

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

---

In the Matter of )

Protecting the Privacy of Customers of )  
Broadband and Other Telecommunications )  
Services )

---

WC Docket No. 16-106

**REPLY COMMENTS OF AT&T SERVICES INC.**

James J.R. Talbot  
Gary L. Phillips  
David L. Lawson  
AT&T SERVICES INC.  
1120 20th Street, N.W.  
Washington, D.C. 20036  
(202) 457-3058

Jonathan E. Nuechterlein  
Alan Charles Raul  
C. Frederick Beckner III  
Clayton G. Northouse  
SIDLEY AUSTIN LLP  
1501 K Street, N.W.  
Washington, D.C. 20005  
(202) 736-8000

July 6, 2016

**TABLE OF CONTENTS**

EXECUTIVE SUMMARY ..... 1

ARGUMENT ..... 7

I. The Proposed Use Restrictions Are Unreasonable And Unlawful ..... 8

    A. The Proposed Opt-In Requirements Would Suppress Broadband Investment and Adoption, Confuse Consumers, and Impede Competition..... 9

    B. The Proposed Opt-In Requirements Would Not Benefit Consumers ..... 16

        1. No Matter What Rules the Commission Adopts, Non-ISP Actors Will Continue to Use All of the Same Personally Identifiable Information the Commission Would Restrict ISPs from Using ..... 16

        2. ISPs Have No Unique Ability to Synthesize Information or Create Individual Profiles..... 20

        3. Asymmetric Regulation Would Defy Consumer Expectations ..... 23

        4. Competition and Switching Costs Cannot Justify Asymmetric Regulation ..... 25

        5. Concerns About Distinguishing Between Sensitive and Nonsensitive Data Cannot Justify Asymmetric Regulation ..... 27

    C. The Proposed Opt-In Requirements Would Be Unlawful ..... 30

II. The Commission Should Not Restrict Information-Sharing Among ISP Affiliates Or Between ISPs And Their Third-Party Agents..... 34

III. The Commission Should Revise Its Proposed Rules Addressing Use And Sharing Of De-Identified Data ..... 36

IV. The Commission Should Revise Its Proposed Data Security and Breach Notification Rules ..... 40

V. The Proposed Data Correction And Retention Proposals Are Unwise And Unnecessary And Would Impose Enormous Costs ..... 49

VI. The Proposed Ban On Arbitration Clauses Is Unlawful..... 52

CONCLUSION..... 55

## EXECUTIVE SUMMARY

Any rules the Commission adopts here should align with the flexible and highly effective privacy regime the Federal Trade Commission has developed over the past two decades. The FTC's regime reflects what the Notice of Proposed Rulemaking neglects: a *cost-benefit analysis*, designed to protect consumers from genuine identified harms while permitting the productive uses of consumer data that fuel the explosive growth of the Internet ecosystem. And under applicable law, this Commission is not only permitted, but required to conduct such an analysis before imposing any rules in this area.<sup>1</sup>

The opening comments fall into two categories: those that do, and those that do not, recognize the need for a cost-benefit analysis in deciding when to limit the productive uses of data. The commenters in the first category overwhelmingly support alignment with the FTC's approach. These include former FTC Chairman Jon Leibowitz, former FTC Commissioner (and now Professor) Joshua Wright, and former Clinton and Obama privacy advisor Peter Swire. They include organizations devoted to closing the digital divide, including (among many others) the National Black Caucus, the NAACP, LULAC, and MMTCC. They include the Chamber of Commerce, representing businesses across the American economy. And they include companies and groups from every corner of the fixed-line and mobile broadband industry.

Perhaps the most significant comments in this proceeding, however, are those filed by the professional staff of the FTC itself with the unanimous approval of the FTC's commissioners. The FTC's comments confirm that many of the NPRM's proposals reflect basic misconceptions of online privacy issues and would subject consumers to confusing and conflicting privacy regimes. As the FTC notes (at 8), "the FCC's proposed rules, if implemented, would impose a

---

<sup>1</sup> See AT&T Comments at 88-91; see also Section I.C, *infra* (refuting Public Knowledge's suggestion that Section 222 precludes harmonization of FCC and FTC regimes).

number of specific requirements on the provision of [ISP] services that would not generally apply to other services that collect and use significant amounts of consumer data.” The FTC concludes, with considerable understatement, that “[t]his outcome is not optimal.” *Id.*

***Use restrictions.*** As a case in point, the proposed rules would subject ISPs to unjustifiable and burdensome opt-in consent requirements for the use of customer information for any “non-communications-related” first-party and all third-party marketing, even for (1) nonsensitive information (such as mere names and addresses) that (2) the ISP does not share with third-party advertisers. As the FTC observes (at 22-23), “this approach does not reflect the different expectations and concerns that consumers have for sensitive and non-sensitive data. As a result, it could hamper beneficial uses of data that consumers may prefer . . . . Therefore, FTC staff recommends that the FCC consider the FTC’s longstanding approach, which calls for the level of choice to be tied to the sensitivity of data[.]” The FTC has further emphasized that the type of consent mechanism should vary with whether information is shared with third parties. Third-party advertising does not generally, or even typically, involve sharing individually identifiable information with third-party advertisers. Yet the proposed rules here would require opt-in consent for all third-party advertising, again contradicting the FTC’s position and foreclosing productive uses of consumer data.

The commenters supporting the proposed opt-in requirement also ignore its most fundamental cost. Any opt-in requirement is not, as those commenters suggest, simply a more consumer-friendly version of opt-out. Instead, it assumes by default that consumers do not want their information used for marketing purposes. That assumption forecloses productive uses of data because, when consumers fail to opt in, they often do so not by considered choice, but because they do not wish to take the time needed to make a choice and do not fully internalize

the social costs of their non-choice.<sup>2</sup> As the Technology Policy Institute explains, requiring an overbroad opt-in mechanism here would exert upward pressure on broadband prices and downward pressure on broadband adoption by “ensur[ing] that [ISPs] continue to cover all their costs from direct payment by end users.”<sup>3</sup>

The NPRM’s supporters recite familiar but empty rationales for subjecting ISPs to unprecedented information burdens imposed on no one else in the Internet ecosystem. They have long based their arguments for ISP-specific burdens on the premise that ISPs have unique visibility into the details of consumers’ online activity, and thus they quibble with Professor Swire’s exhaustive analysis showing that this premise is now false, given, among other developments, the increasing prevalence of encryption and WiFi-enabled smartphones.

These quibbles are technically misconceived, as Professor Swire explains in a supplemental analysis. More important, they are irrelevant. No one seriously disputes that ISPs have rapidly declining visibility into the details of their users’ online activities; that non-ISP platform providers such as Google and Facebook already have at least as much visibility as ISPs, if not more; and that data brokers and ad networks systematically track consumers and collect data across devices and websites in ways that ISPs cannot. Indeed, even some of the NPRM’s most ardent supporters concede, as EPIC does (at 16), that “the more substantial privacy threats for consumers are not the ISPs.” Sector-specific regulation may have made sense in the pre-

---

<sup>2</sup> No analogous market failure can arise under an opt-out regime because the small minority of consumers who “care greatly about” uses of their nonsensitive data will “invest the time to read, understand, and make an informed decision regarding the privacy policies with which they are presented. An opt-out regime places the burden on this set of consumers who, by revealed preference, value their privacy enough to expend resources to monitor it.” Joshua D. Wright, *An Economic Analysis of the FCC’s Proposed Regulation of Broadband Privacy*, at 17 (May 27, 2016) (submitted by United States Telecom Association (“USTelecom”)) (“Wright White Paper”).

<sup>3</sup> Thomas Lenard & Scott Wallsten, *An Economic Analysis of the FCC’s Privacy Notice of Proposed Rulemaking* at 3 (May 25, 2016) (filed by the Tech. Policy Inst.) (“Lenard & Wallsten White Paper”).

broadband telephone era, when telecommunications carriers alone had access to CPNI and were all subject to the same regulation under Section 222. But it makes no sense today to saddle ISPs alone with unprecedented burdens on the use of nonsensitive customer information that is broadly accessible to the rest of the Internet ecosystem, subject to the FTC's much more flexible and balanced regime. Such asymmetric regulation would achieve no privacy benefit and would simply confuse consumers about who is subject to which rules.

A few commenters would reject the sensitivity-based approach recommended by the FTC staff on the ground that it requires drawing lines between sensitive and non-sensitive information, even though the FTC and self-regulatory organizations have drawn such lines for decades. These commenters would then impose a categorical opt-in obligation for ISPs—assigning, in effect, an infinite value even to negligible or non-existent privacy interests and zero value to the productive uses of data. That argument is untenable as both a policy and a legal matter and, taken to its logical conclusion, would undermine the economic foundation of the modern Internet, which rests on broad use of nonsensitive customer information. There is similarly no merit to Public Knowledge's argument (at 24) that basing consent requirements on the sensitivity of data would “necessaril[ly] requir[e] manual inspection of each packet” to “determine whether sensitive information is present in any given communication.” First, that concern can logically apply only to uses of communications *content*, which constitutes a tiny subset of the information the proposed rules would restrict ISPs from using. Second, this “inspection” concern misunderstands how information is used for targeted advertising and, if applied broadly, would wipe out the business models underlying countless ad-based services.

The proposed marketing restrictions would also be as unlawful as they are misguided. As Professor Laurence Tribe explains, the First Amendment forbids the government to discriminate

against particular commercial speakers by imposing opt-in consent requirements on them alone when other commercial speakers will continue to make extensive use of the same information those requirements are designed to keep “private.”<sup>4</sup> The NPRM’s supporters argue that the D.C. Circuit’s 2009 decision in *NCTA*<sup>5</sup> would shield the proposed opt-in requirements from First Amendment challenge. But *NCTA* is doubly inapposite—it involved no underbreadth problem and, just as important, concerned the *disclosure* of individually identifiable information, rather than, as here, the mere *use* of information already within a party’s possession.

***Restrictions on sharing with affiliates and third-party agents.*** The Commission should reject suggestions that it should impose opt-in requirements for any transfer of personal information between ISP affiliates. No consumer attributes significance to such corporate formalism and the FCC’s rules should reflect that reality. Relatedly, the Commission should confirm that no opt-in mechanism is necessary when ISPs share data with third-party *agents* that are subject to the ISPs’ supervision, where the ISPs are liable for their acts.

***De-identified data.*** The comments reflect a broad consensus that use of properly de-identified data—collective and non-collective—can greatly enhance consumer welfare. There is also broad support for allowing ISPs to use and share non-collective de-identified data (in addition to aggregate data) under the same framework that the FTC applies to the rest of the Internet ecosystem. Although some commenters contend that the Commission should impose opt-in/opt-out consent requirements for the use and sharing of such data, that proposal collides with the plain language of Section 222(c)(1) and (c)(3), which requires customer approval only for “individually identifiable customer proprietary network information.” De-identified

---

<sup>4</sup> See Laurence Tribe and Jonathan Massey, *The Federal Communications Commission’s Proposed Broadband Privacy Rules Would Violate the First Amendment* (May 27, 2016) (attached to letter of the same date from CTIA, NCTA, and USTelecom) (“Tribe & Massey White Paper”).

<sup>5</sup> *NCTA v. FCC*, 555 F.3d 996 (D.C. Cir. 2009).

information is, by definition, not “individually identifiable” CPNI. Burdening truthful speech that reveals no personally identifiable information would also violate the First Amendment. Although it may be theoretically possible to re-identify some de-identified data sets, appropriate statistical techniques can reasonably address any re-identification concerns.

***Data security.*** Many commenters agree with AT&T that key aspects of the proposed data security rules would be both unlawful and unwise. They would be unlawful because no statutory provision authorizes the Commission to establish the comprehensive data-security regime it proposes here. And as the FTC and others explain, such rules would make for poor public policy by imposing enormous burdens with little or no benefit. Most fundamentally, the Commission’s proposed rules governing data security, retention, and breaches are vastly overbroad because they would apply even to information that is not sensitive and, in many cases, is generally available to other Internet companies. At a minimum, the Commission should align its rules more closely with the FTC’s regime and state law.

***Arbitration clauses.*** Finally, the NPRM’s proposal to ban arbitration clauses would violate the FAA, as several commenters explain in detail. No provision of the Communications Act even addresses arbitration clauses, much less supplies the clear “congressional command” needed to override the FAA’s federal policy favoring arbitration. Contrary to the comments of a trial lawyer association, this congressional silence requires the enforcement of existing arbitration clauses and precludes the Commission from prohibiting such clauses in new contracts.

## ARGUMENT

As discussed in our opening comments (at 30-33), the federal government has long enforced a flexible but highly effective regime for online privacy and data security. That regime is sensitive to both the costs and the benefits of market intervention, ensures technological neutrality between similarly situated providers, and relies extensively on industry self-governance and, as a backstop, on the FTC's enforcement of consumer protection prohibitions against unfair or deceptive business practices. The Obama White House has explicitly endorsed that regime, warned against "treat[ing] similar technologies within the communications sector differently," and championed reliance on "multistakeholder process[es] to produce enforceable codes of conduct" that industry can voluntarily incorporate into privacy policies.<sup>6</sup> As the White House explains, multistakeholder processes are superior to top-down regulation by any "centralized authority" because they "provide the flexibility, speed, and decentralization necessary to address Internet policy challenges."<sup>7</sup> And just last month, the Department of

---

<sup>6</sup> The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 2, 39 (Feb. 2012), <https://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

<sup>7</sup> *Id.* at 23-24. As several commenters observe, "successful implementation and administration of industry self-regulatory standards for the collection and use of data demonstrates that self-regulation is the appropriate approach to addressing complex data policy issues. Rigid government regulations, unable to adapt to the rapidly changing technological landscape, would disrupt the Internet ecosystem by chilling investment in consumer-friendly products and services." Digital Advertising Alliance ("DAA") Comments at 1; *see also* Direct Marketing Association ("DMA") Comments at 4 ("Voluntary industry self-regulation is and should remain the primary tool to honor consumer preferences . . ."); *id.* at 9-11 (describing process for refining and enforcing DMA's *Guidelines for Ethical Business Practice*); Association of National Advertisers Comments at 5 ("Broad, effective self-regulation, buttressed by Federal Trade Commission (FTC) and state enforcement, provides strong protections to consumers and appropriate business interests. The existing sound regulatory structure should not be replaced with the NPRM's hastily developed and ill-considered proposed rules.").

Commerce reaffirmed the Administration’s position that a flexible, context-based privacy regime is the best means of promoting consumer welfare.<sup>8</sup>

Nothing has changed to warrant a radical departure from that regime, let alone one that is heavily biased against ISPs. As Georgetown University’s S<sup>2</sup>ERC observes, “edge providers have a long history of breaches of consumer trust while [ISPs] have only rarely violated this trust.”<sup>9</sup> It would be highly perverse to create, as the NPRM proposes, a new set of sector-specific regulatory burdens that target only the industry sector with the *best* privacy track record. More generally, the NPRM displays a marked inattention to the negligible benefits and considerable costs of subjecting ISPs to these unprecedented new burdens. For those reasons and the others discussed below, the proposed rules—to the extent they depart from the more flexible policies applicable everywhere else in the online ecosystem—are both irrational and unlawful.

#### **I. THE PROPOSED USE RESTRICTIONS ARE UNREASONABLE AND UNLAWFUL**

As our opening comments explained, any rules the Commission adopts should preserve technological neutrality between ISPs and the rest of the Internet ecosystem and should narrowly target only those data practices that threaten actual consumer harm. That consumer-welfare-based regime should focus, as the FTC’s does, on two key variables: whether the information at issue is (1) sensitive or (2) shared with third parties. FTC staff and many other commenters support that approach. But several commenters continue to advocate categorical opt-in requirements that would restrict ISPs from merely using (without sharing) nonsensitive customer-specific data already in their possession. There is no support in policy or law for

---

<sup>8</sup> See, e.g., U.S. Department of Commerce, *Enabling Growth and Innovation in the Digital Economy* (June 2016), [https://www.ntia.doc.gov/files/ntia/publications/enabling\\_growth\\_innovation\\_in\\_the\\_de.pdf](https://www.ntia.doc.gov/files/ntia/publications/enabling_growth_innovation_in_the_de.pdf).

<sup>9</sup> Security and Software Engineering Research Center at Georgetown University Comments at 3-4; see also Electronic Privacy Information Center (“EPIC”) Comments at 16 (“it is obvious that the more substantial privacy threats for consumers are not the ISPs”).

subjecting ISPs to burdensome opt-in requirements that do not apply to the rest of the Internet ecosystem.

**A. The Proposed Opt-In Requirements Would Suppress Broadband Investment and Adoption, Confuse Consumers, and Impede Competition**

Until now, all online companies have been free to use nonsensitive customer-specific information to engage in first-party marketing without any consent mechanism, even opt-out.<sup>10</sup> All online companies have enjoyed similar flexibility to use such information for third-party marketing as well, particularly if they do not share that information with the third parties on whose behalf they send targeted ads.<sup>11</sup> But the proposed rules would subject ISPs to the most restrictive notice-and-consent mechanism—opt-in—before using customer-specific information for most first-party marketing and all third-party marketing. And they would rigidly impose that mechanism even if the information is as nonsensitive as mere customer names and addresses, and even if the ISP does not share that nonsensitive information with any third parties. For example, under a literal reading of the proposed rules, AT&T could not even use its own ISP customer list to email most types of ads to its subscriber base absent opt-in consent.<sup>12</sup>

As the FTC observes, this proposed consent regime “does not reflect the different expectations and concerns that consumers have for sensitive and non-sensitive data. As a result, it could hamper beneficial uses of data that consumers may prefer . . . . Therefore, FTC staff recommends that the FCC consider the FTC’s longstanding approach, which *calls for the level of*

---

<sup>10</sup> See AT&T Comments at 36-37.

<sup>11</sup> *Id.*

<sup>12</sup> See *NPRM* at p. 103 (defining “customer proprietary information” to include any “[p]ersonally identifiable information,” including “any information that is linked or linkable to an individual”); *id.* at 105 (requiring opt-in consent merely “to use . . . customer PI” for any marketing, except in connection with first-party “communications-related services”). It is unclear whether the Commission intended for its proposed rules to have this radically overbroad and deeply counterintuitive consequence.

*choice to be tied to the sensitivity of data[.]*<sup>13</sup> Similarly, by inflexibly requiring opt-in consent for most first-party and all third-party advertising, the proposed rules ignore the FTC’s longstanding position that any need for notice-and-choice requirements depends in part on whether information is *shared* with third parties.<sup>14</sup> Like the NPRM, several commenters seem to assume that third-party marketing typically involves sharing with third-party advertisers.<sup>15</sup> It does not. Like many other online actors, an ISP can use customer information to convey ads on behalf of third-party advertisers without disclosing any individually identifiable information to the advertisers. In the process, it does not trigger any of the heightened privacy concerns that arise from disclosure of such information to third parties.<sup>16</sup>

The FTC also casts doubt on the NPRM’s proposed distinction between first-party “marketing of communications-related services ... and other first-party uses,” observing that the distinction “does not reflect [consumer] expectations.”<sup>17</sup> As explained in our opening comments (at 40-42) that distinction is indeed an unsupportable anachronism and cannot sensibly be extended from the legacy telephony context to today’s online ecosystem. Although several parties urge the Commission to apply that outdated distinction here, they cite no discernible reason for doing so. For example, CDT simply asserts (at 22) that an ISP’s customers would not “expect their provider to use their customer PI”—presumably including their mere names and addresses—“to offer them a smart refrigerator.” But CDT offers no support for that puzzling assertion. In fact, typical consumers would certainly be no more surprised, let alone

---

<sup>13</sup> FTC Comments at 22-23 (emphasis added).

<sup>14</sup> See FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, at 15-16 (Mar. 2012) (“2012 FTC Privacy Report”).

<sup>15</sup> E.g., Center for Democracy and Technology (“CDT”) Comments at 21, 23.

<sup>16</sup> See AT&T Comments at 43-44; see also Section II, *infra* (ISPs should be permitted to share information with agents).

<sup>17</sup> FTC Comments at 22.

disconcerted, to receive connected-device offers from their ISPs than they are to see shoe ads appear on non-shoe-related webpages after they search for shoes online—a ubiquitous phenomenon in today’s online ecosystem. CDT also identifies no policy basis for saddling ISPs with onerous opt-in requirements before they can offer connected devices and other socially valuable products to consumers. And the First Amendment precludes the Commission from restricting commercial speech on the basis of empirically ungrounded speculation about what might “surprise” or “bother” consumers.

In the teeth of the FTC’s expert judgment about consumer expectations, some commenters nonetheless suggest that opt-in is simply a more consumer-friendly version of opt-out and that if ISPs are willing to use the latter (as AT&T has always been), they should also be willing to use the former whether the information in question is sensitive or not.<sup>18</sup> That argument overlooks a critical point that the FTC has long understood and built into its notice-and-consent regime: overbroad opt-in requirements impose substantial costs, interfere with socially useful economic activity, and harm the very consumers they are intended to help.

As we have explained, most consumers take the path of least resistance when they are presented with an opt-in notice without an express and immediate inducement to click “yes,” such as a lower subscription fee.<sup>19</sup> These consumers will decline to opt in *not* because they object to the data uses in question, but because clicking “no” avoids the transaction costs of reading and digesting a privacy notice and gets them on their way as quickly as possible.<sup>20</sup> Such consumers do not internalize the costs of that non-decision for the Internet ecosystem, which

---

<sup>18</sup> See, e.g., CDT Comments at 24-25.

<sup>19</sup> See AT&T Comments at 52-53.

<sup>20</sup> See *id.*; Wright White Paper at 13-20; Howard Beales Comments at 10-11; Eric Johnson & Daniel Goldstein, *Do Defaults Save Lives?*, 302 Science 1338 (2003).

offers so many low-price or free services precisely because most online companies can broadly use customer information to provide targeted advertising.<sup>21</sup> As Google explains, “[a]ds are what enable us to make our services like Search, Gmail, and Maps available for free for everyone.”<sup>22</sup>

If opt-in became a widespread requirement, applicable even to nonsensitive data, it would scuttle the economic premise of the modern Internet and convert (for example) today’s “free” search engines and social-networking sites into smaller, less efficient, subscription-based enterprises. Any *individual* consumer confronted with an opt-in choice could skip reading the applicable privacy policy and decline by default, expecting that he or she could free-ride on the service provider’s use of *other* customers’ information to subsidize low-cost services. The problem is that most of those other customers would have that same preference, click “no,” and jam the engine powering today’s Internet.<sup>23</sup>

Professor Ohm rejects not only the FTC’s comments but the very premise of that agency’s online privacy regime when he argues that overbroad opt-in requirements impose no real costs because, he says, companies can easily persuade consumers to opt in. That argument is wrong, at least in the online marketing context, for the reasons discussed: the incentives of individual consumers are misaligned with the interests of consumers as a whole. Professor Ohm offers no evidence to the contrary. Indeed, even though Professor Ohm styles his submission as

---

<sup>21</sup> See Wright White Paper at 18-20. As noted above, no similar market failure arises from the use of an opt-out regime because consumers with an unusual aversion to marketing-oriented uses of their information can and do avail themselves of opt-out mechanisms. See note 2, *supra*.

<sup>22</sup> Google, *Data enables us to provide our services like Search, Gmail, and Maps*, <https://privacy.google.com/how-we-use-data.html>.

<sup>23</sup> See AT&T Comments at 51-56; Wright White Paper at 25-28; Statement of FTC Commissioner Maureen K. Ohlhausen Regarding Staff Comment at 3 (May 27, 2016) (“If a regulation imposes defaults that do not match consumer preferences, it imposes costs on consumers without improving consumer outcomes. The burdens imposed by a broad opt-in requirement may also have negative effects on innovation and growth.”) (citing Daniel Castro & Alan McQuinn, *The Economic Costs of the European Union’s Cookie Notification Policy* (Nov. 2014)).

a set of “reply comments,” he does not in fact reply to the substantial record evidence showing that overbroad opt-in requirements impose substantial costs. For example, he does not even cite former FTC Commissioner Joshua Wright’s extensive analysis of that issue.<sup>24</sup> Nor does Professor Ohm address empirical research addressing opt-in in the relevant context: online marketing. Instead, he relies on research involving entirely different factual settings, such as employee 401(k) elections, which involve none of the same externalities or transaction-cost dynamics.<sup>25</sup> In short, all of the record evidence about the effect of opt-in rules in the online marketing context confirms that the FTC has been right all along in concluding that opt-in rules for online marketing impose substantial costs because they “hamper beneficial uses of data”<sup>26</sup> and should thus be limited to narrowly defined contexts, such as the use of sensitive consumer data.

The same economic concerns that militate against overbroad opt-in requirements for the Internet ecosystem in general militate against such requirements for ISPs in particular. Although ISPs today rely largely on broadband subscription fees to recover network costs, they do not rely on them exclusively, and the size of those fees will depend in part on the regulatory choices the Commission makes in this proceeding. Given any level of competition, the market price for broadband service depends in part on what collateral revenues an ISP can earn by serving each customer. These can take the form of revenues for additional services offered by the ISP (or its corporate affiliates) or revenues the ISP obtains from using customer-specific information to target ads on behalf of third-party advertisers (again, without disclosing that information to the

---

<sup>24</sup> Wright White Paper at 13-20.

<sup>25</sup> Ohm Reply Comments at 8-9.

<sup>26</sup> FTC Comments at 22-23.

third-party advertisers themselves).<sup>27</sup> Any consent requirement that hamstring an ISP's efforts to pursue either category of collateral revenues will impose upward pressure on the subscription fees for the broadband service itself, just as limits on newspaper advertising would impose upward pressure on newspaper subscription rates.<sup>28</sup> In short, if the Commission adopts its plan to impose opt-in requirements on most first-party and all third-party advertising, it will raise consumer prices to the detriment of the Commission's most central mission: the promotion of widespread, affordable broadband access.<sup>29</sup>

Any broad opt-in requirement would also inflict a variety of additional harms on the Internet ecosystem, as described in more detail in our opening comments (at 55-58). Because that requirement would break sharply with the FTC regime applicable to the rest of the Internet, it would confuse consumers about who may use their data and on what terms. It would likewise require ISPs to increase the complexity of their privacy notices by distinguishing between the information they collect in their capacity as ISPs and the information they collect in their capacity as edge providers (*e.g.*, by means of mobile apps). Here, too, the victims would be consumers. Most of them would not understand the fine distinctions, rooted in jurisdictional happenstance, between the online entities subject to the FTC's flexible regime and those subject to this Commission's regulatory straitjacket. The Commission can avoid that confusion only by aligning its marketing rules with the FTC's regime.

---

<sup>27</sup> See AT&T Comments at 53-55; Wright White Paper at 20-22.

<sup>28</sup> See Wright White Paper at 20-22; Lenard & Wallsten White Paper at 3 (May 25, 2016) (opt-in requirement would "ensure that [ISPs] continue to cover all their costs from direct payment by end users").

<sup>29</sup> As noted in our opening comments (at 54 n.120), the Commission would compound those costs if, as the NPRM contemplates (at ¶ 142), it requires ISPs to obtain customer consent *each time* they collect customer information or put it to new uses. The FTC thus urges a sensible "alternative to the FCC's proposed approach": obtaining consent "when the consumer signs up for service, because this the time when the consumer will likely be considering material terms." FTC Comments at 24-25.

The proposed marketing restrictions would also harm consumers by suppressing competition. As the Technology Policy Institute explains, “[t]reating ISPs differently from edge companies would put ISPs at a competitive disadvantage in the large and growing digital advertising market, which had revenues of approximately \$60 billion in 2015.”<sup>30</sup> Subjecting ISPs to that disadvantage would be particularly egregious because they are *new entrants* in a highly concentrated market. Against that backdrop, it is risible for Public Knowledge to argue (at 3) that this regulatory entry barrier is necessary to keep ISPs from gaining an unfair “competitive advantage” against market incumbents Google and Facebook, which alone account for more than 60 percent of all online advertising revenues.<sup>31</sup>

Finally, the Commission would sabotage its central mission to promote affordable broadband if it bans ISPs from seeking, and consumers from giving, even opt-in consent to the use of their data in exchange for discounted services.<sup>32</sup> Few, if any, commenters oppose such discounts outright, and any opposition is conflicted and sometimes incoherent. For example, Public Knowledge professes (at 32) in one passage to be “deeply concerned about” such discounts but elsewhere insists (at 27) that “[i]f [a] consumer wants to sell or trade away her

---

<sup>30</sup> Lenard & Wallsten White Paper at 3.

<sup>31</sup> See Russell Brandom, *Google and Facebook still dominate tracking on the web*, The Verge (May 16, 2016), <http://www.theverge.com/2016/5/18/11692228/google-facebook-web-tracking-survey-advertising>; Mary Meeker, *Internet Trends Report 2016* (“Google + Facebook = 76% (& Rising) Share of Internet Advertising Growth, USA”), [http://www.slideshare.net/kleinerperkins/2016-internet-trends-report/44-KPCB\\_INTERNET\\_TRENDS\\_2016\\_PAGE](http://www.slideshare.net/kleinerperkins/2016-internet-trends-report/44-KPCB_INTERNET_TRENDS_2016_PAGE). For similar reasons, it makes no sense to argue, as Public Knowledge does (at 34), that Section 222(b) should be “updated” to support Public Knowledge’s anticompetitive agenda. Section 222(b) was enacted in 1996 to keep local telephone carriers—then undisputed monopolists—from using information proprietary to long-distance carriers to compete against those same carriers. Applying that provision to exclude ISPs from the digital advertising market would turn the pro-competitive purpose of that provision on its head. The provision is also facially inapplicable here. First, as the NPRM concedes (at ¶ 271), the Commission has always (properly) construed this provision to “apply[] specifically to *carriers*’ proprietary information,” and it thus has no bearing on this proceeding, which addresses consumer privacy concerns. Moreover, Section 222(b) applies by its terms only to information received “from another carrier,” whereas this proceeding concerns information received from end users and non-carrier online companies.

<sup>32</sup> See *NPRM* ¶ 259.

information in a value exchange for targeted goods and services, she should have that right.” Public Knowledge is right in the second passage and wrong to be “deeply concerned” in the first. Such discounts enable consumers to share directly in the value created by the use of their information—the same value proposition that underlies the explosive proliferation of free and low-cost services on the Internet today. The Commission would inflict much consumer harm with no countervailing benefits if it prohibited such value exchanges in connection with broadband services. And such a prohibition would be particularly indefensible if the ISP in question lacks market power, as AT&T does in the areas where it offers such discounts in connection with its Gigapower services.<sup>33</sup>

## **B. The Proposed Opt-In Requirements Would Not Benefit Consumers**

Because the proposed marketing restrictions would cause the harms discussed above, the Commission would bear a heavy burden if it sought to justify those restrictions anyway on the ground that their benefits outweighed their costs.<sup>34</sup> In fact, to the extent those restrictions would impose regulatory burdens beyond those applicable to the rest of the Internet ecosystem, they would create no consumer benefits and, in particular, would do nothing to promote any genuine “privacy” interest.

### ***1. No Matter What Rules the Commission Adopts, Non-ISP Actors Will Continue to Use All of the Same Personally Identifiable Information the Commission Would Restrict ISPs from Using***

Some supporters of ISP-specific marketing restrictions assert that ISPs present a unique threat to consumer privacy on the theory that they can see more about each Internet user than the rest of the ecosystem can, despite the increasing prevalence of encryption and multiple ISP

---

<sup>33</sup> See AT&T Comments at 58-61.

<sup>34</sup> See *id.* at 88-91 (explaining that the Commission must conduct a cost-benefit analysis and to justify any rules and that this is not one of the rare contexts in which Congress has foreclosed the use of such an analysis by enacting rigid statutory imperatives).

connections per user.<sup>35</sup> That is incorrect. As we and many other commenters have explained, ISPs have access to little consumer-specific information that is not already known to and used by the rest of the broadband ecosystem, including ad networks like DoubleClick, social media platforms like Facebook, mobile operating systems like Android, and browsers like Chrome.<sup>36</sup> No matter what rules the Commission adopts here, the rest of that ecosystem will still be subject, in the FTC’s words, to “the FTC’s longstanding approach, which calls for the level of choice to be tied to the *sensitivity* of data[.]”<sup>37</sup> For the vast majority of information that is *not* sensitive, the Commission would succeed only in hamstringing ISPs’ ability to put that information to productive use, but would not keep the data from being used by everyone else.

These points are set forth in the rigorous and highly publicized analysis coauthored by renowned privacy expert Peter Swire earlier this year—a white paper that the NPRM does not cite, even though it refutes the technological assumptions underlying the proposed rules.<sup>38</sup> As Professor Swire explains, a clear and rapidly growing majority of web traffic is encrypted, which means that ISPs can “see” less than large platform edge providers such as Google and Facebook about any given user’s online activities. And as consumers rely increasingly on WiFi-enabled mobile devices for Internet connectivity, they use multiple ISPs in the course of a day, and they

---

<sup>35</sup> See, e.g., Public Knowledge Comments at 9-17; Upturn Comments at 3-6.

<sup>36</sup> See AT&T Comments at 9-30; Verizon Comments at 17-24; Comcast Comments at 26-34. As in our opening comments, references to the practices of particular edge providers are not intended as criticisms of those practices, many of which have generated substantial consumer value.

<sup>37</sup> FTC Comments at 23 (emphasis added).

<sup>38</sup> See Peter Swire et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* (Geo. Tech. Inst. for Infor. Sec. & Privacy, May 2016) (“Swire Report”). Numerous other technical experts support Swire’s analysis and explain how web browsing data is collected and used by many companies other than ISPs. See Richard Bennett Comments at 3-4; Arvind Narayanan Comments at 2; William Lehr Comments at 5; Eric Burger Comments at 3-4.

“go dark” to each ISP they are not using at any given moment, even though they remain continuously visible to their operating systems, browsers, and mobile apps.<sup>39</sup>

Although the NRPM’s supporters quibble with some aspects of Professor Swire’s analysis, they can identify no actual inaccuracies in that analysis. They also cannot deny that companies such as Google and Facebook have at least as much visibility as ISPs (and more) into the online activities of individual users.<sup>40</sup> Indeed, EPIC forthrightly embraces that point:

The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. *This description is inconsistent with the reality of the online communications ecosystem.* Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. However, all pathways lead to essentially one Internet search company and one social network company. Privacy rules for ISPs are important and necessary, but it is obvious that *the more substantial privacy threats for consumers are not the ISPs.*<sup>41</sup>

---

<sup>39</sup> AT&T Comments at 26-27. Public Knowledge (at 14-15) quotes a press interview with an AT&T executive for the proposition that AT&T’s AdWorks division uses “data [it] ha[s] that nobody else has access to.” Public Knowledge Comments at 14-15 (quoting eMarketer interview). The ISP data in that category, however, are simply details of a customer’s commercial relationship with AT&T: “how large a data plan they have, and when their contract expires.” *See id.* Of course, ISPs are hardly unique in having proprietary information about their own customer relationships. Public Knowledge also notes that AdWorks makes use of information categories that are widely available to edge providers, such as geolocation data. *Id.* But AdWorks shares such information with third-party advertisers only in de-identified form.

<sup>40</sup> Professor Swire’s critics try in vain to identify nontrivial examples of customer data that ISPs can see but non-ISPs cannot. For example, Public Knowledge devotes much space (at 13-14) to a hypothetical customer’s use of her fixed-line broadband connection to sync a FitBit. FitBit encrypts transmissions between its users and its servers, so the ISP in this hypothetical could at most know that the user was communicating with those servers. And the ISP could not even know that fact whenever—as routinely happens—the user syncs her FitBit with her smartphone (via a mobile network or WiFi hotspot). In contrast, the full content of her FitBit activity is visible not only to FitBit itself, but to Google if she syncs with an Android smartphone. In all of these respects, Public Knowledge has it exactly backwards when it claims (at 13) that “Comcast . . . knows everything that Google knows” and that “Google can never know . . . information” about the user’s FitBit activity once she activates her device. Similarly, Public Knowledge’s discussion of “multi-platform apps and ‘push alert’ systems” (at 17) ignores the basic fact that the content transferred via such apps (such as Gmail, Facebook, or Apple iMessage communications) is typically encrypted and visible only to edge providers, not ISPs.

<sup>41</sup> EPIC Comments at 16 (emphasis added).

Likewise, Georgetown University's S<sup>2</sup>ERC acknowledges that, "[a]t times, edge providers may have a broader and more detailed understanding of consumer information as few consumers rely on only a single [ISP]. Edge providers can collect information across all networks a customer uses."<sup>42</sup>

Moreover, if one looks forward rather than backward in time, encryption is gaining so much traction so quickly that edge providers are rapidly widening the visibility gap between what Internet traffic they see and what ISPs could even theoretically see. In its most recent report, Sandvine "forecasts that 70% of global Internet traffic will be encrypted in 2016, with many networks expected to exceed 80%."<sup>43</sup> And by the end of the year, all iPhone apps will have to use Apple's App Transport Security, which uses HTTPS to encrypt communications between apps and the servers that feed apps information.<sup>44</sup> The Commission should adopt policies designed for the emerging market realities to which they will apply, not for the now-superseded market conditions of the recent past.

A few commenters argue that, even where Internet traffic is encrypted, ISPs can draw certain highly generalized conclusions about a customer's online activities by observing port usage, high-level domain names (but not detailed URLs), and the timing and intensity of Internet traffic.<sup>45</sup> As EPIC's remark suggests, none of that information holds a candle to the type of

---

<sup>42</sup> Security and Software Engineering Research Center at Georgetown University Comments at 3-4.

<sup>43</sup> Sandvine, *2016 Global Internet Phenomena*, at 1 (June 2016), <https://www.sandvine.com/downloads/general/global-internet-phenomena/2016/global-internet-phenomena-report-latin-america-and-north-america.pdf>.

<sup>44</sup> See, e.g., Christian de Looper, *Apple is Mandating HTTPS Connections for iOS Apps by 2017* Yahoo Tech (June 17, 2016), <https://www.yahoo.com/tech/apple-mandating-https-connections-ios-190751421.html>; Swire Reply Comments at 2-5.

<sup>45</sup> E.g., Public Knowledge Comments at 4-6; CDT Comments at 16-17; Upturn Comments at 6-9.

detailed information that edge providers on the other end of encrypted communications can see.<sup>46</sup> For example, port information can be used to determine only whether someone is engaged in certain very general types of Internet activities (such as email or VoIP). And domain-level information can reveal, for example, only that someone visited Google.com but not the search terms used or particular pages viewed. Of course, ISPs can draw *some* inferences from these information sources, but those inferences are not particularly sensitive, especially when compared to the types of highly personalized information visible to edge providers, ad networks, and the providers of operating systems and browsers. And they certainly do not give ISPs a pervasive view of their customers' Internet usage, let alone support the differential, burdensome regulation proposed by the NPRM.

## ***2. ISPs Have No Unique Ability to Synthesize Information or Create Individual Profiles***

Some commenters suggest that, even if the rest of the ecosystem in the aggregate sees what ISPs see and more, each non-ISP entity is individually less capable than any ISP to form a complete view of each user's online activities.<sup>47</sup> Chairman Wheeler's congressional testimony summed up this argument as follows: "I go to WebMD, and WebMD collects information on me. I go to Weather.com and Weather.com collects information on me. I go to Facebook and Facebook collects information on me. But only one entity connects all of that information, that I'm going to all of those different sites, and can turn around and monetize it."<sup>48</sup> This argument is wrong on two separate levels.

---

<sup>46</sup> See, e.g., Swire Report 8-13, 42-122; Swire Reply Comments at 6-9; Future of Privacy Forum ("FPF") Comments at 9-25.

<sup>47</sup> Public Knowledge Comments at 3-4; Feamster, et al. Comments at 2-3.

<sup>48</sup> *Examining the Proposed FCC Privacy Rules*, Hearing Before the S. Comm. on the Judiciary, Subcomm. on Privacy, Tech., and the Law, 114th Cong. (2016) (statement of Chairman Wheeler), <http://www.judiciary.senate.gov/meetings/examining-the-proposed-fcc-privacy-rules>.

First, it focuses on what is seen by individual websites (such as WebMD.com or weather.com) and completely ignores what is seen, collected, and used by large platform providers such as Android, Chrome, and Google Maps. In the FTC’s words, “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.”<sup>49</sup> That basic point, which is undisputed, flatly refutes the suggestion that “only one entity [*i.e.*, an ISP] connects all of that information.” To the contrary, Google and similar platform providers own the best seats in the house. The increasing prevalence of encryption and multiple ISP connections per user limit what ISPs can see, but do *not* limit what these non-ISP platform providers can see. To take just one example, the Android operating system keeps track of a user’s movements (physical and online) throughout the course of a day; it “sees” everything the user sees and more; and everything it sees is at least potentially available for collection and use by Google and countless app developers.<sup>50</sup> And social networks typically require users to sign in before using their services, facilitating the most direct form of cross-device tracking available.

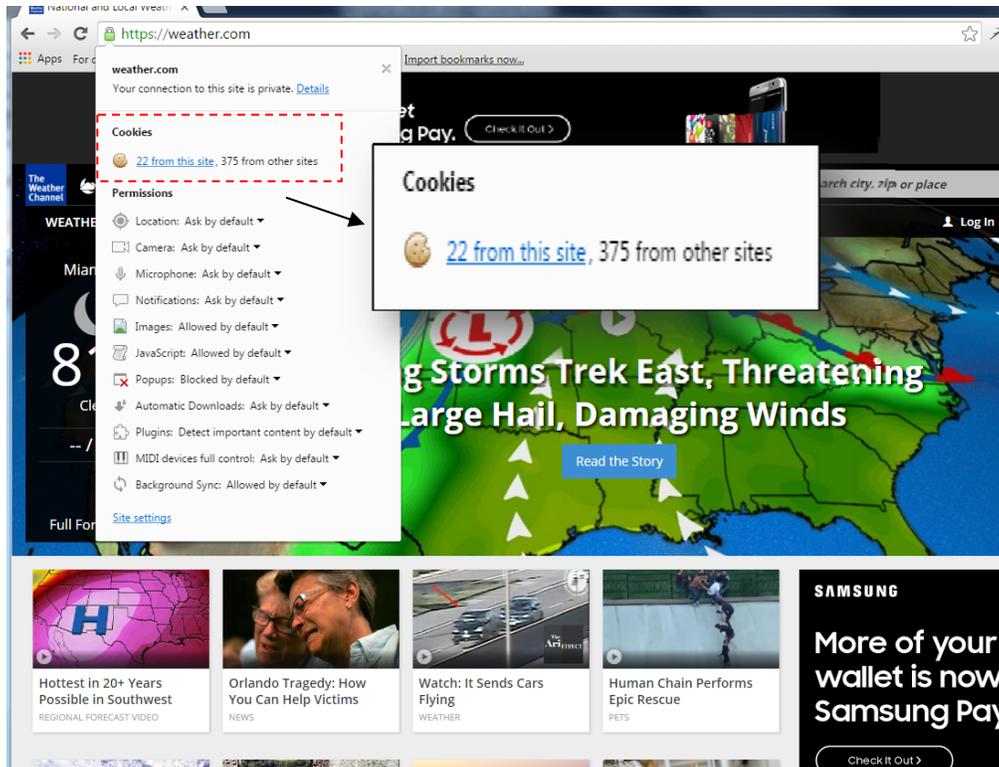
Second, even if it were meaningful to focus only on individual websites rather than operating systems, browsers, and other large non-ISP platform providers, those websites do not exist in isolation; to the contrary, they often work with third parties to pool information about any given end user’s activities.<sup>51</sup> For example, on a simple visit to weather.com, 22 cookies are dropped on a user’s web browser:

---

<sup>49</sup> 2012 *FTC Privacy Report* at 56; *see* FPF Comments at 9 (the quoted passage from Chairman Wheeler’s congressional testimony “reflects a fundamental misunderstanding of the current online ecosystem”).

<sup>50</sup> *See* AT&T Comments at 21-24, 44-49.

<sup>51</sup> *See* FPF Comments at 9-12.



These cookies feed third parties, which are essentially invisible to the user, information about a user's web browsing history and are used to deliver targeted advertisements that appear both on weather.com and on other many websites the user visits. On the other hand, because weather.com uses HTTPS, ISPs have no means of viewing the contents of this webpage.

Further, to serve targeted third-party ads, other parties such as Google and Facebook collect web-browsing information from the millions of third-party webpages that contain social media plugins, such as Google's "Google+" and Facebook's "Like" button.<sup>52</sup> Similarly, many mobile apps continue tracking an individual's location and online activities even after the individual has stopped actively using those apps and they remain running in the background.<sup>53</sup>

<sup>52</sup> See AT&T Comments at 11. In fact, CDT and other commenters filed comments in the FTC's cross-device proceeding discussing the prevalence of probabilistic and deterministic cross-device tracking by edge providers. See, e.g., CDT Comments for November 2015 Workshop on Cross-Device Tracking, at 2-7 (Nov. 16, 2015), [https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00056-99849.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00056-99849.pdf).

<sup>53</sup> See AT&T Comments at 22-23.

More generally, collecting and synthesizing customer-specific information across multiple apps and websites is a core business purpose of many data brokers and ad networks.<sup>54</sup> Data brokers further associate online activity with identifiable people and sell individual profiles to any number of willing buyers.

Although Professor Feamster asserts (without support) that ISPs are uniquely able to associate web activity with actual people,<sup>55</sup> that assertion crashes headlong into the basic market function of data brokers. It also ignores the countless individual web services that make it their business to know the real-life identities of their users. For example, hundreds of millions of consumers who use Facebook, Twitter, Google+, and LinkedIn provide their real names and a variety of other highly specific biographical information, such as birthdates and cities of residence. And some of those providers, such as Facebook and LinkedIn, generally require the use of such information as a condition for using their services.

### 3. *Asymmetric Regulation Would Defy Consumer Expectations*

Echoing a passage in the NPRM, a few supporters of the proposed rules argue that, even if the rest of the ecosystem collects and uses all the same data as ISPs, users somehow exercise greater “choice” when they share the data with the rest of the ecosystem than with ISPs.<sup>56</sup> This claim, too, is factually baseless. For example, most consumers do not affirmatively “choose” to share their information with multiple third-party entities when they visit weather.com (see above) or more than two dozen such entities when they visit WebMD’s website, but that is what

---

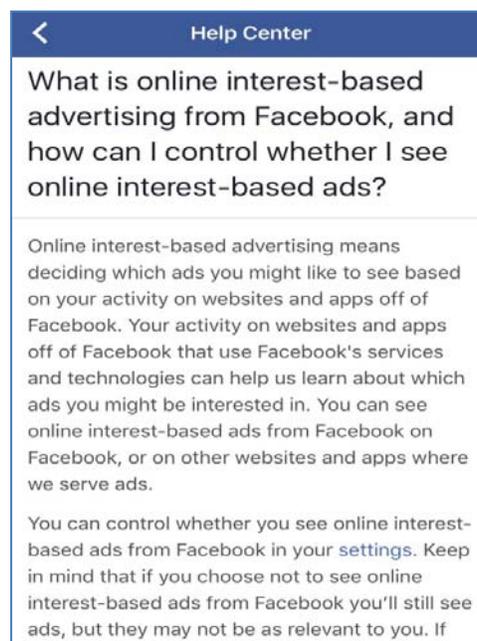
<sup>54</sup> See, e.g., Dan Tynan, *Web trackers are totally out of control*, IT World (Mar. 21, 2013), <http://www.itworld.com/article/2832940/it-management/web-trackers-are-totally-out-of-control.html>.

<sup>55</sup> Feamster, et al. Comments at 2.

<sup>56</sup> E.g., *id.* at 3 (arguing that consumers exercise more “choice” about the uses of their data “when deciding whether to reveal th[eir] information to an edge provider”) (emphasis omitted); see NPRM ¶ 132 (“edge providers only have direct access to information that customers choose to share with them by virtue of engaging their services”).

happens, as the Future of Privacy Forum explains (at 9-10). Nor do consumers affirmatively choose to accommodate those unseen third parties' business practice of "buying and selling the data at third party data exchanges," which "match up consumer behavior across the Internet, creating comprehensive and detailed individual profiles." *Id.* at 10.

Likewise, most consumers do not affirmatively "choose" to have mobile app developers track them even when they are not using those apps, but that, too, is what happens. For example, subject to an opt-out mechanism, Facebook conveys ads to consumers based not only on what they do on Facebook, but also on "their activity on websites and apps off of Facebook":



Again, moreover, many mobile apps likewise continue to track users who are not actively engaged with those apps unless the subscribers take additional steps to stop such tracking—a practice that many consumers may find surprising.<sup>57</sup> Nor do most consumers affirmatively "choose" to let mobile operating systems such as Android use their location information for

---

<sup>57</sup> See, e.g., Kashmir Hill, *Change This iPhone Setting to Stop Closed Apps from Tracking Your Location*, Forbes (Aug. 11, 2014), <http://www.forbes.com/sites/kashmirhill/2014/08/11/iphone-app-location-tracking/>.

advertising or choose to let third-party app developers share location information with advertising networks, but that is also what happens.<sup>58</sup>

In short, notions of consumer “choice” cannot justify differential treatment of ISPs and non-ISP actors that collect online information. A recent consumer survey confirms that conclusion. According to a telephone survey of 800 Internet users nationally, an overwhelming majority of consumers (94 percent) agree with the statement that “[a]ll companies collecting data online should follow the same consumer privacy rules so that consumers can be assured that their personal data is protected regardless of the company that collects or uses it.”<sup>59</sup> And a similarly overwhelming majority of consumers likewise agree that “online privacy should be protected based on the sensitivity of different types of online data” rather than “based on the type of Internet company that uses the data, like broadband providers, social networks or search engines.”<sup>60</sup>

#### **4. *Competition and Switching Costs Cannot Justify Asymmetric Regulation***

Several commenters also repeat the premise that ISPs benefit from higher switching costs and face less competition than other major Internet companies and should thus be subject to unusually burdensome marketing restrictions.<sup>61</sup> As discussed in our opening comments, the

---

<sup>58</sup> See AT&T Comments at 21-25. Although some operating systems (such as Apple’s iOS) allow consumers to turn off location information for particular apps (*e.g.*, when not in use), they do not enable consumers to opt out of marketing uses for the location information those apps do collect.

<sup>59</sup> Public Opinion Strategies & Peter D. Hart, Memorandum to Progressive Policy Institute, at 2 (attached to Letter from Will Marshall, Progressive Policy Institute, to Marlene Dortch, FCC, May 26, 2016).

<sup>60</sup> *Id.* at 3.

<sup>61</sup> Electronic Frontier Foundation (“EFF”) Comments at 10-11; Consumer Watchdog Comments at 4; New America’s Open Technology Institute (“OTI”) Comments at 5-6; American Civil Liberties Union (“ACLU”) Comments at 3. We are here addressing questions of *retail* competition. Some commenters appear to invoke the distinct “gatekeeper” (or “terminating monopoly”) concept as a basis for asymmetric regulation. *E.g.*, Public Knowledge Comments at 3. As we have explained, however, that concept has

empirical premise of this argument is false, and the policy conclusion would not follow even if it were true.

First, ISPs do not in fact face less competition or enjoy higher switching costs than other major platform providers. For example, we have submitted voluminous evidence into this record concerning the competition faced by mobile providers, which is as intense as it is precisely because switching costs are so low. That evidence is unrebutted: the commenters who raise the “lack of competition” point generally ignore mobile broadband competition.<sup>62</sup> In contrast, the FTC has found that consumers “might have limited ability to block or control ... tracking” by an operating system such as Android unless, for example, they “chang[e] th[at] operating system”—*i.e.*, by purchasing a new phone and abandoning all of their Android-associated apps.<sup>63</sup> Similarly, as a moment’s reflection confirms, it would be no less difficult—and sometimes far more difficult—for privacy-conscious users to switch from T-Mobile to AT&T (or vice versa) than to switch from Facebook to another social-networking site with a fraction of the users, to abandon their long-held Gmail accounts, or to throw away their Android phone (and its apps) and switch to an iPhone.

In any event, it would be inappropriate to invoke “competition” here as a basis for asymmetric opt-in requirements even if ISPs did face less competition or enjoy greater switching costs than Google or Facebook. Professor Christopher Yoo explains in his comments (at 5): “Every major privacy regulatory regime of which I am aware applies equally to all industry players regardless of the level of competition. ... [S]mall companies often look to more

---

nothing to do with retail competition and is logically unrelated to any issue in this proceeding. *See* AT&T Comments at 47 n.102.

<sup>62</sup> *See, e.g.*, CDT Comments at 18 (relying on fixed-broadband statistics).

<sup>63</sup> *2012 FTC Privacy Report* at 56.

widespread use of private information to gain a competitive advantage against their larger rivals, and harm to consumers associated with disclosures or abuses of private information does not turn in any way on the size of the company involved.”

**5. *Concerns About Distinguishing Between Sensitive and Nonsensitive Data Cannot Justify Asymmetric Regulation***

Some commenters contend that the Commission should reject the FTC’s recommendation for a sensitivity-based notice-and-choice regime, and should saddle ISPs with a categorical opt-in requirement, on the theory that it is too problematic to do what the FTC and the Internet ecosystem have long done: distinguish between sensitive and nonsensitive data. That claim is meritless.

Public Knowledge wrongly contends (at 24) that it would not be technologically “feasible” in “the broadband context” to follow the FTC’s “‘by type’ privacy classification regime,” under which “only information deemed especially sensitive (*e.g.*, financial and health information) [is] subject to unique handling and collection restrictions.” Public Knowledge reasons that, to follow that regime in this context, ISPs must “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” (*id.* (emphasis omitted)). That argument is logically inapplicable to most data at issue here and, in any event, rests on a basic misconception of how targeted advertising works.

First, the argument could logically apply, if at all, only to a tiny subset of the data that the proposed rules would restrict ISPs from using: the *content* of particular communications, addressed in a single paragraph of the NPRM (at ¶ 67). It cannot justify restrictions on uses of data categories that are nonsensitive, such as an ISP’s use of its customers’ mere names and email addresses or the fact that they visited particular websites indicating nonsensitive interest

categories.<sup>64</sup> For example, an ISP would trigger no genuine privacy concerns if it designs an algorithm to serve third-party sports-related ads to customers who use that ISP to connect them to a web address such as espn.com, particularly if the ISP does not even share the identities of those customers with the third-party advertisers. Despite Public Knowledge’s contrary suggestion, the ISP also need not “inspect” the content in any of those customers’ “packet[s]” to determine whether they are sensitive;<sup>65</sup> it need only use the address header that provides routing information. And there is nothing particularly sensitive about the mere fact that a customer has visited a sports-related website. Again, countless online companies serve ads to consumers on the basis of such nonsensitive information, and the ad-based Internet ecosystem would collapse if—as Public Knowledge appears to propose—opt-in were required for such innocuous uses of customer data.

In any event, Public Knowledge’s argument is meritless for the independent reason that it misconceives how providers ensure that sensitive information is not used for marketing purposes. Many online providers gain access to a wide range of customer information in the ordinary course of business. Restricting their ability merely to use that information for marketing purposes would serve no privacy interest where the provider is (1) accessing no information to which it would not otherwise have access; (2) not sharing any information with third-party advertisers; and (3) not using any sensitive information for marketing purposes. To satisfy that third criterion, providers need not “inspect” the contents of a customer’s

---

<sup>64</sup> The FTC recognizes this point when it limits any concern about the “inspect[ion]” of communications to the “*content* of customer communications,” FTC Comments at 22 (emphasis added), such as “contents of emails; communications on social media; search terms; web site comments; items in shopping carts; inputs on web-based forms; and consumers’ documents, photos, videos, books read, [and] movies watched,” *id.* at 20. Even as to such content, the FTC’s concerns about “inspection” are misplaced for the reasons discussed below.

<sup>65</sup> Public Knowledge Comments at 24-25.

communications to determine whether they are sensitive; instead, such providers simply avoid using categories of sensitive information.<sup>66</sup> Such providers typically rely on industry self-regulatory guidelines, widely followed throughout the digital advertising industry, that preclude the use of categories of presumptively sensitive information to target marketing.<sup>67</sup> For example, consistent with the National Advertising Initiative’s industry standards, online advertising providers would not place ads targeting certain sensitive medical conditions without consent. No less than Google or any other company that delivers online advertising, ISPs are just as capable of following the same guidelines and protecting the same consumer privacy interests without any need for “manual inspection of each packet.”<sup>68</sup>

Professor Ohm separately argues that the Commission should reject the FTC’s recommendation for a sensitivity-based notice-and-choice regime because, he says, people disagree about how to draw lines between sensitive and nonsensitive data elements.<sup>69</sup> That argument is untenable. The FTC and the rest of the Internet ecosystem have been drawing precisely such lines for decades, and they have done so because they understand that opt-in imposes substantial costs that should be incurred only when necessary to prevent genuine consumer harm. At bottom, Professor Ohm’s recommendation for a categorical opt-in regime assigns no weight to those costs, no matter how large, and infinite weight to any privacy interest,

---

<sup>66</sup> See, e.g., Google, *Interest-based advertising* (visited June 8, 2016), <https://support.google.com/adwordspolicy/answer/143465?hl=en>.

<sup>67</sup> See, e.g., DAA, *Application of Self-Regulatory Principles to the Mobile Environment* (July 2013), [http://www.aboutads.info/DAA\\_Mobile\\_Guidance.pdf](http://www.aboutads.info/DAA_Mobile_Guidance.pdf); Network Advertising Initiative (“NAI”) Code of Conduct (2013), [https://www.networkadvertising.org/2013\\_Principles.pdf](https://www.networkadvertising.org/2013_Principles.pdf).

<sup>68</sup> Public Knowledge Comments at 24. Public Knowledge also expresses concern (at 15-17) that ISPs may use information about customers they obtain from third parties (such as credit-reporting agencies) to discriminate against customers in impermissible ways. But various federal statutory schemes already protect consumers against discriminatory and other socially undesirable uses of financial and other sensitive data. Those concerns have no bearing on whether, under ordinary notice-and-choice principles, ISPs should be free to use data for otherwise permissible marketing purposes.

<sup>69</sup> Ohm Reply Comments at 11-13.

no matter how negligible. As discussed below, the First Amendment does not permit such ill-tailored restrictions on commercial speech, and neither do sound policy considerations. Again, the modern Internet economy has generated countless high-value, low-cost services because flexible notice-and-choice rules have permitted all participants to make productive use of nonsensitive customer-specific information. The government would slam the brakes on the Internet's phenomenal growth if, as Professor Ohm proposes, it jettisoned any cost-benefit analysis in this context and dispensed with the need to distinguish between sensitive and nonsensitive information.

Professor Ohm further argues that any information that *would be useful* for advertising would necessarily *cause harm* to consumer privacy.<sup>70</sup> That is plainly incorrect. To begin with, mere ISP customer lists (names and email addresses) are useful for advertising, yet the proposed rules would bar their use for most advertising purposes in the absence of opt-in consent. Just as important, non-ISP Internet companies routinely make use of nonsensitive web data, such as top-level URLs visited (espn.com or shoes.com), in order to tailor relevant advertising to consumers, and they do so without confronting burdensome opt-in requirements. Likewise, an ISP does not “harm privacy” when, like all these other Internet companies, it uses *the same information* to tailor advertising of its own. Taken to its logical conclusion, application of Professor Ohm's sweeping argument would effectively tear down that pillar of the modern Internet economy.

### **C. The Proposed Opt-In Requirements Would Be Unlawful**

To the extent the Commission is authorized to regulate ISP marketing practices in the first place,<sup>71</sup> it has ample authority to do what the FTC suggests: align its rules with that

---

<sup>70</sup> *Id.* at ii (“data that contains so little information about individuals that it cannot be used to harm privacy is data that is also not useful in other ways, for example for advertising”).

<sup>71</sup> *Cf.* AT&T Comments at 100-113.

agency’s “longstanding approach, which calls for the level of choice to be tied to the sensitivity of data[.]”<sup>72</sup> A few commenters obliquely suggest that Section 222 deprives the Commission of that authority and requires it to subject ISPs to asymmetrically burdensome privacy rules, including opt-in requirements for most marketing purposes.<sup>73</sup> That assertion is baffling. Section 222 provides that “approval of the customer” must take the form of opt-in consent (“express prior authorization”) in only two contexts: access to “call location information” for cellular and VoIP telephone calls and certain uses of “automatic crash notification information.”<sup>74</sup> For all other contexts, Congress preserved the Commission’s discretion to permit less rigid choice mechanisms, including opt-out. And the Commission has done precisely that for many years, calibrating the level of choice to various policy considerations consistent with the general requirements of Section 222.<sup>75</sup>

Indeed, insofar as the Commission has authority in this area at all, it not only *may* ensure harmony with the FTC’s context-sensitive regime, but *must* do so. As we and many other commenters have explained, the Commission would violate both the Administrative Procedure Act and the First Amendment if, at odds with the FTC’s approach, it subjected ISPs to an opt-in requirement for any first- or third-party marketing that involves neither the use of sensitive information nor sharing with third-party advertisers.<sup>76</sup> That requirement would in fact fail all three prongs of the applicable *Central Hudson* analysis.

---

<sup>72</sup> FTC Comments at 23.

<sup>73</sup> *See, e.g.*, Public Knowledge Comments at 4.

<sup>74</sup> 47 U.S.C. § 222(f).

<sup>75</sup> *See, e.g.*, Third Report and Order, *Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, 17 FCC Rcd 14860, ¶¶ 5-9 (2002). Notably, the NPRM’s proposed distinction between communications-related and non-communications-related services is itself found nowhere in Section 222 or elsewhere in the Communications Act.

<sup>76</sup> *See* AT&T Comments at 88-100.

*First*, the requirement would promote no discernible privacy interest where information is neither sensitive nor shared with third-party advertisers.<sup>77</sup> Indeed, as the FTC and other commenters suggest, a blanket opt-in requirement would contradict customer expectations about how their information is used online—expectations informed by the FTC’s “longstanding approach, which calls for the level of choice to be tied to the sensitivity of data[.]”<sup>78</sup>

It also is useful to contrast the position the Commission would have to take in any constitutional defense of the proposed marketing restriction with the very different position the federal government has recently persuaded several courts of appeals to adopt under the Fourth Amendment. For example, the Fourth Circuit recently agreed that, in the context of criminal investigations, “an individual can claim ‘no legitimate expectation of privacy’ in information that he has voluntarily turned over to a third party”—in that case, historical cell-tower location information that an individual revealed to a mobile wireless operator simply by using its services.<sup>79</sup> Of course, reasonable people disagree with that conclusion as a legal and policy matter, and ISPs do not generally disclose personally identifiable data about their customers to third parties except in limited circumstances, such as where disclosure is required by law or where a customer has provided consent. Our point is simply that the federal government cannot square its position in these Fourth Amendment cases with any claim in this context that consumers in fact have a strong interest in keeping the same wireless operators from merely *using* (rather than disclosing) the same information at issue in those cases and much less sensitive information as well.

---

<sup>77</sup> See AT&T Comments at 93-94.

<sup>78</sup> FTC Comments at 23.

<sup>79</sup> *United States v. Graham*, No. 12-4659, slip op. at 10 (4th Cir. May 31, 2016) (en banc).

*Second*, the proposed requirement would also be radically underinclusive, and thus fail the second *Central Hudson* prong, because it would do nothing to keep all other non-ISP actors from collecting and using all the same information for their own marketing purposes. Again, the widespread accessibility of those data to multiple online companies not only informs consumer expectations in this context, but underscores how ineffective the proposed rules would be in protecting any genuine “privacy” interest.<sup>80</sup>

*Third*, under the final *Central Hudson* prong, the proposed opt-in rule would not be narrowly tailored because, if the government had any legitimate interest in “protecting” consumers from unshared uses of nonsensitive information, it could achieve that interest through a less intrusive opt-out mechanism.<sup>81</sup>

For these reasons, the Tenth Circuit’s *U.S. West* decision,<sup>82</sup> which invalidated the Commission’s initial opt-in rules on the basis of a single *Central Hudson* prong, would apply *a fortiori* here. No commenter supporting the proposed opt-in requirement faces up to these concerns. Supporters that address the constitutional issues at all simply assume that this case would be controlled by the D.C. Circuit’s 2009 decision in *NCTA*.<sup>83</sup> But that decision is inapposite. First, the opt-in requirement upheld there targeted not the mere *use* of individually identifiable customer information, but the *sale* of such information to third-party data brokers. The D.C. Circuit attached decisive importance to that fact, explaining that “[t]he evidence showed that customers were less willing to have their information *shared with third parties* as

---

<sup>80</sup> See AT&T Comments 94-96.

<sup>81</sup> See *id.* at 96-97; see also note 2, *supra* (noting that unusually privacy-conscious customers can be expected to avail themselves of opt-out options).

<sup>82</sup> *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999).

<sup>83</sup> See *NCTA v. FCC*, 555 F.3d 996 (D.C. Cir. 2009); see, e.g., Public Knowledge Comments at 38-39.

opposed to affiliated entities,” and finding that the Commission “reasonably concluded that customer information would be at a greater risk of disclosure *once out of the control of the carriers and in the hands of entities not subject to § 222.*”<sup>84</sup> In contrast, the opt-in requirement proposed here would apply to mere *uses* of information for first- and third-party marketing even when no information is shared with third-party advertisers. The requirement’s supporters overlook that distinction in part because they seem to assume that third-party marketing necessarily involves disclosing individually identifiable information to third-party advertisers. As we have explained, however, that assumption is simply incorrect. Like Google, an ISP can *use* customer-specific information to tailor advertisements on behalf of third parties without *disclosing* individually identifiable information to those third-party advertisers.

Moreover, because *NCTA* involved the traditional closed telephone network rather than the Internet ecosystem, the rule’s challengers in that case were unable to raise any underbreadth challenge under *Central Hudson*’s second prong. Here, in contrast, such an underbreadth challenge would be a central component of the First Amendment litigation because this case would involve the Internet ecosystem, where information is pervasively already “in the hands of entities not subject to § 222.”<sup>85</sup>

## **II. THE COMMISSION SHOULD NOT RESTRICT INFORMATION-SHARING AMONG ISP AFFILIATES OR BETWEEN ISPs AND THEIR THIRD-PARTY AGENTS**

Some commenters ask the Commission to impose opt-in requirements for any transfer of personal information between ISP affiliates, even if they share a common brand.<sup>86</sup> As Verizon

---

<sup>84</sup> *NCTA*, 555 F.3d at 1002 (emphasis added). As Professor Tribe explains, *NCTA* is distinguishable for that reason and others and, in any event, is questionable precedent to the extent it conflicts in principle with the Supreme Court’s subsequent decision in *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2563 (2011). Tribe & Massey White Paper at 7.

<sup>85</sup> *NCTA*, 555 F.3d at 1002.

<sup>86</sup> See New America’s OTI Comments at 13-14; Access Now Comments at 9-10.

explains, that position ignores consumer expectations and would create arbitrary regulatory burdens with no consumer benefit.<sup>87</sup> Under the FTC’s regime, no choice mechanism (let alone an opt-in requirement) is necessary when formally separate entities within a corporate family share information and cross-market their services where the corporate relationship is clear to customers, such as through branding or marketing activities.<sup>88</sup> The Commission’s rules should align with that common sense approach. Any contrary approach would simply induce ISPs to undertake costly and pointless corporate restructurings simply to avoid undue regulatory burdens.

The Commission should also reaffirm its longstanding position that no opt-in mechanism is necessary when carriers share data with third-party service providers who act as the carriers’ agents. Like traditional telephone companies, ISPs often depend on third-party agents to help deliver service, operate retail stores, and perform other essential functions, such as billing, technical maintenance, and marketing. The Commission has previously recognized that, subject only to opt-out approval, carriers should be allowed “to share CPNI with their agents because the principles of agency law hold carriers responsible for the acts of their agents.”<sup>89</sup> Any rules adopted in this proceeding should reaffirm that principle. A contrary approach would serve no privacy interest and would wastefully induce ISPs to take in-house a variety of functions that are more efficiently provided by an agent.

---

<sup>87</sup> Verizon Comments at 24-28 (citing Lee Rainie & Maeve Duggan, Pew Research Center, *Privacy and Information Sharing*, at 24 (Jan. 14, 2016)).

<sup>88</sup> *2012 FTC Report* at 41-42.

<sup>89</sup> Third Report and Order, *Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, 17 FCC Rcd 14860, ¶ 46 (2002).

### III. THE COMMISSION SHOULD REVISE ITS PROPOSED RULES ADDRESSING USE AND SHARING OF DE-IDENTIFIED DATA

Our opening comments explained that allowing ISPs to create, use, and share de-identified data produces enormous social benefits. AT&T provides such data to business customers, research institutions, and governmental entities, which use the data, among other things, to enhance customer service, develop new products, undertake cutting-edge research, and improve urban planning.<sup>90</sup> We further explained that AT&T's use of such data creates these benefits without substantial risk to consumer privacy because AT&T takes reasonable precautions to ensure the anonymity of customer data it shares with third parties.<sup>91</sup>

Many other commenters confirm the substantial benefits that flow from the use and sharing of de-identified data,<sup>92</sup> and thus agree that broadband providers should be free to use and share de-identified customer data under the same framework that the FTC applies to the rest of the Internet ecosystem.<sup>93</sup> Under that framework, providers may “use and disclose individual de-identified data” where commercially reasonable steps have been taken to prevent re-identification.<sup>94</sup> Indeed, as AT&T has explained, the Commission lacks legal authority to adopt

---

<sup>90</sup> AT&T Comments at 63-66.

<sup>91</sup> *Id.* at 66.

<sup>92</sup> See Consumers' Research Comments at 22-24; CTIA Comments at 42-43; T-Mobile Comments at 36. Notably, since the filing of the comments, the New York Times has reported that researchers at Microsoft were able to use anonymized search data to distinguish Internet users that were suffering from pancreatic cancer “even before they have received a diagnosis of the disease.” John Markoff, *Microsoft Finds Cancer Clues in Search Queries*, The New York Times (June 7, 2016), <http://www.nytimes.com/2016/06/08/technology/online-searches-can-identify-cancer-victims-study-finds.html>.

<sup>93</sup> See CTIA Comments at 37-39; FPF Comments at 1, 3; ITIF Comments at 19; Sprint Comments at 8; State Privacy and Security Coalition (“SPSC”) Comments at 5; T-Mobile Comments at 35-36; Verizon Comments at 44.

<sup>94</sup> See CTIA Comments at 38; Sandvine Comments at 20-21; Sprint Comments at 8; T-Mobile Comments at 35-36; Verizon Comments at 44; *see also* FPF Comments at 3.

a contrary position.<sup>95</sup> Section 222(c) authorizes the Commission to restrict use only of “individually identifiable” CPNI. Information that has been de-identified using appropriate statistical techniques (such as those used by AT&T) is, by definition, not “individually identifiable.”

EFF is thus wrong in contending that de-identified non-collective data can legally be made “subject to the [NPRM’s] proposed opt-out and opt-in customer consent requirements.”<sup>96</sup> Even though de-identified non-collective data may not constitute “aggregate customer information” under Section 222(c)(3), Section 222(c)(1) requires customer approval only for the use and disclosure of “individually identifiable customer proprietary network information.”<sup>97</sup> Again, de-identified data are not “individually identifiable” CPNI, and are thus not subject to Section 222(c)(1) restrictions, as the whole point of de-identification is to create data that are not “individually identifiable.”<sup>98</sup> EFF’s position would also violate the First Amendment. There is simply no privacy interest in de-identified customer information because, again, such information reveals nothing about any identifiable person. Thus, EFF’s “opt-in” proposal for de-

---

<sup>95</sup> AT&T Comments at 68; *see also* Comcast Comments at 85-86; CTIA Comments at 35-37; Sprint Comments at 7-8; T-Mobile Comments at 35.

<sup>96</sup> EFF Comments at 16; *see also* New America OTI Comments at 27-28.

<sup>97</sup> 47 U.S.C. §§ 222(c)(1), (3).

<sup>98</sup> The plain language of Section 222(c)(1) permits no other conclusion, and the rule of constitutional avoidance would resolve any statutory ambiguity even if there were one. *See* AT&T Comments at 99-100. Reading Section 222(c)(1) to mean what it says also preserves independent significance for Section 222(c)(3), which addresses “aggregate customer information.” That provision not only confirms that aggregate data can be used without customer consent for any purpose, but independently requires local exchange carriers to provide aggregate information to “other carriers or persons on reasonable and nondiscriminatory terms and conditions upon reasonable request therefore.” This provision thus focuses on protecting *competition*. It nowhere suggests that Section 222(c)(1), contrary to its plain text, applies to information that is not “individually identifiable.” Moreover, CPNI and “aggregate customer information” that is derived from CPNI are defined as mutually exclusive categories—aggregate data are not CPNI at all. *See* 47 U.S.C. 222(h)(1) & (2). Thus, anonymized customer information, if it is not “aggregate,” is simply CPNI that is not individually identifiable. Such non-individually identifiable information does not become subject to Section 222(c)(1) simply because it is not aggregate.

identified data flunks the *Central Hudson* test because it would burden truthful commercial speech without advancing any cognizable public interest.<sup>99</sup>

That said, ISPs should of course take reasonable safeguards to keep de-identified data from re-identification.<sup>100</sup> Thus, as noted, AT&T undertakes industry-standard statistical processes to anonymize non-aggregate data it shares with third parties and requires those third parties to agree that they will refrain from attempting to re-identify those data. The Commission need not, however, dictate specific approaches to de-identifying data. Any Commission-mandated approach would quickly become obsolete as new de-identification techniques are developed. But the Commission can rely on the types of “best practices” that AT&T currently uses to produce non-collective data sets that cannot reasonably be re-identified.<sup>101</sup> As FPF explains, a “range of de-identification tools ... are available to make it difficult or impossible to re-identify data as pertaining to a specific individual,” including use of statistical “blurring,” “perturbation,” and “suppression.”<sup>102</sup> The Commission should also avoid drawing undue

---

<sup>99</sup> See AT&T Comments at 91-100.

<sup>100</sup> See, e.g., FPF Comments at 6; Verizon Comments at 44. The Marketing Research Association (“MRA”) appears to suggest that use and sharing of non-collective, de-identified data should be permitted only in the context of use for research, but not any commercial purpose. MRA Comments at 7. Any such limitation would be unlawful. First, as explained above, the Commission would have no statutory authority for such a distinction. Section 222 gives the Commission regulatory authority only over “individually identifiable” CPNI. Second, MRA’s proposed restriction would enmesh the Commission in pointless disputes about whether data is being used and shared for “authorized” purposes. Finally, such a distinction would violate the First Amendment, as it would burden truthful speech simply because it was “commercial” in character without any plausible governmental interest, given that the speech would involve the sharing of information that has been statistically de-identified to preclude the data from being linked to individuals. See AT&T Comments at 99; see also *id.* at 91-98.

<sup>101</sup> *Id.* at 67 n.140.

<sup>102</sup> FPF Comments at 6; see also EPIC Comments at 22-23 (discussing scholarship on developing robust de-identification techniques); Sandvine Comments at 21 (discussing de-identification techniques). AT&T agrees with various commenters that the Commission should not try to develop a “list” of data fields that must be removed for data to be considered “aggregate.” Cf. *NPRM* ¶ 163. It is doubtful that any “one-size-fits-all” list could be developed and, in any event, the list would likely be need to be continuously updated as industry standards evolve over time.

inferences from publicized cases involving the “re-identification” of anonymized data. In contrast to most real-world uses of de-identified data, as FPF notes, the information at issue in those cases was not kept secure, was instead made fully public and thus subject to any conceivable re-identification process, and “was actually unprotected pseudonymous data containing well-recognized indirect identifiers.”<sup>103</sup>

There is also no merit to EFF’s proposal to require ISPs to publicize the statistical methods they use to de-identify particular data sets.<sup>104</sup> That requirement would in fact undermine data security by giving would-be hackers important clues for potential re-identification. The requirement is also unnecessary to promote development of more effective de-identification techniques. EFF offers no basis for concluding that existing collaborative processes among industry stakeholders are insufficient. And EFF likewise identifies no case in which de-identified data created and secured by ISPs (or shared with third parties that were obligated to keep it secure) has been re-identified.

Finally, as explained in our opening comments, the Commission should scale back aspects of the proposals that are overbroad or that might otherwise be read to impose excessive regulatory obligations. *First*, consistent with its prior CPNI orders, the Commission should clarify that providers may use individualized data in order to create aggregate or non-collective de-identified data sets.<sup>105</sup> *Second*, the Commission should apply any privacy rules only to

---

<sup>103</sup> FPF Comments at 4. *See also* Ann Cavoukian and Daniel Castro, *Big Data and Innovation, Setting the Record Straight: De-identification Does Work*, 4, 5-6 (June 16, 2014); *cf.* EPIC Comments at 22.

<sup>104</sup> EFF Comments at 15.

<sup>105</sup> AT&T Comments at 68-69; *see also* Sandvine Comments at 20. Correlatively, “if the carrier de-identifies data to add protection in some contexts ... that should not preclude the carrier from using the underlying data in a way that is consistent with consumers’ expressed preferences, *e.g.*, re-identifying the data to serve more effective and relevant advertisements.” Verizon Comments at 45 n.128. *See also* AT&T Comments at 69 n.144.

customer data that can “reasonably” be linked to a specific person.<sup>106</sup> *Third*, the Commission should clarify that an ISP has no obligation to enter into contractual provisions with third parties to keep them from re-identifying aggregate data that are so aggregated that there is no reasonable possibility of re-identification. Such an obligation would impose substantial burdens without any benefits.<sup>107</sup> *Finally*, the Commission should clarify that it does not seek to hold ISPs strictly liable for actions of third parties with whom they have shared de-identified data.<sup>108</sup> Instead, any liability in such circumstances should be based on a fact-specific “reasonableness” standard.

#### **IV. THE COMMISSION SHOULD REVISE ITS PROPOSED DATA SECURITY AND BREACH NOTIFICATION RULES**

The NPRM proposes detailed rules governing virtually all aspects of data security and breach reporting. As discussed in our opening comments (at 100-103), the Commission lacks statutory authority to regulate customer data that is broadly collected and used by non-ISP entities and is therefore not “proprietary” for purposes of any provision of Section 222.<sup>109</sup> But even if such data did qualify as “CPNI,” the operative provisions of Section 222—subsections (b) and (c)—do not authorize the Commission to issue prescriptive rules concerning how to secure and maintain any customer-specific information and report any data breaches.<sup>110</sup> Those

---

<sup>106</sup> AT&T Comments at 69; *see also* Comcast Comments at 84-85.

<sup>107</sup> AT&T Comments at 70-71. It also logically follows that the Commission should not require ISPs to “monitor” contractual requirements with third parties regarding re-identification of highly aggregated data. There should be no obligation to enter into such contracts in the first place when there is no reasonable likelihood that such data can be re-identified.

<sup>108</sup> *Id.* at 72.

<sup>109</sup> This is reinforced by the Third Circuit’s recent decision in *In re Nickelodeon Consumer Privacy Regulation*, No. 15-1441, slip op. (3d Cir. June 27, 2016). As the Third Circuit noted, in the Children’s Online Privacy Protection Act, Congress gave the FTC express “authority to *expand* the types of information that count as personally identifiable under that law,” but underscored that courts should not expand the scope of “personally identifiable information” in statutes that define that term without specifically “empower[ing] an administrative agency to augment the definition.” *Id.* at 55-57 (emphasis in original).

<sup>110</sup> *See generally* AT&T Comments at 100-13.

provisions address only CPNI as defined in Section 222(h)(1), not other types of customer-specific information, and govern only the use and disclosure of such CPNI. They nowhere purport to give the Commission general regulatory authority over data security, retention, and breach disclosure by ISPs.

Taking their lead from the NPRM (at ¶ 300), some commenters assert that subsection (a) grants the Commission the sweeping data-security authority that subsections (b) and (c) withhold.<sup>111</sup> It does not. As AT&T and others have explained, subsection (a) identifies *who* has duties under Section 222, while subsections (b) and (c) specify *what* those duties are.<sup>112</sup> Nor does Section 201(b) supply the missing authority, as some commenters contend.<sup>113</sup> That provision is inapplicable because, under established principles of statutory construction, more general statutory provisions are unavailable as sources of regulatory authority where Congress has adopted a comprehensive and much more specific provision to address the subject matter at issue.<sup>114</sup> Here, Section 222 reflects Congress's considered decisions about which consumer privacy protections are necessary and which are not. Moreover, data privacy and security practices related to non-CPNI customer information cannot be considered "in connection with" broadband service subject to Section 201(b).<sup>115</sup> Finally, the Commission would be entitled to no

---

<sup>111</sup> See, e.g., CDT Comments at 11-12; EFF Comments at 2; EPIC Comments at 8; New America OTI Comments at 18-19.

<sup>112</sup> AT&T Comments at 103-08; see also American Cable Association ("ACA") Comments at 13-15; CenturyLink Comments at 15-16; Comcast Comments at 71-75; CTIA Comments at 25-35; Independent Telephone & Telecommunications Alliance ("ITTA") Comments at 3-11; Sprint Comments at 5-6; T-Mobile at 15-18; USTelecom Comments at 7-8; Verizon Comments at 53-60.

<sup>113</sup> Cf. Common Sense Kids Action Comments at 2; Free Press Comments at 15-16; New America OTI Comments at 12.

<sup>114</sup> AT&T Comments at 108-09 (citing cases); see also ACA Comments at 15-16; Comcast Comments at 69; CTIA at 60-62; Verizon Comments at 53-60.

<sup>115</sup> See, e.g., AT&T Comments at 109; see also *id.* at 110-113 (addressing other putative sources of statutory authority).

deference in its interpretation of these provisions. As the Supreme Court has explained, “[w]hen an agency claims to discover in a long-extant statute an unheralded power to regulate a significant portion of the American economy, we typically greet its announcement with a measure of skepticism. We expect Congress to speak clearly if it wishes to assign to an agency decisions of vast economic and political significance.”<sup>116</sup>

In any event, the NPRM’s proposed rules governing data security and data breaches are untenable as a policy matter—and would thus violate the APA—because they depart starkly and unjustifiably from the corresponding regime governing the rest of the economy.<sup>117</sup> The Commission could mitigate, though not eliminate, many of the problems with the proposed rules by confining them to genuinely sensitive customer information whose disclosure could harm consumers.<sup>118</sup> There is no cognizable policy justification for requiring data security, data minimization, and breach reporting obligations with respect to customer information that poses no such risk of harm. At a minimum, the Commission should substantially revise its rules to reflect the several flaws identified by the FTC as well as many other commenters in this proceeding.

**Data Security.** While the NPRM purports to adopt a “reasonableness” standard for data security that allows for “flexibility,”<sup>119</sup> the proposed data security rules fall short of that promise. The rules would deem virtually all customer data to be sensitive regardless of whether release

---

<sup>116</sup> *Utility Air Regulatory Grp. v. EPA*, 134 S. Ct. 2427, 2444 (2014).

<sup>117</sup> AT&T Comments at 72-87.

<sup>118</sup> *Id.* at 75-78; *see also* ACA Comments at 35; CenturyLink Comments at 35-36, 39; Comcast Comments at 62-63; Consumers’ Research at 24; CTIA Comments at 175-76; DMA Comments at 28; Leibowitz Comments at 11; Sprint Comments at 13; SPSC Comments at 10-11; T-Mobile Comments at 51; Verizon Comments at 69; Wireless Internet Service Providers Association (“WISPA”) Comments at 21-23.

<sup>119</sup> *NPRM* ¶¶ 175, 217.

would actually harm consumers, and the proposed “reasonableness” standard does not expressly provide for any cost-benefit calculus in deciding what security measures are reasonable.<sup>120</sup> The Commission should clarify that both the seriousness of a potential threat and the costs of addressing it are both highly relevant factors in assessing the reasonableness of data security measures.

In fact, the current proposal’s failure to incorporate such cost-benefit considerations imperils the very data security objectives the proposal is designed to advance. In particular, many commenters observe that, by failing to distinguish between sensitive and nonsensitive data, the proposed rules would impair efforts to target the most important security threats.<sup>121</sup> In the words of one security professionals organization, those rules would “potentially interfere with a considerable amount of anti-abuse work” and make it more difficult for researchers and cybersecurity professionals to target vulnerabilities and malicious actors.<sup>122</sup>

The Commission should likewise withdraw or at least substantially revise the proposed requirement that companies “promptly remedy *any*” security concern found in a risk management assessment, regardless of the cost of doing so, regardless of the sensitivity of the underlying data, and regardless of the risk of breach.<sup>123</sup> The Commission lacks statutory authority to mandate how ISPs undertake and follow up on risk management assessments. But even if the Commission had such authority, it cannot reasonably impose overbroad data security rules whose costs far outweigh their benefits.

---

<sup>120</sup> AT&T at 78; *see also* CTIA Comments at 155-56.

<sup>121</sup> *See, e.g.*, Messaging Malware Mobile Anti-Abuse Working Group (“M3AAWG”) Comments at 2-6; Feamster, et al. Comments at 4-7.

<sup>122</sup> M3AAWG Comments at 2-6

<sup>123</sup> AT&T Comments at 79-80; *see also* ACA Comments at 24; CTIA Comments at 149-50, 163-64; Sprint at 18-19.

Just as important, the Commission should dispel any concern that, under the current wording of Proposed Rule 64.7005(a), ISPs could be held *strictly* liable for data breaches that they took reasonable steps to prevent.<sup>124</sup> As the FTC explains (at 26-27), any strict-liability requirement would conflict with the FTC’s own longstanding approach, which predicates liability on unreasonable data security practices rather than the mere fact of a breach. A strict-liability requirement would also contradict the Commission’s own recognition that security practices should be “calibrated to the nature and scope of the BIAS provider’s activities, the sensitivity of the underlying data, and technical feasibility.”<sup>125</sup> In short, as the FTC concludes, the Commission should revise any rule in this area to require ISPs to “ensure the *reasonable* security, confidentiality, and integrity” of proprietary customer data.<sup>126</sup> That approach aligns with the prevailing industry standards of the NIST Cybersecurity Framework and others, which permit a flexible and evolving approach to cybersecurity to meet the demands of “different threats, different vulnerabilities, and different risk tolerances.”<sup>127</sup>

Finally, the Commission should reject EPIC’s astonishing suggestion that the Commission should “require that service providers offer robust, end-to-end encryption for all

---

<sup>124</sup> AT&T Comments at 79; CenturyLink Comments at 32-33; CCA Comments at 37-38; CTIA Comments at 159-60; T-Mobile Comments at 47-48. The proposed rule states that an “ISP must ensure the security, confidentiality, and integrity of all customer [proprietary information]” that the provider holds. It does not appear that the Commission intended to create a strict-liability regime.

<sup>125</sup> *NPRM* ¶ 51.

<sup>126</sup> FTC Comments at 27-28 (emphasis in original); *see also* FTC, Data Security, <https://www.ftc.gov/datasecurity> (“[A] company’s data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.”). In this regard, AT&T agrees with the FTC that the Commission should establish “safe harbors” in any data security rules that it adopts. *Id.* at 29-30. The FTC is correct that safe harbors will provide “regulatory certainty for businesses” while “improv[ing] customer protections.” *Id.* at 30.

<sup>127</sup> *See* NIST, Framework for Improving Critical Infrastructure Cybersecurity, at 2 (Feb. 12, 2014), <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.

consumers free of charge.”<sup>128</sup> Here, too, no provision of the Communications Act authorizes the Commission to impose such a sweeping and burdensome mandate. In any event, compliance with this requirement would be impossible. The sender and the recipient of a communication are the “ends” between which end-to-end encryption secures information. ISPs transmit information—encrypted or unencrypted—between endpoints, and they are not themselves endpoints, at least in typical mass-market settings where they do not operate the network on a customer’s premises. As such, ISPs cannot themselves provide “end-to-end” encryption in those settings.

***Data Breach Reporting.*** The comments—particularly those of the FTC—confirm that, in multiple respects, the proposed data breach rules would impose costs exceeding any benefits.<sup>129</sup>

*First*, unlike the approach taken by most states, the Commission’s proposed rules would not base notification on whether there is a real likelihood of *harm* to the consumer.<sup>130</sup> The federal government itself uses this likelihood-of-consumer-harm standard when determining when to report unauthorized disclosures of the data it holds.<sup>131</sup> And, as former FTC Chairman Leibowitz explains, “the FTC has long supported requirements for companies to notify consumers of security breaches in *appropriate* circumstances, such as when information has been compromised that can lead to harms such as financial loss or identity theft.”<sup>132</sup> Thus, the

---

<sup>128</sup> See EPIC Comments at 23.

<sup>129</sup> FTC Comments at 30-33; *see also* AT&T Comments at 80-87.

<sup>130</sup> AT&T Comments at 80-81. Treating any unsuccessful attempt to access a customer account as a notification trigger would lead to massive over-notification: the overwhelming majority of such instances involve inadvertent mistakes by customers, not any nascent threat. *Id.* at 85; *see also* Verizon Comments at 67.

<sup>131</sup> AT&T Comments at 81 n.162.

<sup>132</sup> Leibowitz Comments at 11.

Commission should, at a minimum, include a “risk of harm” trigger for any reporting rules it adopts.<sup>133</sup>

Instead of focusing on risk of harm, the NPRM’s proposed breach reporting obligations instead would cover unauthorized access to *any* “customer proprietary information,” which, given how expansively the proposed rules would define that term, includes non-sensitive information and information not linkable to any person.<sup>134</sup> As the FTC observes, any obligation to disclose “breaches” involving such information would lead to counterproductive over-notification.<sup>135</sup> For example, a “breach” of customer IP addresses may trigger customer notification under the proposed rules even if those IP addresses are not associated with any other customer-specific information and could not be used to engage in identify theft or financial fraud. It is unclear what customers would do with such notifications; most likely, they would simply grow annoyed and confused. As the FTC adds, the proposed rules could also counterproductively require ISPs to collect and retain personal information they might otherwise not collect or retain simply to provide their customers needless notifications about security non-events.<sup>136</sup>

As the FTC suggests, therefore, the Commission should not require notification where the breach involves the release of “device identifiers, cookies, or other persistent identifiers standing

---

<sup>133</sup> AT&T Comments at 81; *see also* ACA Comments at 36-37, 55-56; CenturyLink Comments at 41-42; CTIA Comments at 176-77; Hughes Comments at 6-7; INCOMPAS Comments at 16-17; SPSC Comments at 10-13; T-Mobile Comments at 51; Verizon Comments at 69; WTA Comments at 17; XO Comments at 9-12.

<sup>134</sup> FTC Comments at 30-31.

<sup>135</sup> *Id.* at 31-32.

<sup>136</sup> *Id.* at 31.

alone,”<sup>137</sup> or where information has been inadvertently disclosed to an ISP’s employee.<sup>138</sup> In both cases, the unauthorized release of such information cannot realistically threaten harm to consumers. Similarly, the Commission should not require notification whenever an ISP employee accesses unauthorized information if there is no evidence that the employee improperly used or disclosed that information.

*Second*, as the FTC further explains, the Commission should not extend reporting obligations to agents of ISPs.<sup>139</sup> Such a requirement would lead only to duplicative notification, as the ISP itself will be providing any required customer notifications.<sup>140</sup> Allowing the ISP to control the notification process “ensures that the consumer would be receiving a breach notice from an entity with which the consumer has a pre-existing relationship, rather than a potentially unknown agent.”<sup>141</sup>

*Finally*, the Commission should eliminate the requirement that ISPs provide notice within ten days of discovering a breach. As the FTC explains, it often takes much longer than ten days to conduct an appropriate investigation to determine the scope of a breach and who is affected.<sup>142</sup> The proposed ten-day rule, therefore, would force ISPs to barrage consumers with incomplete

---

<sup>137</sup> *Id.* at 32; *see also* Leibowitz Comments at 11 (the NPRM’s requirements “should be more narrowly tailored to customer information that carries a risk of harm to the customer in the event of a breach, and in no case should apply to simple IP addresses, MAC addresses, or individually de-identified or aggregate data”).

<sup>138</sup> FTC Comments at 32; *see also* ACA Comments at 55-56; AT&T Comments at 86; Consumers’ Research at 24; CTIA Comments at 177; SPSC Comments at 16-17; T-Mobile Comments at 52.

<sup>139</sup> FTC Comments at 32.

<sup>140</sup> AT&T Comments at 86-87.

<sup>141</sup> FTC Comments at 32.

<sup>142</sup> *Id.* at 32-33; *see also* ACA Comments at 35-36, 55-56; CenturyLink at 43-44; Comcast Comments at 63-64; CCA Comments at 45; CTIA Comments at 180; DMA Comments at 26; INCOMPAS Comments at 17-18; SPSC Comments at 13-14; T-Mobile Comments at 53-54; Verizon Comments at 69-70; WISPA Comments at 21-23; XO Comments at 12-13.

and erroneous notifications followed by multiple corrections as more information comes to light.<sup>143</sup>

Unfortunately, the flaws in the NPRM extend even beyond the specific problems on which the FTC focuses. In at least two additional respects, the Commission should scale back obligations contemplated by the NPRM to avoid imposing overbroad notification requirements. First, the Commission should not require ISPs to issue notifications whenever they have identified no actual breach but merely discover conduct that might “reasonably lead to exposure of customer PI.”<sup>144</sup> As we and others have explained, ISPs cannot be expected to anticipate all conduct that may require reporting under such a subjective standard and to report it if it occurred.<sup>145</sup> Second, as previously noted, the Commission should not require ISPs to notify customers of unsuccessful attempts to access customer account information because that requirement, too, would generate massive over-notification.<sup>146</sup> There is no justification for requiring notice to customers unless there is some non-speculative basis for concern about actual consumer harm.

Nor should the Commission adopt NRF’s proposal to shift the burden of consumer notification from retailers to ISPs in connection with theorized breaches of commercial data conveyed over ISP networks.<sup>147</sup> Consumers that provide their information to a business expect

---

<sup>143</sup> FTC Comments at 33; *see also* Cincinnati Bell Comments at 13; CTIA Comments at 181. The FTC also recommends changes to the Commission’s proposal to require ISPs to include in notices contact information for national credit reporting agencies. Not all breaches will have the potential to affect credit history, and when they do not, including such information would simply confuse consumers. FTC Comments at 33. Instead, contact information for credit reporting agencies should be included only if the information breached could be used to open a new account (*e.g.*, Social Security numbers). *Id.* at 33-34.

<sup>144</sup> *NPRM* ¶ 250.

<sup>145</sup> AT&T Comments at 84; CTIA Comments at 177.

<sup>146</sup> AT&T Comments at 85 (discussing *NPRM* ¶ 203).

<sup>147</sup> National Retail Federation (“NRF”) Comments at 3-4.

*that business* to safeguard that information, as state breach notification laws recognize.<sup>148</sup> And if *that business's* systems are compromised, they expect that business, not their ISP, to inform them. Adopting NRF's proposal could thus generate significant confusion. To the extent that a business wishes to shift the burdens of notification to an ISP, or any other service provider, such commercial considerations are properly addressed through contractual provisions. AT&T is committed to ensuring the security and integrity of information that it maintains about its customers. Just like the businesses that make up NRF, it is of course subject to consumer notification obligations in the event of a reportable incident involving customer data that it holds.<sup>149</sup>

**V. THE PROPOSED DATA CORRECTION AND RETENTION PROPOSALS ARE UNWISE AND UNNECESSARY AND WOULD IMPOSE ENORMOUS COSTS**

Some commenters support the NPRM's suggestion (at ¶¶ 205-09) that ISPs be required to provide access to "all customer PI" in their possession and permit customers to "correct" their data as well as the NPRM's separate suggestion (at ¶¶ 221-32) that ISPs limit their collection and retention of customer data.<sup>150</sup> Those proposals would not only exceed the Commission's authority to regulate ISPs (see above) but would create enormous administrative burdens with no consumer benefits. No commenter advocating data correction and retention obligations

---

<sup>148</sup> See *id.* at 3.

<sup>149</sup> The breach examples cited by NRF overlook the independent legal and contractual obligations of businesses to encrypt "sensitive personal information"—including payment card information—that those businesses transmit over any ISP's network. See *e.g.* PAYMENT CARD INDUSTRY DATA SECURITY STANDARD QUICK REFERENCE GUIDE, version 3.2, Requirement 4.1 (requiring businesses to "use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks (e.g. Internet, wireless technologies, cellular technologies, General Packet Radio Service [GPRS], satellite communications)"); see also NEV. REV. STAT. § 603A.215 (2015) (affirmatively requiring Payment Card Industry Data Security Standard ("PCI-DSS") compliance for "data collectors" that accept payment cards). Again, ISPs cannot read encrypted data. Thus, when encrypted information is compromised, an ISP cannot even identify the individuals to whom the information pertains.

<sup>150</sup> See, *e.g.*, EFF Comments at 6-7, 13-14; EPIC Comments at 24-25.

addresses these fundamental concerns. The Commission should not impose prescriptive rules in this area but should instead work with industry to develop a set of best practices regarding consumer access and transparency.

First, insofar as the NPRM's proposed rules would require ISPs to make all customer data available for inspection and correction, they would *increase* data security risks by establishing an obvious target for hackers.<sup>151</sup> The proposed rules would also impose tremendous costs with no corresponding consumer benefit. Many commenters underscore the economic burden of designing systems that could compile all customer online behavior to permit consumer access and correction.<sup>152</sup> Neither the Commission nor any commenter has explained how consumers actually would benefit from (or even understand) information relating to such technical information categories as the IP addresses they visit, the port information associated with their access, and the DNS requests made. The Commission should not impose such enormously burdensome requirements because they would lack any practical utility, cause consumer confusion, and pose great security risks. Again, moreover, the Commission lacks authority to adopt such a far-reaching proposal.

The NPRM's proposed requirement for "privacy dashboards" is similarly misplaced. As explained in our opening comments (at 57 n.124), the Commission should instead permit ISPs to establish transparency- and privacy-enhancing mechanisms as a matter of industry best practices. AT&T recognizes the practical benefits of transparency and permits customers to adjust privacy settings and limit the use of their personal information. By prescribing in advance the types and means by which information must be disclosed to consumers, however, the Commission would preclude innovative and adaptive mechanisms to increase transparency. Consumers'

---

<sup>151</sup> CTIA Comments at 167-70; ACA Comments at 46.

<sup>152</sup> CenturyLink, Inc. Comments at 39; NTCA Comments at 64-65; CTIA Comments at 167-70.

information-access needs change over time and with new technologies. Accordingly, the Commission should encourage the adoption of innovative transparency mechanisms by issuing informal guidance and setting general objectives, not by adopting one-size-fits-all regulations.

Some commenters support the Commission’s proposal to limit the collection, retention, and deletion of consumer data.<sup>153</sup> But neither the Commission nor any commenter specifies what limitations might be appropriate, let alone what practical effects such limitations might have on the use of customer information. Indeed, as the FTC has cautioned, requirements related to data collection, minimization, and deletion must balance “beneficial uses of data with privacy protection” in order to avoid unintended social harms.<sup>154</sup> Before adopting any such requirements, therefore, the Commission must rigorously analyze how data-minimization rules could threaten the consumer benefits derived from customer information, including the development and delivery of high-quality consumer services and the socially valuable uses of aggregate data. The Commission has not yet undertaken any such analysis.

In all events, Section 222 does not authorize the Commission to impose rules in this area. Section 222 only authorizes the Commission to regulate the use and disclosure of CPNI *after* it has been collected. It does not permit the Commission to restrict the *collection* or *retention* of CPNI or any other consumer data. Indeed, the NPRM recognizes (at ¶¶ 222, 226, 231) that, while some statutes may authorize the regulation of such activities, “Section 222 does not

---

<sup>153</sup> EFF Comments at 6-7; EPIC at 24-25.

<sup>154</sup> FTC, *Internet of Things: Privacy & Security in a Connected World* 38 (2015), <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>; *see also* Return Path Inc. Comments at 4-5; Competitive Carriers Association (“CCA”) Comments at 42-43.

contain an analogous provision regarding the collection of customer information,” nor does it authorize the Commission to limit retention periods or regulate data deletion methods.<sup>155</sup>

## **VI. THE PROPOSED BAN ON ARBITRATION CLAUSES IS UNLAWFUL**

We have discussed the proposed rules’ legal shortcomings in detail in our opening comments (at 87-118) and above. We here add several points on one specific issue: the proposed ban on arbitration clauses.

As many commenters explain,<sup>156</sup> the NPRM’s proposal (at ¶ 274) to prohibit arbitration clauses in contracts for broadband services would violate the Federal Arbitration Act (“FAA”).<sup>157</sup> Congress enacted that statute to “embody a national policy favoring arbitration”<sup>158</sup> because it recognized that arbitration “‘is usually cheaper and faster than litigation; it can have simpler procedural and evidentiary rules; it normally minimizes hostility and is less disruptive of ongoing and future business dealings among the parties; [and] it is often more flexible in regard to scheduling of times and places of hearings and discovery devices.’”<sup>159</sup> To effectuate that national policy, the FAA compels enforcement of arbitration clauses absent a “contrary congressional command” in some other statutory scheme.<sup>160</sup>

---

<sup>155</sup> Even if Section 222(a) were an independent grant of authority—which it is not—the Commission has not established any factual basis to justify the NPRM’s proposed collection, retention, and deletion requirements.

<sup>156</sup> See, e.g., AT&T Comments at 114-15; Comcast Comments at 102-05; CCA Comments at 46-47; CTIA Comments at 55-59; Sprint Comments at 21-22; T-Mobile Comments at 55; Verizon Comments at 70-75.

<sup>157</sup> 9 U.S.C. § 1 *et seq.*

<sup>158</sup> *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 345-46 (2011) (brackets omitted).

<sup>159</sup> *Allied-Bruce Terminix Cos. v. Dobson*, 513 U.S. 265, 280 (1995) (quoting H. R. Rep. No. 97-542, p. 13 (1982)). Several commenters elaborate on these efficiencies and the extensive empirical support for them. E.g., Comcast at 105-07; CTIA at 50-53; Verizon at 76-78 (“Multiple studies have found that consumers obtain relief in arbitration at rates higher than they do in court.”).

<sup>160</sup> *Shearson/American Express Inc. v. McMahon*, 482 U.S. 220, 226 (1987).

Here, no provision of the Communications Act even addresses arbitration clauses, much less contains a “command” by Congress to override them in contracts for telecommunications services. The American Association for Justice nonetheless argues (at 6) that “Congress contemplated a private enforcement mechanism of violations in §§ 206 and 207” of the Communications Act.<sup>161</sup> That argument ignores controlling Supreme Court precedent, which holds that a statute’s creation of a cause of action is insufficient to establish a “congressional command” overriding the FAA.<sup>162</sup> AAJ is likewise wrong to argue (at 6) that such a command can be inferred from either Sections 201 or 222 of the Communications Act. Those provisions also say nothing about arbitration clauses, and the Supreme Court has held that when a statute “is silent on whether claims under the Act can proceed in an arbitrable forum, the FAA requires the arbitration agreement to be enforced according to its terms.”<sup>163</sup>

AAJ also asserts (at 6) that the FAA does not “preclude ... regulations that prevent a party from placing such provisions in their contracts in the first place.” That too is incorrect. No less than a court, an agency is bound by Congress’s policy choice in the FAA to promote

---

<sup>161</sup> 47 U.S.C. §§ 206, 207.

<sup>162</sup> *CompuCredit Corp. v. Greenwood*, 132 S. Ct. 665, 670 (2012) (“If the mere formulation of the cause of action in this standard fashion were sufficient to establish the contrary congressional command overriding the FAA, valid arbitration agreements covering federal causes of action would be rare indeed.”) (internal quotation and citation omitted).

<sup>163</sup> *Id.* at 673. Public Knowledge argues (at 33) that the Commission can prohibit arbitration clauses that preclude consumers from invoking the Section 208 administrative complaint process. The arbitration provision in AT&T Mobility’s customer agreement, however, allows consumers to bring claims under that process. See AT&T Wireless Customer Agreement, Section 2.2.1 (“This arbitration agreement does not preclude you from bringing issues to the attention of federal, state, or local agencies, including, for example, the Federal Communications Commission. Such agencies can, if the law allows, seek relief against us on your behalf.”), <https://m.att.com/shopmobile/legal/terms.wirelessCustomerAgreement.html>. See also Verizon Wireless Customer Agreement, *How do I resolve disputes with Verizon Wireless?*, section (1) (“YOU CAN ALSO BRING ANY ISSUES YOU MAY HAVE TO THE ATTENTION OF FEDERAL, STATE, OR LOCAL GOVERNMENT AGENCIES, AND IF THE LAW ALLOWS, THEY CAN SEEK RELIEF AGAINST US FOR YOU”), <http://www.verizonwireless.com/b2c/support/customer-agreement>.

arbitration absent a contrary congressional command in its governing statute.<sup>164</sup> Although AAJ cites various administrative bans on arbitration clauses in other statutory contexts, those orders in fact cut against AAJ because the relevant agencies all acted pursuant to clear statutory commands.<sup>165</sup> Again, the Communications Act contains no such command.

---

<sup>164</sup> See, e.g., *D.R. Horton, Inc. v. NLRB*, 737 F.3d 344, 355-62 (5th Cir. 2013) (overturning an NLRB order prohibiting an arbitration clause that had banned employees from pursuing class or collective actions, finding that the National Labor Relations Act (“NLRA”) contained no “Congressional command” about arbitration clauses and that there was no inherent conflict between the FAA and the NLRA’s purposes).

<sup>165</sup> The Military Lending Act, for example, prohibits arbitration clauses in certain consumer credit agreements with services members and expressly provides that “[n]otwithstanding section 2 of title 9 [the FAA], or any other Federal or State law, rule, or regulation, no agreement to arbitrate any dispute involving the extension of consumer credit shall be enforceable against any covered member or dependent of such a member, or any person who was a covered member or dependent of that member when the agreement was made.” 10 U.S.C. §§ 987(e)(3), (f)(4). The Dodd-Frank Act likewise directs the Consumer Financial Protection Bureau (“CFPB”) to study the use of arbitration clauses in contracts for consumer financial products or services and expressly authorizes the CFPB to adopt regulations that “prohibit or impose conditions or limitations on the use of an agreement between a covered person and a consumer for a consumer financial product or service providing for arbitration of any future dispute between the parties.” 12 U.S.C. §§ 5518(a) & (b).

## CONCLUSION

The Commission should reject the NPRM's proposals to the extent, and for the reasons, discussed in our opening comments and above.

Respectfully submitted,

James J.R. Talbot  
Gary L. Phillips  
David L. Lawson  
AT&T SERVICES INC.  
1120 20th Street, N.W.  
Washington, D.C. 20036  
(202) 457-3058

/s/ Jonathan E. Nuechterlein

Jonathan E. Nuechterlein  
Alan Charles Raul  
C. Frederick Beckner III  
Clayton G. Northouse  
SIDLEY AUSTIN LLP  
1501 K Street, N.W.  
Washington, D.C. 20005  
(202) 736-8000

July 6, 2016