to the communication has consented, and then conduct the DPI and classify the information accordingly. This task becomes increasingly difficult when the parties to the communication have multiple ISPs.

Clearly, DPI is not the most effective way to ensure that the most sensitive information is properly protected. It would be far more efficient — and much more in line with the

FTC’s framework requiring elevated protection for certain sensitive data types — for the Commission to establish a baseline of privacy for *all* communications, any one of which could carry financial, health, or other sensitive information. The Commission should require ISPs treat all information as if it was sensitive, by requiring an opt-in for the sharing of that information. We agree with the FTC’s recognition that certain types of data are, *prima facie*, more sensitive than others. The only way to ensure those extra-sensitive communications are given adequate protection against collection and dissemination by ISPs is to assume that *all* communications could potentially contain such highly sensitive information.

2. Consumers Must Not Be Expected To Adopt Expensive “Self-Help” Measures In Order To Protect Their Statutory Rights

As we have argued elsewhere in the record,⁵³ consumers — low-income or otherwise vulnerable consumers in particular — should not be extorted for an additional monthly VPN subscription, over and above the hefty price of a broadband subscription, in order to protect their statutory privacy rights. Congress did not intend to convert the right of privacy into a luxury good available only to those who can afford it. The design of the Commission’s privacy mandate in § 222 was explicitly designed to “represent a careful balance of competing, often conflicting, considerations. First, of course, is the need *for customers to be sure that personal information that carriers may collect is not misused.*”⁵⁴

⁵³Harold Feld et al., Pub. Knowledge, Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World (Feb. 2016) (white paper), *available at* <https://www.publicknowledge.org/documents/protecting-privacy-promoting-competition-white-paper>.

⁵⁴H.R. 1555, 104th Cong. 90 (1995).

II. The Customer Must Be Queen Of Her Information

Consumer preferences in this realm are not static or even uniform, and consumers must retain the ability to express those preferences on an individualized level. If the consumer wants to sell or trade away her information in a value exchange for targeted goods and services, she should have that right. By the same token, if she places a high value on her privacy and decides that she is better served by restricting the information collected about her online habits, she must have that right as well, and must have the option to exercise it with minimal barriers.

To ensure that both consumers are afforded the individualized levels of protection to which they are entitled, the privacy rules must offer a meaningful scope of protection; the user must be provided meaningful control over her information; and she must have meaningful opportunity to exercise that control.

A. Privacy Rules Must Offer A Meaningful Scope Of Protection

As a preliminary matter, this proceeding — while representing a substantial step toward protecting consumer privacy online — undoes, without explanation, a central holding of the Commission’s 2007 CPNI order. In that Order, the Commission based its decision upon a holding that “CPNI includes personally identifiable information derived from a customer’s relationship with a provider of communications services.”⁵⁵ That conclusion was the central basis upon which the rest of the order rested. Despite the placement of this conclusion in a footnote, its rationale provides the very basis for the decision, thus rendering

⁵⁵*In re* Telecomms. Carriers’ Use of Customer Proprietary Network Info. & Other Customer Info., 22 F.C.C. Rcd. 6927, n.2 (Apr. 2, 2007) (Report and Order and Further Notice of Proposed Rulemaking).

it an agency action under the APA. In order to preserve the proceeding's integrity under the APA, the FCC must address its rationale for rescinding the policy holding underlying the 2007 Order.⁵⁶

Provided, however, that the Commission articulate its reasoning for overturning the 2007 Order, we support the Commission's proposed definitions of customer proprietary information, CPNI, and personal information. In particular, we applaud the Commission's proposal to define "personally identifiable information" as information that is "linked or linkable" with a given individual, as it recognizes the advancements in de-anonymizing technology and the ongoing evolution of that ability in the market.⁵⁷

B. The User's Control Over Her Information Must Be Meaningful

The plain language of § 222 flatly prohibits carriers from using CPNI without customer consent for any purpose other than "provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories." The NPRM proposes applying the Commission's "total service approach"⁵⁸ to broadband, thus allowing

⁵⁶"[T]he agency must examine the relevant data and articulate a satisfactory explanation for its action including a rational connection between the facts found and the choice made," which includes decisions to rescind prior orders. *Motor Vehicle Manufacturers Ass'n of the United States, Inc. v. State Farm Mutual Automobile Insurance Co.*

⁵⁷See e.g. Arvind Narayanan and Vitaly Shmatikov, Robust De-anonymization of Large Sparse Datasets (2008) (IEEE Symposium on Security and Privacy), http://www.cs.utexas.edu/~shmat/shmat_oako8netflix.pdf.

⁵⁸"Under the total service approach, the customer's implied approval is limited to the parameters of the customer's existing service, and is neither extended to permit CPNI use in marketing all of a carrier's telecommunications services regardless of whether subscribed to by the customer, nor narrowed to permit use only in providing a discrete service feature. In this way, the total service approach appropriately furthers Congress' intent to balance privacy and competitive concerns, and maximize customer control over carrier use of CPNI." *In re Telecomms. Carriers' Use of Customer Proprietary Network Info. & Other Customer Info.*, 13 F.C.C. Rcd. 12390 (May 21, 1998) (Order).

for the use of CPNI and PII to “upsell” broadband products. However, previous industry attempts to paint that the concept of “broadband service” as amorphous, and then harness that imaginary ambiguity to commit regulatory arbitrage, makes such a distinction both unworkable and unwise.

When it best suits them, incumbent carriers have attempted to classify all types of services as “broadband,” including services that the average consumer would not expect to be classified as broadband. One example is the ongoing discussion over how to classify video-over-IP or IPTV. Current IPTV providers have argued that they are exempt from public, educational, and governmental (“PEG”) programming requirements because they deliver their services over IP, and (in their vision) are not cable operators offering a cable service under Title VI.⁵⁹ This argument is only one example of the regulatory arbitrage incumbent providers regularly engage in, and it requires little imagination to see that if the total service approach is brought to broadband, incumbents will scramble to claim that IPTV, voice-over-IP, and other IP-delivery services are, in reality, broadband offerings that can therefore be marketed under “implied consent” regimes. It is surely not the Commission’s intention to have services marketed to broadband customers without their consent simply because they are IP enabled, and applying the total service approach to broadband risks exactly that.

⁵⁹See Letter, *In the Matter of Petition for Declaratory Ruling of the City of Lansing, Michigan, on Requirements for a Basic Service Tier and for PEG Channel Capacity Under Sections 543(b)(7), 531(a), and the Commission’s Ancillary Jurisdiction Under Title I 1* (Mar. 9, 2009) (Comments of AT&T Opposing Petitions for Declaratory Ruling), available at https://www.att.com/Common/about_us/public_policy/FCC_PEG_Comments.pdf.; see also *The Impact and Legal Propriety of Applying Cable Franchise Regulations to IP-Enabled Video Services 1* (Sept. 14, 2005) (attached to letter from James C. Smith, Senior Vice President, SBC Services), available at [http://apps.fcc.gov/ecfs/document/view;jsessionid=f2dvTc7GoM1T2S1org8Llh3QQvVyF3KgJ27MyYV8HQkdm8oF8W7z!1281169505!1675925370 ? id=6518157935..](http://apps.fcc.gov/ecfs/document/view;jsessionid=f2dvTc7GoM1T2S1org8Llh3QQvVyF3KgJ27MyYV8HQkdm8oF8W7z!1281169505!1675925370? id=6518157935..)

This exception (and the inevitable arbitrage game that will result) also falls short when measured against the reality of consumer expectations. Under the current rules for use of CPNI in the telephone context, a local exchange carrier could use local service CPNI to market local service offerings, but could not use local service CPNI to target customers to market long distance offerings or CMRS without customer approval. The Commission came to this conclusion based on a finding that “Congress intended that section 222(c) would protect customers’ reasonable expectations of privacy regarding personal and sensitive information.”⁶⁰ In addition, the Commission found that customers do not expect that carriers will need their approval to use CPNI for offerings within the existing total service to which they subscribe.⁶¹ Applying the total service approach to broadband services would run directly *against* consumer expectations, as it would open the door to their “implied consent” being used to market products that do not meet their expectations of “broadband services.”

Moreover, this carte blanche for in-house upselling, when combined with the proliferation of zero-rating among both mobile and fixed carriers, creates a sizable loophole in the opt-in/opt-out framework that forms the backbone of the proposed rules at hand. Rather than endure the burden of complying with a consumer choice framework, carriers would have a monumental incentive to simply market plans which contained zero-rating provisions for affiliated video, voice, or other services. These plans would, under a rational reading of the proposed rules, qualify as “additional BIAS offerings in the same category of

⁶⁰*Telecomms. Carriers’ Use of Customer Proprietary Network Info. & Other Customer Info.*, 13 F.C.C. Rcd. 12390.

⁶¹*Id.*

service (e.g., fixed or mobile BIAS).” To the extent that the Commission has expressed repeated concern about zero-rating, such concern cannot be reconciled against a rule which not only allows, but incentivizes carriers to reframe their marketing as a zero-rating-based incentive program in order to make an end-run around the opt-in/opt-out regime laid out elsewhere.

1. An Opt-In Framework Would Be More Appropriate For Affiliate And “Related Telecommunications Services” Marketing

As the language of the statute clearly requires “approval of the customer” as a prerequisite to sharing data for any purpose other than technical necessity, we feel that the Commission should require affirmative opt-in consent for all such uses of consumer data in the broadband context. The rationale that unexercised opt-out expresses consent relies on numerous, far-reaching assumptions about consumers’ behavior, preferences, and the accessibility of the opt-out mechanism.

However, to the extent that the Commission decides to maintain an “opt-out” category, they should circumscribe it as narrowly as possible. As noted above, the proliferation of IP-based services has opened up numerous attempts at regulatory arbitrage. As such, the Commission should narrowly circumscribe the definition of “communications-related services,” in order to prevent further mischief and attempts to short-circuit the opt-in provisions of the current rulemaking. The Commission must not draw a definition so broad as to include directional service offerings such as music or video streaming, or other “walled gardens” that providers could offer in lieu of obtaining the required opt-in consent for similar non-IP-based services.

2. “Pay for Privacy” Regimes May Deprive Users Of Meaningful Choice Regarding Management Of Their Private Data

We are deeply concerned about the effects of “pay for privacy” regimes on minority communities, low-income neighborhoods, the elderly, and other vulnerable groups. While the current availability of such service (namely AT&T’s \$30 per month “discount” gigabit service) is limited to middle- to high-income areas, such practices in low-income or other vulnerable communities could quickly become prohibitively priced. In households with low income elasticity, even moderate price discrimination between privacy and no-privacy offerings can become coercive inducements. Such inducements could force low-income consumers to choose between exercising their privacy rights, and having a broadband connection at all. This is a choice that no consumer should be required to make, particularly in light of the Commission’s mission of universal access to broadband communications.

3. The User Must Be Given Meaningful Opportunities To Exercise Control Over Their Data

Any interface for communicating a customer’s preferences must be consistently available, static, and as easy as possible to use. We endorse the NPRM’s proposal of a “dashboard” interface which would remain available to all customers and allow them to control the usage of their data for various purposes.

C. Other Issues

1. Mandatory Arbitration Contracts In Title II Services Have Been Found Violative of §208 And Thus Should Be Prohibited In BIAS Contracts

We support the Commission’s proposal to prohibit mandatory arbitration clauses in BIAS contracts. When Congress explicitly provides for remedies to be available to consumers in the agency’s originating statute, as it did in 47 U.S.C. § 208, it is by definition unjust and unreasonable to place arbitrary obstacles in the way of obtaining the relief envisioned by Congress. Implementing §551, §228, and §338(i) requires that consumers have access to those remedies Congress intended to grant. Practices which deny consumers these avenues of relief — and in particular those practices which foreclose access to the FCC complaint process — by necessity violate §201 and §202.

Moreover, the Commission has clear authority and precedent in prohibiting such clauses. The Commission has previously found mandatory arbitration clauses to be violative of §208 and thus of §201(b).⁶² It similarly acknowledged the limitations of arbitration contracts as applied to consumers in the Open Internet Order.⁶³

⁶²“Section 208(a) of the Act authorizes complaints by any person ‘complaining of anything done or omitted to be done by any common carrier subject to the provisions of the Act,’ and under section 208, a party may obtain equitable relief or recover damages if it can establish that a carrier-initiated tariff violates the Act or a rule or order of the Commission.” In the Matter of Gs Tex. Ventures, LLC, 29 F.C.C. Rcd. 10541 (2014) (Order).

⁶³“Commenters suggest that mandatory arbitration, in particular, may more frequently benefit the party with more resources and more understanding of dispute procedure, and therefore should not be adopted. We agree with these concerns and conclude that adoption of arbitration rules is not necessary or appropriate in this context.” Open Internet Order, *supra* note 2, par 267.

2. Competitive Concerns Underlying The Role Of Section 222(b) Require A Similarly Updated Framework

The CPNI provisions of the Telecommunications Act reflect important competitive concerns which should be reflected in the Commission's current rulemaking. The Senate version of the Telecommunications Act of 1996, S. 652, focused primarily on restricting the use of information collected by ILECs from competitors. S. 652 included restrictions on the use of proprietary information in 47 U.S.C. § 252, the section describing structural and non-accounting safeguards for competition in telecommunications services.⁶⁴ Specifically, proposed § 252(f) created:

rules to ensure that the Bell companies protect the confidentiality of proprietary information they receive and to prohibit the sharing of such information in aggregate form with any subsidiary or affiliate unless that information is available to all other persons on the same terms and conditions.⁶⁵

As demonstrated by the limitation of this provision to ILECs and its overall placement as one subsection among other non-accounting safeguards, it is clear that the Senate bill focused primarily on the pro-competitive aspect of what would become known as the CPNI rules. And, as the decade-long BDS proceeding demonstrates, the competitive concerns expressed by Congress in 1996 have not entirely vanished; rather, they have continued and arguably worsened in the 20 years since the Act's passage, and deserve particular consideration in the rulemaking at hand.

⁶⁴S. Rep. No. 104-23, at 22–24 (1995).

⁶⁵*Id.* at 23–24.

3. The Current Proceeding Fulfills The Commercial Speech Test

Because the current proceeding explicitly considers the relative benefits of opt-in and opt-out frameworks in great detail, it fulfills the requirements set forth in *Central Hudson Gas & Electric Corp. v. Public Service Commission* for regulation of commercial speech, and *National Cable & Telecommunications Ass’n v FCC* — not *U.S. West, Inc. v FCC* — controls.

The Commission’s 1998 CPNI Order required carriers to obtain opt-in consent from customers before marketing services to which they do not already subscribe.⁶⁶ The opt-in framework was first challenged in the Tenth Circuit in *U.S. West*, where petitioner telecommunications corporation prevailed on its claim that the framework ran afoul of the First Amendment under the doctrine of commercial speech.⁶⁷ In its 2007 order, the Commission likewise obliged carriers to acquire opt-in consent from carrier customers in order to share their CPI with “joint venture partners or independent contractors for the purpose of marketing communications-related services.”⁶⁸ But ten years after the *U.S. West* decision, the same framework was upheld in the D.C. Circuit, under the same doctrine.⁶⁹ The key difference in outcome between the two seemingly contradictory cases rests on the completeness of the appellate record insofar as it reflects the government’s constitutional burden in defending the opt-in framework’s limitation on commercial speech. An opt-in

⁶⁶*In re* Telecomms. Carriers’ Use of Customer Proprietary Network Info. & Other Customer Info., 13 F.C.C. Rcd. 12390 (May 21, 1998) (Order).

⁶⁷*U.S.W., Inc. v FCC*, 182 F.3d 1224 (10th Cir. 1999).

⁶⁸*In re* Telecomms. Carriers’ Use of Customer Proprietary Network Info. & Other Customer Info., 22 F.C.C. Rcd. 6927 (Apr. 2, 2007) (Report and Order and Further Notice of Proposed Rulemaking).

⁶⁹*Nat’l Cable & Telecomms. Ass’n v FCC*, 555 F.3d 996 (DC Cir. Feb. 13, 2009).

framework, when presented with sufficient evidence, meets the traditional test for an acceptable limitation on commercial speech.

Commercial speech, at its core, is defined as an action that “proposes a commercial transaction.”⁷⁰ Nonmisleading commercial speech is generally safeguarded as a First Amendment concern, though less protected than other forms of speech and subject to certain limitations.⁷¹ There is no dispute in either case that requiring opt-in consent prior to marketing communications-related services is a limitation of commercial speech; however, if such a limitation passes muster under the test set forth in *Central Hudson*, it is constitutionally permissible.⁷² Because the government bears the burden of providing the court a comprehensive record articulating the bases on which its proposed limitation meets the *Central Hudson* test, the Tenth Circuit in *U.S. West* could not find the FCC’s opt-in framework constitutionally permissible due chiefly to a lack of evidence.⁷³ Ten years later, in *NCTA*, the opt-in framework advanced by the Commission in 2007 passed constitutional muster in the D.C. Circuit when the FCC presented a complete record to the court outlining its justification for adopting such a framework. Should the FCC choose to adopt an opt-in framework in order to protect CPI, this approach easily meets *Central Hudson*’s constitutional speech test.

The government’s first requirement under *Central Hudson* is to present a clearly ar-

⁷⁰*Bolger v Youngs Drug Prods. Corp.*, 463 U.S. 60, 64 (1983) (quoting *Ohralik v. Ohio State Bar Assn.*, 436 U.S. 447, 455-456 (1978)).

⁷¹*See Fla. Bar v Went For It, Inc.*, 515 U.S. 618 (1995).

⁷²*Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n*, 447 U.S. 557, 566 (1980).

⁷³*U.S.W., Inc. v FCC*, 182 F.3d 1224, 1234 (10th Cir. 1999).

articulated state interest in limiting commercial speech.⁷⁴ In *U.S. West*, the Tenth Circuit concluded that the government failed to meet its burden because it merely “assert[ed] a broad interest in privacy” rather communicating a specific privacy interest and articulating a justification for defending it.⁷⁵ The 2009 D.C. Circuit, however, found in favor of the opt-in framework when the FCC argued that this requirement, when disclosing CPI to third-party marketers, serves to protect that information from a “greater risk of loss once out of the carrier’s control,” a risk amplified by the simple fact that third parties may not be subject to the same confidentiality demands as carriers under § 222.⁷⁶ Furthermore, the D.C. Circuit held, contrary to the Tenth Circuit’s conclusion, that the interest in protecting consumer privacy is considered a substantial government interest in other commercial contexts and is therefore analogous to the telecommunications space.⁷⁷ An opt-in requirement is likely to meet this initial test of constitutionality where the FCC clearly articulates its reasoning.

Second, the government must show that an opt-in requirement “directly advances the governmental interest asserted.”⁷⁸ In *U.S. West*, the Commission did not present any evidence that a world without an opt-in requirement prior to CPI disclosure for marketing purposes would result in harm to personal privacy, nor did the Commission describe “how and to whom” a carrier would disclose private information without the requirement.⁷⁹ The

⁷⁴*Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n*, 447 U.S. at 566.

⁷⁵*U.S.W., Inc. v FCC*, 182 F.3d at 1235.

⁷⁶*Nat’l Cable & Telecomms. Ass’n v FCC*, 555 F.3d 996, 999 (DC Cir. Feb. 13, 2009).

⁷⁷*Id.* at 1001 (citing *Trans Union Corp. v Fed. Trade Comm’n*, 245 F.3d 809, 818 (D.C. Cir. 2001)).

⁷⁸*Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n*, 447 U.S. at 566.

⁷⁹*U.S.W., Inc. v FCC*, 182 F.3d at 1237.

Court was, again, unable to find in favor of the opt-in requirement merely because of an incomplete record. In *NCTA*, however, the FCC clearly explained that CPI simply cannot be protected without such a restriction, reasoning that it serves to prevent the opportunity for disclosure of private information to multiple third-party entities without the customer’s knowledge or consent.⁸⁰ It is therefore feasible to make a robust argument that an opt-in framework directly and materially advances the state’s interest in protecting customer privacy for purposes of the commercial speech test.

Finally, the government must show that its restriction on commercial speech is narrowly tailored to serve the state’s interest.⁸¹ To satisfy this test, the government need not adopt the “least restrictive” or “best conceivable option”;⁸² it must, however, show that the restriction is proportionate to the interest in requiring it.⁸³ Again, the Tenth Circuit in *U.S. West* could not conclude that the opt-in requirement was narrowly tailored because the appellate record lacked any consideration of potentially less-restrictive alternatives, such as an opt-out framework.⁸⁴ In *NCTA*, the Commission showed that it considered the benefits an opt-in framework as opposed to an opt-out framework. The FCC provided evidence that customers generally preferred to opt-in before their CPI would be shared with non-affiliated entities, and further that customer information would be subject to greater privacy concern if it were obtained by those entities not subject to the confidential-

⁸⁰*Nat’l Cable & Telecomms. Ass’n v FCC*, 555 F.3d at 1001.

⁸¹*Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n*, 447 U.S. at 566.

⁸²*Nat’l Cable & Telecomms. Ass’n v FCC*, 555 F.3d at 1002.

⁸³*Id.* at 1002 citing *suny* at 480.

⁸⁴*U.S.W., Inc. v FCC*, 182 F.3d at 1238–39.

ity requirements of §222, a result which the 2007 Order sought to combat.⁸⁵ By explicitly demonstrating the benefits of an opt-in requirement as compared to possible alternatives, an opt-in framework will likely meet the final prong of the *Central Hudson* commercial speech test.

III. Conclusion

For the foregoing reasons, the Commission should move forward with all due speed to protect broadband consumers' privacy.

Respectfully submitted,

Dated: May 27, 2016

/s/ Meredith F. Rose
Meredith F. Rose, Harold Feld, Dallas
Harris, and Mojdeh Bowers⁸⁶
Public Knowledge
1818 N Street NW, Suite 410
Washington, DC 20036

May 27, 2016

⁸⁵*Nat'l Cable & Telecomms. Ass'n v FCC*, 555 F.3d at 1002.

⁸⁶Special thanks to Tennyson Holloway, former Mozilla Fellow at Public Knowledge, for his research and technical expertise.