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 VERIZON

William H. Johnson
Of Counsel

Karen Zacharia
Catherine M. Hilke
Verizon
1300 I Street, N.W. – Suite 400 West
Washington, D.C. 20005
(202) 515-2438

Scott H. Angstreich
Geoffrey M. Klineberg
Kellogg, Huber, Hansen, Todd,
Evans & Figel, P.L.L.C.
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
(202) 326-7900

Henry Weissmann
Munger Tolles & Olson, LLP
355 South Grand Avenue
35th Floor
Los Angeles, California 90071
(213) 683-9100

Counsel for Verizon

July 6, 2016

TABLE OF CONTENTS

Page

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 VERIZON[1]

EXECUTIVE SUMMARY

Verizon reiterates its support for the goal of maintaining a robust and consistent consumer privacy framework for all Internet participants. Consistent with the record here, if the Commission adopts any privacy and data-security rules specific to broadband providers, it should do so in a manner that is consistent with how the rest of the industry is regulated and that recognizes the sensitivity of the customer's data as the key in determining the appropriate level of protection. Verizon strongly believes that consumers will benefit most if a common set of standards protect consumers' data in a consistent manner, regardless of who has the data.

The comments filed in this proceeding confirm a consensus as to the core principles of any effective privacy regime on the Internet: transparency, customer choice, and data security. This view is shared by a large and diverse set of commenters including manufacturers, small and mid-size communications companies, innovative technology companies, advertisers, economists, as well as intergovernmental, consumer, business, and social justice organizations. The Federal Trade Commission ("FTC") staff has urged the Commission to avoid imposing specific

[1] In addition to Verizon Wireless, the Verizon companies participating in this filing are the regulated, wholly owned subsidiaries of Verizon Communications Inc. (collectively, "Verizon").

requirements on broadband providers "that would not generally apply to other services that collect and use significant amounts of consumer data."[2] In addition, the FTC has called on the FCC to follow the FTC's "longstanding approach, which calls for the level of choice to be tied to the sensitivity of data."[3]

Those commenters who support the Commission's proposed rules — as well as those few who argue that the rules should be expanded even further — have failed to provide any justification for applying unique (and especially burdensome) rules on broadband providers that are imposed on them alone and that are inconsistent with the standards that apply to other Internet companies. Moreover, they fail to recognize the substantial harm to competition and, therefore, to consumers that would result from extending the opt-in regime to ISPs' efforts to market their own services to their own customers. These commenters also ignore the First Amendment principle that the creation and dissemination of information to customers is protected speech, and make no claim, much less a showing, that the proposed restrictions advance *any* substantial or compelling government interest in a narrowly tailored way.

The commenters supporting the Commission's lead proposal, or more extreme ones, also fail to square their arguments with section 222 or to justify them under any other statutory provision. They misread the text, structure, and history of section 222 — a statutory provision regulating a telecommunications provider's "customer proprietary network information" — in their zeal to confer on the Commission broad authority over *all* customer information that broadband providers receive.

---

[2] FTC's Bureau of Consumer Protection Staff Comments ("FTC Staff Comments") at 8.

[3] *Id.* at 23.

The record also reveals strong support for the Commission to adopt a reasonable, flexible framework for data-breach notifications and data security that will provide consumers with the information they need about potentially harmful breaches without over-notifying them. The Commission should therefore reject various proposals to expand the rules regarding breach notifications. In addition, Verizon supports reasonable and flexible data-security procedures for providers' customer information; prescriptive data-security regulations that create a one-size-fits-all approach will divert limited resources away from the specific data-security issues that would matter most to consumers.

Finally, the record confirms that the Commission's proposal to ban arbitration provisions in customer contracts is unlawful under the Federal Arbitration Act. Those commenters supporting the Commission's proposal fail to explain why such a ban would promote consumer welfare, particularly in light of the substantial benefits that consumers obtain from the best practices that Verizon and others have adopted to make the arbitration process more consumer friendly.

I. THERE IS WIDESPREAD SUPPORT FOR BROADBAND PRIVACY RULES THAT MIRROR THOSE THAT APPLY TO THE REST OF THE INTERNET ECOSYSTEM

A large and diverse group of commenters, including the staff of the FTC, urge the Commission to adopt an approach to customer privacy that is consistent with the well-established regime that has applied to all participants in the Internet ecosystem — from ISPs to edge providers.[4] For example, the National Association of Manufacturers argues that "[c]reating

[4] *See*, *e.g.*, FTC Staff Comments at 8 (labeling as "not optimal" the imposition of "a number of specific requirements on the provision of [broadband provider] services that would not generally apply to other services"); American Commitment Comments at 3 ("At a minimum, the rule should be completely rewritten to conform to the FTC approach."); Consumer Technology Ass'n Comments at 11-12 ("The Commission should instead take a page from the FTC's playbook, which has been successful in assuring strong consumer privacy and other

a new and duplicative regulatory regime at a time when a consistent regulatory framework across the entire internet ecosystem is needed will lead to an undue burden on our nation's telecommunications providers."[5] And the Association of National Advertisers "does not believe that the FCC needs to impose a new privacy regulatory framework on a system that is working effectively" and that the Commission's proposal "is antithetical to FTC precedent carefully developed and enforced for decades."[6] As Verizon explained in its opening comments, a technology-neutral approach that requires the same consumer safeguards regardless of the entity

---

protections without inhibiting industry's flexibility to innovate."); ITTA Comments at 14 ("Unless there is a very good reason to depart so completely from the privacy framework that guides and is applied to virtually all other businesses in the nation, it stands to reason that this Commission should defer to the FTC's experience and expertise in this area — or, at a minimum, adopt a similar, consistent approach."); LocationSmart Comments at 2 ("We believe it is important that the rules put in place by the Commission be as consistent as possible with, if not identical to, those already in place for the plethora of internet and mobile applications utilizing location information under Federal Trade Commission (FTC) and other local and federal regulations. Establishing a new set of rules that results in disparate user experiences, privacy policies and terms of use will only confuse end users and stifle innovation."); ADTRAN Comments at 10 (urging the Commission to "adopt[ ] privacy regulations and guidelines that more closely track the FTC regulation that has worked well for customers, for edge providers, and for [broadband] providers before the *Open Internet Order*'s re-classification of [broadband] as a Title II service"); The Internet Ass'n Comments at 4 ("The FTC's existing data privacy and security enforcement framework provides strong consumer protections, and there is no need for the FCC to impose regulations that duplicate, displace, or 'supplement' that framework."); MediaFreedom Comments at 4 ("MediaFreedom urges the Commission to abandon its heavy-handed, 'traditional' approach to privacy and security protection and align its practices and actions with the FTC instead. The FTC's model has worked admirably for consumers and the Internet ecosystem these past two decades. The FCC would do well not to 'fix' what isn't broken."); CALinnovates Comments at 2 ("[T]he FCC should adopt a set of privacy rules mirroring the time-tested approach that guides the Federal Trade Commission's (FTC) enforcement actions."); James C. Cooper (George Mason University School of Law) Comments at 8 ("Cooper Comments") ("[T]he FCC should abandon the prescriptive rules in the NPRM, and instead adopt a harm-based standard fashioned after the FTC's approach to consumer protection."); Roslyn Layton (American Enterprise Institute) Comments at 11 ("The proposed privacy regulations are falling on heavily regulated broadband providers — and wresting the enforcement function from the capable and relevant agency, the FTC.").

[5] National Ass'n of Manufacturers Comments at 1.

[6] Ass'n of National Advertisers Comments at 20.

that collects the data would provide consumers a consistent level of protection across the Internet, while being flexible enough to meet the demands of a constantly evolving marketplace.[7] Moreover, the Commission has authority to adopt such a regime under section 222, because the statutory terms "protect the confidentiality of proprietary information" (section 222(a)) and "the approval of the customer" (section 222(c)(1)) are sufficiently ambiguous that the Commission can reasonably interpret section 222 to establish a privacy regime that varies based on the sensitivity of the information at issue.[8]

The Internet ecosystem is paid for largely through advertising, and striking an appropriate balance that allows the use and disclosure of some customer information while protecting the most sensitive information is critical.[9] But as the Future of Privacy Forum explained in its

---

[7] *See* Verizon Comments at 6-24. We note that the European Commission has sought public comment on the efficacy of its e-Privacy Directive (2002/58/EC), which imposes sector-specific privacy regulations in addition to generally applicable privacy laws. On July 5, 2016, a large number of stakeholders — a group of 12 different industry associations, representing a broad cross-section of industry — issued a statement calling upon the European Commission to repeal the outdated, telecom-specific e-Privacy Directive and instead to rely on the framework that applies a consistent approach to all companies. *See* Joint Industry Statement, *Empowering Trust and Innovation by Repealing the e-Privacy Directive* (July 5, 2016), *available at* https://etno.eu/newsletters/preview?m=1164 ("We believe that simplifying and streamlining regulation will benefit consumers by ensuring they are provided with a simple, consistent and meaningful set of rules designed to protect their personal data.").

[8] *See* Letter from William Johnson, Verizon, to Marlene H, Dortch, FCC (July 5, 2016).

[9] *See* Ass'n of National Advertisers Comments at 18-19 ("[A]ny requirements regarding data collection and use should carefully take into account the sensitivity of information. In this regard, it is worth emphasizing that a vast amount of marketing data, even if potentially personally identifiable, is not sensitive data and is highly unlikely to be used to harm consumers in any way."); *see also* Deepfield Networks Comments at 6 ("[L]egitimate concerns for consumer control over their personal information must be balanced against the unique needs of [broadband] providers and service providers. Well-crafted privacy protections should not hinder [broadband] providers' ability to supply quality service and continue to innovate better and safer ways to deliver information over the Internet."); Internet Commerce Coalition Comments at i ("Any rules adopted by the Commission should reflect the varying sensitivity of individual data elements and the well-established FTC 'respect for context' principles, including as they apply to advertising to a business' own customers without disclosing personally identifying information

comments, it makes no sense for the Commission to propose an opt-in approach for virtually all customer information when held or used by broadband providers when most of the same data is shared broadly throughout the rest of the Internet ecosystem under an opt-out framework.[10] Standards for choice and transparency that change depending on how consumers access the Internet or what websites they visit will confuse, exhaust, and frustrate them.[11] In contrast, establishing a consistent framework that ensures that an individual's data will be treated the same regardless of what company possesses it will protect consumer choice while avoiding the creation of "artificial barriers to either competition or innovation."[12]

II. COMMENTERS SUPPORTING HEIGHTENED REGULATION OF BROADBAND PROVIDERS FAIL TO PROVIDE ANY RATIONALE FOR SINGLING THEM OUT FOR UNIQUELY BURDENSOME REGULATION

A. The Commission's Opt-In Proposal Will Cause Consumer Harm

Some commenters have argued for imposing a regulatory regime on broadband providers that would require them to obtain opt-in consent for *any* use of information (even non-sensitive

---

to third parties, in order to avoid significant potential unintended consequences and unnecessary costs.").

[10] Future of Privacy Forum Comments at 30 ("[T]he proposed Opt In has a cost: here, that cost is the exclusion of ISPs from a much larger market."); *see also* Hance Haney (Discovery Institute) Comments at 3 ("The Commission has an obligation to set out why, from a consumer perspective, it's a materially more significant privacy threat for broadband service providers to know 'what websites a customer has visited,' at what hours of day, from what location using which type of device than it is for a search engine to view search terms and click-throughs.") (footnote omitted).

[11] *See* Multicultural Media, Telecom and Internet Council *et al.* Comments at 3 (urging the Commission "to harmonize its approach with the Federal Trade Commission ('FTC') to minimize consumer confusion"; "[a]gainst this background, the Commission should not depart from the groundwork laid by other privacy experts in government and elsewhere").

[12] J. Howard Beales III (George Washington School of Business) Comments at 2 ("Beales Comments").

information) beyond what is necessary to provide the subscribed services themselves.[13] But Verizon agrees with the FTC staff that opt-in should be reserved for sensitive information "because the more sensitive the data, the more consumers expect it to be protected and the less they expect it to be used and shared without their consent."[14]

Moreover, as the submissions of multiple economists and other experts demonstrate, an overly broad opt-in model is flawed and harmful to consumers for a host of reasons, including: (1) it ignores the consumer and societal benefits of more relevant advertising; (2) it skews consumers' consent calculation and imposes unnecessary and inefficient transaction costs; and (3) it distorts competition for digital advertising and entrenches the market power of the leading advertisers, which would not be subject to the Commission's proposed rules.

1. Personalized Advertising Benefits Consumers

Commenters favoring a rigid opt-in approach to consumer consent fail to acknowledge — much less grapple with — the many benefits (to both consumers and businesses) of personalized digital advertising. As the President's Council of Advisors on Science and Technology stated, data-driven digital advertising is "near-ubiquitous" and "fuel[s] an increasingly important set of economic activities."[15] Consumers have come to expect to "pay" for the many "free" services they receive by providing access to their information. As Thomas Lenard and Scott Wallsten of

[13] *See, e.g.*, Free Press Comments at 13; ACLU Comments at 8; Consumer Action Comments at 2; Online Trust Alliance Comments at 2; Privacy Rights Clearinghouse Comments at 4.

[14] FTC Staff Comments at 21.

[15] President's Council of Advisors on Science and Technology, Executive Office of the President, *Big Data and Privacy: A Technological Perspective* at x (May 2014), *available at* https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

the Technology Policy Institute have observed, "most consumers are willing to trade information for something useful to them."[16]

Consumers benefit from this personalized advertising in multiple ways.

First, consumers get the benefit of free or discounted online goods and services. By providing the means for advertisers to target ads that consumers are more likely to appreciate, broadband providers facilitate the provision of free services. The Internet landscape would look fundamentally different if the use of personal data were curbed or eliminated. Consumers have readily embraced this model, as evidenced by the fact that the use of social networks, mobile apps, and other online services has grown exponentially. According to Lenard and Wallsten, "the purpose of obtaining information about consumers is to provide them with targeted advertising — advertising of products likely to be of use to them — as well as with services, such as free search and email."[17] And Professor James C. Cooper of the George Mason University School of Law noted that empirical evidence shows consumers "generally are comfortable with the tradeoffs of data for content and lower prices."[18] Professor Cooper further noted that, while sharing on social media has exploded in popularity among online adults, "very few people bother to opt-out of online tracking or adopt privacy-protecting technology."[19]

Second, one result of using customer data is that consumers receive more tailored and relevant advertising suited to their interests and needs, which in turn fuels the creation of new and socially beneficial digital innovation and platforms. Because the $200 billion digital

---

[16] Thomas Lenard, President and Senior Fellow, and Scott Wallsten, Vice President for Research and Senior Fellow, Technology Policy Institute, *An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking* 26 (May 2016) ("Lenard and Wallsten Comments").

[17] *Id.*

[18] Cooper Comments at 4.

[19] *Id*. at 4-5.

advertising industry[20] is the lifeblood of the Internet, consumers will encounter digital advertising regardless of the Commission's default consent regime. According to Professor J. Howard Beales III of the George Washington School of Business, "[c]onsumer data and feedback also enable[ ] the increased customization and personalization of online experiences and offerings for consumers, which is helping to fuel growth in broadband usage and e-commerce. The Commission should not risk undermining these numerous benefits without clear evidence of a problem that needs to be solved."[21] Similarly, Lenard and Wallsten noted that "[a]dvertising revenues — and targeted advertising in particular — have played a key role in supporting new online services, which are often provided to consumers free of charge. Perhaps the most prominent example is the search engine, which would likely not exist as we know it were it not for the ability of Google and others to develop new sources of revenue based on targeted advertising."[22]

Nor is advertising the only socially beneficial use of consumer data. Lenard and Wallsten explained that Netflix uses customer data in developing original content and it "can also be used to improve algorithms, protect against security threats, and notify buyers of a product of important recalls, to name but a few."[23]

In light of the ubiquitous use of consumer data by all types of "large platform"[24] providers, economists noted it is inappropriate to single out broadband providers for special heightened regulation — particularly given the lack of evidence that broadband providers have

---

[20] *See* Lenard and Wallsten Comments at 30.

[21] Beales Comments at 3.

[22] Lenard and Wallsten Comments at 5.

[23] *Id.*

[24] *Id.* at 9.

unique access to customer data or are more susceptible to data breaches.[25]

2. The Opt-In Default Imposes Costs on Consumers and Businesses Without Offsetting Benefits

The record also demonstrates that the Commission's proposed opt-in approach would ignore and obscure the many benefits of data-sharing, while imposing on consumers and businesses unnecessary and inefficient transaction costs.[26]

The privacy regime that applies to all other actors in the Internet ecosystem is premised on an opt-out model of consent, except for the most sensitive data. This opt-out model predominates across the Internet economy, including with social networks, search engines, email services, and mobile applications.[27] Professor Joshua D. Wright has noted that the Commission's proposed opt-in model "myopically focuses upon advancing a single value — privacy — without considering the economic costs that decision imposes on consumers and without apparent consideration of other important values such as prices, innovation, and competition."[28]

In practical terms, the choice of default (whether opt-out or opt-in) makes a huge difference. To illustrate, Lenard and Wallsten cited the popular book *Nudge*, in which Richard Thaler and Cass Sunstein argued that "humans will often consider required choice to be a nuisance or worse, and would much prefer to have a good default . . . . When choice is

---

[25] *See id.* at 7-14; Beales Comments at 2 ("The FCC offers *no* evidence of *any* inadequacies in [the current] privacy regime."); *id.* at 3-8; Cooper Comments at 2-4 ("Not only does the NPRM fail to articulate a theory of privacy harm, more importantly, it also lacks *any* empirical evidence that [broadband] providers' conduct is harming consumers.").

[26] *See*, *e,g.*, Lenard and Wallsten at 5-6; Joshua D. Wright, University Professor, Antonin Scalia Law School at George Mason University, *An Economic Analysis of the FCC's Proposed Regulation of Broadband Privacy* at 10-28 (May 27, 2016) ("Wright Comments"), attached to Letter from Jonathan Banks, US Telecom, to Marlene H. Dortch, FCC (May 27, 2016).

[27] *See* Wright Comments at 13.

[28] *Id.* at 10-11.

complicated and difficult, people might greatly appreciate a sensible default."[29] Here, according to Lenard and Wallsten, "efficiency argues for giving the initial right to businesses — that is, for opt-out. If the default is opt-in, then information is lost — it does not flow to its highest-valued uses. This loss of information is costly and leads either to price increases as firms attempt to compensate for the loss of information or elimination of services."[30]

According to Professor Beales, "[w]ith privacy preferences, the most important cost of exercising choice may well be the cost of considering the issue at all."[31] The costs of reading privacy policies are significant, and, for consumers, it is often not worth their time. "The default rule is therefore likely to dominate choices. If the default is no sharing, most consumers will end up not sharing."[32] And "not sharing" — the "path of least resistance"[33] under the Commission's proposal — has potentially significant consequences for the Internet economy, for it is likely to raise costs and distort the market for Internet advertising. Indeed, Professor Wright noted that "consumers tremendously value the advertising model that dominates the Internet today and that is largely based on opt-out consent," yet the Commission's proposed rules would undermine this model, "inflict costs on both ISPs and consumers, raise retail prices, and deter the information uses that are vital to the success of the Internet ecosystem."[34]

---

[29] Lenard and Wallsten Comments at 25 (alteration in original).

[30] *Id.* at 26 (footnote omitted).

[31] Beales Comments at 11.

[32] *Id.* (footnote omitted).

[33] Wright Comments at 14 ("[F]or many consumers, it is simply not worthwhile to incur the transaction costs of opting in — devoting time and attention to understanding a privacy policy's implications and taking the steps necessary to provide the required consent . . . . In those circumstances, most consumers will simply take the path of least resistance and make no decision at all — thereby failing to opt in by default under the NPRM's scheme.").

[34] *Id.* at 15-16; *see id.* at 16-20 (explaining costs and inefficiencies associated with Commission's proposed opt-in scheme).

Moreover, these experts identified other drawbacks and irregularities with the Commission's proposed opt-in regime. As Professor Beales noted, the Commission's proposed rules do not "protect information, but instead protect[ ] a *certain channel* for obtaining information," i.e., mass-market broadband Internet.[35] This crucial distinction will confuse consumers by creating a false understanding if consumers decline to opt in to the sharing of data by their broadband providers, they are likely to believe their information will not be collected and shared (at least while using the broadband service). But that is not true. "In fact, . . . the same information will be used by other participants in the Internet ecosystem, because it is not uniquely in the hands of the [broadband] provider."[36] Professor Beales continued: "In this regard, the presumed 'extra protection' of an opt-in rule is an illusion. Consumers who do not opt in prevent the broadband provider's use of that information. To prevent others from using the information, they have to do what they do now — opt out at each of the entities (or a centralized opt out mechanism like the Digital Advertising Alliance) that may have access to the information."[37]

3. The Opt-In Default Would Impede Competition in Digital Advertising

Commenters also demonstrate that the Commission's proposed opt-in system — which would apply *only* to broadband providers and *not* to other major players in the Internet economy — would distort and impede the competitive marketplace for digital advertising. The Commission's proposed rules would operate against the backdrop of a heavily concentrated online advertising industry. "Online advertising continues to remain concentrated with the 10

[35] Beales Comments at 10 (emphasis added).

[36] *Id.* at 10.

[37] *Id*. at 11.

leading ad-selling companies . . . account[ing] for 75% of total revenues in Q4 2015."[38] None of those top 10 Internet advertisers is a broadband provider; accordingly, they would not be subject to the Commission's proposed opt-in rules.

The Commission's proposal to create a "separate regulatory regime for broadband providers" would "inadvertently create or perpetuate market power in one or more sectors of the market," according to Professor Beales.[39] In particular, the Commission's rules would raise barriers to broadband providers entering this marketplace, by applying heightened rules that do not apply to the leaders in the digital advertising space — including the search engines and social networking sites that enjoy the bulk of digital display ad revenues. Not only would it raise broadband providers' costs as compared to their rivals, but it may make it impractical for broadband providers to compete at all if only a small percentage of customers provide opt-in consent. "Because it protects the less regulated firms from actual or potential competition, the proposed regulation can be a source of monopoly power and its consequences of higher prices, lower quality, and less innovation."[40]

Lenard and Wallsten have similarly observed that the Commission's proposed rules would impede broadband providers' efforts to gain a foothold in the digital advertising market and challenge the entrenched leaders.[41] Thus, the "asymmetric nature of the rules" would "reduce competition and potential competition in the growing market for digital advertising,

---

[38] *IAB Internet Advertising Revenue Report: 2015 Full Year Results* at 11 (Apr. 2016), *available at* http://www.iab.com/wp-content/uploads/2016/04/IAB-Internet-Advertising-Revenue-Report-FY-2015.pdf.

[39] Beales Comments at 8.

[40] *Id*.

[41] *See* Lenard and Wallsten Comments at 35.

potentially harming the businesses that rely on advertising to reach consumers for their products."[42]

B. The Commission Should Not Impose Special Rules for Sharing Information with Affiliates and Contractors

As Verizon and other commenters explained, broadband providers should be permitted to share customer information with affiliates and contractors if the provider (1) provides clear and transparent notices about how customer information may be used; (2) ensures that their affiliates and contractors use customer information in accordance with the choices the customer has made; (3) ensures that the affiliates and contractors secure the information appropriately; and (4) provides any required notices in the unlikely event of a breach.[43] Such sharing should be permitted based on inferred approval.

Broadband providers frequently use various affiliates and contractors to perform functions associated with providing broadband Internet access service as well as to enable advertisers to serve more relevant ads to consumers, whether for convenience, to comply with financial reporting requirements, or out of necessity.[44] For example, the broadband provider may rely on one affiliate or contractor to conduct billing for broadband service and may rely on another affiliate or contractor to market the service. And, even if they don't, broadband providers themselves have the obligation and the incentive to respect their customers' choices with respect to their information and will remain responsible should any issues arise.[45] Requiring opt-in or

---

[42] *Id.* at 31.

[43] *See* Verizon Comments at 26-28; T-Mobile Comments at 32; Comcast Comments at 50; CTIA Comments at 132-33.

[44] *See, e.g.*, Verizon Comments at 26-27; NTCA Comments at 12 (affiliates); Cincinnati Bell Telephone Company Comments at 14 (contractors); T-Mobile Comments at 32-33 (contractors); Comcast Comments at 87-89 (contractors).

[45] *See* Verizon Comments at 27.

opt-out consent to share customer information with affiliates or contractors will therefore simply increase the costs of operations for providers, as broadband providers are forced to structure or restructure their businesses inefficiently to comply.

These burdens on broadband providers are unwarranted in light of the fact that consumers are accustomed to and understand that companies also have many affiliates and a consistent level of protection will apply regardless of the affiliate or contractor involved.[46] Consumers have received bundled services from broadband providers for many years.[47] Indeed, consumers frequently receive marketing communications from edge providers and non-Internet businesses for their affiliates' services.[48] There is no evidence in the record indicating that consumers want or need opt-in or opt-out approval before their information can be shared with affiliates.[49]

As Verizon and other commenters note,[50] the Commission's restrictive proposal also is inconsistent with other federal laws, which require that corporate affiliates and contractors *not* be treated as third parties, including the Gramm-Leach-Bliley Act.[51] Even the Commission's voice CPNI rules permit CPNI to be shared with agents on an opt-out basis.[52] There is no justification for treating broadband data differently than these other similar types of data.

---

[46] *See, e.g.*, T-Mobile Comments at 32.

[47] *See* CTIA Comments at 132; NTCA Comments at 47; Comcast Comments at 49-50.

[48] *See* Verizon Comments at 24.

[49] *See id.* at 27 (pointing out that the broadband provider has the obligation and incentive to ensure that the data is used by the affiliate according to the customer's choice, because the broadband provider will be responsible if a mistake is made); *see also* Comcast Comments at 92.

[50] *See, e.g.*, Verizon Comments at 27; Comcast Comments at 88.

[51] *See* 15 U.S.C. § 6802(b)(1) (prohibiting a financial institution from disclosing "nonpublic personal information" only to a "nonaffiliated third party," unless the consumer opts out).

[52] *See* Comcast Comments at 88.

Nevertheless, certain commenters urge the Commission to require opt-in consent before a provider can share customer information even with affiliates, claiming that the Communications Act requires opt-in consent[53] and that opt-in better conforms to consumer behavior and preferences.[54] Neither argument has merit.

First, the Tenth Circuit has already held that opt-in consent is not required in every instance.[55] The court correctly concluded that the Commission had failed adequately to consider the less restrictive opt-out approach and rejected as mere speculation the Commission's assumption that individuals who care about their privacy would not bother to opt-out if given notice and the opportunity to do so.[56] In addition, section 222(f) of the Communications Act[57] states that opt-in consent for using or disclosing CPNI is only required by statute for the use or disclosure of precise geo-location information and automatic crash notification information. Section 222(f) would not make any sense if section 222 always required express, opt-in approval. A customer's consent may therefore be provided through either implied consent or opt-out consent except for those listed in section 222(f). Thus, the Commission has never accepted that opt-in consent is required for all use or disclosure of CPNI. Even in the *1998*

---

[53] *See, e.g.*, Public Knowledge *et al.* Comments at 31; Free Press Comments at 13; New America's Open Technology Institute Comments at 39.

[54] *See, e.g.*, Public Knowledge *et al.* Comments at 31; Access Now Comments at 9; Privacy Rights Clearinghouse Comments at 4-5; Electronic Frontier Foundation Comments at 9; Center for Digital Democracy Comments at 18.

[55] *See U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1238-39 (10th Cir. 1999) (vacating a Commission order regarding CPNI because it did not consider whether opt-out consent would also meet the Commission's interests); *see also National Cable & Telecomms. Ass'n v. FCC*, 555 F.3d 996, 998-99 (D.C. Cir. 2009) (describing implied consent, opt-out consent, and opt-in consent regimes).

[56] *See U.S. West*, 182 F.3d at 1238-39.

[57] 47 U.S.C. § 222(f).

CPNI Order[58] that the Tenth Circuit vacated, the Commission permitted the use or disclosure of CPNI to market products to customers who already subscribed to that category of products on an implied-consent basis.[59]

Second, customers understand and expect that their data will be shared with a company's various affiliates and contractors. As noted above, customers have benefited from bundled services for years and frequently interact with edge providers' affiliates.[60] Rather, commenters are concerned that "companies can qualify as 'affiliates' with virtually no obvious connection to a customer's known provider."[61] But this concern can be solved with clear and transparent notices to customers about exactly how their data will be shared, as Verizon proposed in its initial comments.[62]

Finally, the Commission should also reject the proposal made by the Center for Digital Democracy[63] to require ISP affiliates to obtain opt-in consent before marketing *their own services*. Of course, to the extent an ISP affiliate provides services that are *not* telecommunications services, the Commission's authority under section 222 does not extend that far. In any event, an ISP affiliate that is not a telecommunications provider would remain subject

---

[58] Second Report and Order and Further Notice of Proposed Rulemaking, *Implementation of the Telecommunications Act of 1996*, 13 FCC Rcd 8061 (1998).

[59] *See U.S. West*, 182 F.3d at 1230.

[60] *See* CTIA Comments at 132; Verizon Comments at 24.

[61] Electronic Frontier Foundation Comments at 9; *see also* Privacy Rights Clearinghouse Comments at 4-5 ("In many, if not most, cases a consumer will have a difficult time determining a [broadband] provider's affiliates as well as the extent to which affiliate sharing occurs. As the FCC notes, affiliates may have completely different branding and provide completely different services from the [broadband] provider with whom the customer has a relationship.") (footnote omitted); Center for Digital Democracy Comments at 18 ("We do not believe common branding works, given how the digital market works today.").

[62] *See* Verizon Comments at 27.

[63] Center for Digital Democracy Comments at 18.

to the FTC's privacy regime, where opt-in consent is generally required only for the use or disclosure of sensitive customer information such as social security numbers and health, financial, children's, or precise-geolocation data.[64]

In sum, if broadband providers provide clear and transparent notices to their customers about how their information may be used and ensure that affiliates and contractors respect the choices their customers have made regarding the use of their information, appropriately secure it, and provide any required data-breach notices, broadband providers should be permitted to share customer information with those affiliates and contractors on an implied-consent basis.

C. The Commenters Who Support the FCC's Opt-In Regime and Those Who Argue for Expanding It Ignore the Limitations Imposed by the First Amendment

Requiring opt-in consent for everything other than the narrowly defined "communications-related services" violates the First Amendment: it would prohibit broadband providers from obtaining customers' consent using even clear, conspicuous, and fair opt-out notices, "an obvious and substantially less restrictive alternative" to opt-in consent.[65] Moreover, the proposed rules go far beyond selling or sharing information with unaffiliated third parties. The proposed rules apply to wholly internal use of information within an ISP. As Professor Tribe points out, because "opt-in would be required before a broadband ISP could disclose information to an affiliate for non-communications-related services *even if the affiliate does not*

[64] *See* FTC Staff Comments at 19-20.

[65] *U.S. West*, 182 F.3d at 1238; *see* Verizon Comments at 37-40; Laurence H. Tribe & Jonathan S. Massey, *The Federal Communications Commission's Proposed Broadband Privacy Rules Would Violate the First Amendment* at 12 (May 27, 2016) ("Tribe White Paper") (recognizing that "an opt-in consent requirement that 'merely' *burdens* (rather than explicitly prohibits) speech remains subject to heightened constitutional scrutiny"), attached to Letter from Thomas C. Power, CTIA, Rick Chessen, NCTA, and Jon Banks, US Telecom, to Marlene H. Dortch, FCC (May 27, 2016).

actually use the data," such a requirement "fails to meet the requirement of *Central Hudson* that the restriction on speech be tailored to the asserted governmental interest" in preventing disclosure of sensitive or personal information.[66]

The commenters that argue that the Commission's proposed rules are too permissive — and urge the Commission to require opt-in consent for *every* disclosure or use beyond what is required to provision the subscribed service[67] — fail even to acknowledge, much less to confront, the serious limitations that the First Amendment imposes on regulation in this area. If the Commission's proposed rules fail to satisfy the relevant test because they do not "directly advance[ ] a substantial governmental interest" and are not narrowly "drawn to achieve that interest,"[68] the proposal to extend the opt-in consent requirement even further is clearly unconstitutional. The choice of an opt-in regime does not promote the Commission's "core" privacy principles of choice and transparency,[69] and it does not advance these interests any more than a well-designed opt-out regime would.

None of the commenters supporting the Commission's opt-in proposal (and certainly none who advocates extending it) explains why a well-crafted, clear, and conspicuous opt-out notice would not give customers "*the opportunity* to affirmatively choose how their information is used."[70] The Commission's proposed rules would prohibit broadband providers not just from

---

[66] Tribe White Paper at 29.

[67] *See, e.g.*, Consumer Action Comments at 2; Center for Digital Democracy Comments at 16; Consumer Watchdog Comments at 5.

[68] *See* Verizon Comments at 37 (quoting *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 572 (2011)); *accord Greater New Orleans Broad. Ass'n, Inc. v. United States*, 527 U.S. 173, 188 (1999).

[69] NPRM ¶ 5.

[70] *Id.* ¶ 127 (emphasis added).

obtaining customers' consent through unfair or deceptive means; it would prohibit them from using even *clear, conspicuous, and fair* opt-out notices to obtain customer consent. This plainly violates the First Amendment. Just as many edge providers have adopted opt-in regimes for sharing some sensitive information, so, too, have broadband providers.[71] This only emphasizes how much extending the opt-in consent requirement would restrict more speech than necessary to accomplish the Commission's goals.

D. The Commission Should Reject Certain Proposals That Are Clearly Unsound

Although most commenters supporting the Commission's proposed rules have done little more than repeat the Commission's own attempted justifications, a few have gone further and made arguments that are particularly problematic and unsupported. Verizon briefly responds to them here.

1. Deep-Packet Inspection Should Not Be Banned Categorically and Is Not Necessary To Implement a Sensitivity-Based Approach to Consent

The Commission has defined "deep-packet inspection" broadly to include any inspection of packets beyond looking at the top-level domain name, even if the substantive contents of the packets are not reviewed.[72] As Verizon has already explained, there is no justification for preventing broadband providers — and only broadband providers — from using particular technologies. There is no reason for a categorical ban — indeed, many uses of deep-packet inspection are affirmatively beneficial, such as fighting spam, facilitating new services, and identifying child pornography. Where customers are given notice about a broadband provider's practices and a fair opportunity to consent, such practices are reasonable.

---

[71] *See* Verizon Comments at 40.

[72] *See* NPRM ¶ 264.

Public Knowledge argues that implementing an approach to privacy that turns on the sensitivity of the data "is not feasible, as it would necessarily require ISPs to first determine whether sensitive information is present in any given communication — a task necessarily requiring *manual inspection of each packet — before* applying the appropriate amount of protection."[73] There are several problems with this argument.

First, as Verizon has already explained, there is nothing inherently dangerous or problematic with deep-packet inspection.[74] There is certainly no reason why broadband providers should be subject to a unique prohibition on the use of a technology when equivalent technologies are routinely used by other companies. Indeed, certain edge providers' practices, like scanning content of messages or search results, provide similar access to this type of information. So long as ISPs provide their customers with notice about their practices and a fair opportunity to consent to those practices, there is no reason to prohibit deep-packet inspection.

Second, Public Knowledge is wrong that deep-packet inspection is necessary in order to implement a choice regime that turns on the sensitivity of the information at issue. Much of the information that is used for both marketing and advertising purposes does not require deep-packet inspection. This includes data ranging from customer interests (e.g., sports fan or dog owner) purchased from third parties to precise geo-location information. While the latter data is certainly sensitive — and the former is not — deep-packet inspection has nothing to do with applying a choice regime that varies based on the sensitivity of the information at issue.[75] It is

---

[73] Public Knowledge *et al.* Comments at 24.

[74] *See* Verizon Comments at 42-43.

[75] Even where information is obtained from the contents of the packets themselves, providers are capable of protecting and refraining from using highly sensitive information, such as medical data. Indeed, looking at the packets is not substantively different from what edge providers do when they review the contents of emails or posts for the purpose of targeting advertisements. For example, advertisers can now apparently target advertisements to Twitter

also possible to define categories that reflect the sensitivity of the information and employ a targeted opt-in where needed. For example, the FTC has defined "sensitive" information to include precise location information and health, financial, and children's information. Ensuring that sensitive data is protected — and that the disclosure or use of such information for purposes other than the provision of service and the protection of the network is subject to opt-in consent — is the important point; the technology used to obtain that data should not matter, so long as the customers' informed choice is respected.

2. Broadband Providers Should Be Permitted To Employ Device Identifiers No Differently Than Every Other Participant in the Internet Ecosystem

Advertising is the essential engine of the Internet ecosystem, and the use of identifiers is already a practice used widely. Device identifiers permit marketers to target advertisements that are more likely to be useful for consumers, and they are, therefore, more valuable to potential advertisers, in a way that protects the customer's privacy. As Verizon has already explained, prohibiting broadband providers from doing what edge providers and mobile operating system manufacturers already do will simply mean that competition in the marketplace for Internet advertising will be lessened as broadband providers cannot compete on a level playing field with the dominant players that will continue to use advertising identifiers. This will harm consumers, depriving website and app developers of essential revenue to keep innovating and providing the services that customers enjoy.

---

users based on the emojis they use. *See* https://www.engadget.com/2016/06/15/now-advertisers-can-target-users-who-tweet-a-certain-emoji/ ("In other words, use the pizza emoji in a tweet and expect an ad from Dominos or someone similar coming your way soon.").

Some commenters insist that broadband providers should be prohibited from using device identifiers, such as the UIDH, claiming that they constitute unjust and unreasonable practices.[76] Yet they offer no explanation for this position, alleging incorrectly that these identifiers "facilitate collection of extensive information about [ISP] customers without customers' knowledge, and are not easily defeated by customers."[77] As Verizon explained, however, its UIDH is not used by Verizon for the collection of any data, nor does it reveal any personally identifiable information. Verizon also limits the sharing of such identifiers to its own affiliates. They would only be shared with third parties with a customer's opt-in consent.[78] And Verizon provides a means for consumers to choose not to participate in its advertising programs, which includes opting out of the UIDH. Customers can, therefore, easily avoid the insertion of these device identifiers.

3. The Commission Should Reject the Proposal To Require Disclosure of Methods Used To Aggregate and De-Identify Customer Data

As Verizon has already explained, broadband providers should be permitted to use and, in appropriate circumstances, share de-identified customer information.[79] So long as appropriate guidelines are followed, de-identified data does not pose the same privacy risks to consumers as the use or sharing of identified data. Indeed, there is no privacy risk to consumers if the data cannot be reasonably re-identified. So providers should be allowed to use and disclose de-identified data as long as the provider — and anyone it shares the data with — honors a consumer's choices prior to using that data in a way that would target the customer. And anyone

[76] *See, e.g.*, New America's Open Technology Institute Comments at 46.

[77] *Id.* at 45.

[78] *See* Verizon Comments at 42.

[79] *See id.* at 44-45.

with whom the provider shares such de-identified data should be prohibited from trying to re-identify it.

In its comments, the Electronic Frontier Foundation suggests that, in order to ensure that de-identified data is not "linkable" to specific customers or devices, "the Commission must add a transparency requirement that would force [broadband] providers, whenever they use a new method for generating aggregate customer PI, to disclose the details of that method to their customers (or preferably, directly to the public)."[80] Such a requirement would force broadband providers — and *only* broadband providers — to disclose their proprietary business methods to their competitors, further undermining competition in the digital advertising market. Moreover, it could be both counterproductive and affirmatively harmful for broadband providers to disclose their aggregation and de-identification methodologies: doing so could provide a useful roadmap for identity thieves and other disreputable entities in their efforts to re-identify the customer data. There is no evidence that the Electronic Frontier Foundation's suggestion would solve any actual problem and yet there is reason to believe that it would make matters considerably worse. The Commission should reject this proposal.

III. THE PROPOSED RULES, AND OTHER MORE EXTREME PROPOSALS, WOULD VIOLATE THE STATUTE

A. Those Commenters Who Claim That Section 222(a) Confers Broad Authority To Regulate the Use and Disclosure of Non-CPNI Misread the Text, Structure, and History of Section 222

With respect to the use and storage of customer information, section 222 — the only provision of the Communications Act that specifically governs telecommunications providers' use and storage of that information — is limited to CPNI. As Verizon[81] and numerous other

[80] Electronic Frontier Foundation Comments at 14.

[81] *See* Verizon Comments at 53-60.

commenters[82] have shown, the text, structure, and legislative history of section 222 all demonstrate that CPNI is the *only* type of customer information subject to regulation. Before section 222 was enacted, the Commission regulated only the use of CPNI and only by the BOCs, AT&T, and GTE; Congress enacted section 222 to protect the CPNI of customers of all telecommunications carriers.[83] Indeed, Congress rejected broadly worded drafts of section 222 that would have granted the Commission authority over "such other information concerning the customer as is available to the local exchange carrier"[84] or "customer-specific proprietary information."[85] Instead, Congress specifically defined CPNI in section 222(h) and did not permit the Commission to expand that term through rulemaking.

The reference in section 222(a) to the "proprietary information" of customers is not a free-standing source of authority to regulate carriers' use and disclosure of non-CPNI. Reading section 222(a) in this manner would conflict with the remainder of the statute. Section 222(d) exempts certain uses of CPNI, such as to bill customers, from the limitations of section 222(c), and section 222(e) exempts the publication of subscriber list information from the limitations of sections 222(b), (c), and (d). But both customer bills and subscriber lists include "personally identifiable information" (or PII) that is not also CPNI, which the Commission now says is subject to use limitations found in section 222(a). Neither section 222(d) nor section 222(e) exempts their permissible uses of customer information from the purported requirements of

---

[82] *See*, *e.g.*, CTIA Comments at 25-35; Competitive Carriers Ass'n Comments at 14-16; Sprint Comments at 5-6; NTCA Comments at 26-28; T-Mobile Comments at 16-22; Comcast Comments at 71-75; AT&T Comments at 103-07; ITTA Comments at 3-11; American Cable Ass'n Comments at 13-15; Senator Jeff Flake Comments at 4-5.

[83] *See* Notice of Proposed Rulemaking, *Implementation of the Telecommunications Act of 1996*, 11 FCC Rcd 12513, ¶ 8 (1996).

[84] H.R. Rep. No. 104-204, pt. 1, at 23 (1995).

[85] S. Rep. No. 104-23, at 24 (1995).

section 222(a). Moreover, section 222(a) speaks only of "protect[ing] the confidentiality" of information. The Commission's proposed interpretation ignores the fact that "protect" has a different meaning than "use, disclose, or permit access to," as sections 222(c) and (d) state, and cannot support restrictions on the use or disclosure of information. The best and only reasonable interpretation of section 222(a) is that its reference to "proprietary information of . . . customers" means CPNI. The Commission had acknowledged this interpretation of section 222(a) for 18 years and even denied a "request that the Commission hold that section 222 controls all issues involving customer information, rather than issues pertaining to CPNI," stating that it was "not persuaded that any portion of section 222 indicates that Congress intended such a result."[86]

In sum, the Commission was correct, and its newly revised interpretation is unlawful. Section 222 can only be read to regulate telecommunications carriers' use of CPNI and does not reach PII that does not meet the statutory definition of CPNI. Congress does not "hide elephants in mouseholes,"[87] and, where it intends to protect PII, it does so by name.[88]

Few commenters offer any support for the Commission's claim in the NPRM that section 222 confers legal authority to regulate carriers' use and disclosure of PII that is not also CPNI. The few arguments that are raised lack merit.

First, Public Knowledge asserts that the Commission ruled in 2007 that section 222 includes all PII within the definition of CPNI.[89] Not so. Their argument is entirely based on the

---

[86] Order on Reconsideration and Petitions for Forbearance, *Implementation of the Telecommunications Act of 1996*, 14 FCC Rcd 14409, ¶ 147 (1999).

[87] *Whitman v. American Trucking Ass'ns, Inc.*, 531 U.S. 457, 468 (2001).

[88] *See, e.g.*, 47 U.S.C. § 551.

[89] *See* Public Knowledge *et al.* Comments at 27-28.

following sentence in a footnote in the Commission's *2007 CPNI Order*[90]: "CPNI includes personally identifiable information derived from a customer's relationship with a provider of communications services."[91] This sentence is true: CPNI *does* include some PII, such as the location of a telecommunications service.[92] But it does not mean, as Public Knowledge argues, that *all* PII is *also* CPNI. Indeed, the Commission just a few paragraphs later defined CPNI more specifically by quoting its statutory definition in section 222(h).[93] Nothing about the *2007 CPNI Order* required a revised definition of CPNI, and no basis exists to conclude that the Commission has already ruled that CPNI includes *all* PII.

Second, several commenters argue that section 222(a) prohibits carriers' use of customer information unless the following subsections, such as sections 222(c) and (d), affirmatively permit its use.[94] This argument suffers from several flaws. Section 222(c)(1) tells telecommunications carriers that they "shall only" use individually identifiable CPNI in the circumstances it specifies. If section 222(a) separately prohibited the use of *all* customer information, section 222(c)(1) would not need to say "shall only." Because all uses of customer information would be already barred, section 222(c)(1) would say that carriers *may* use individually identifiable CPNI in those circumstances.

---

[90] Report and Order and Further Notice of Proposed Rulemaking, *Implementation of the Telecommunications Act of 1996*, 22 FCC Rcd 6927 (2007).

[91] *Id.* ¶ 1 n.2.

[92] *See* 47 U.S.C. § 222(h)(1).

[93] *See* 2007 CPNI Order ¶ 5.

[94] *See, e.g.*, Electronic Frontier Foundation Comments at 2; Free Press Comments at 8-10; Center for Democracy & Technology Comments at 11-12; New America's Open Technology Institute Comments at 11-12; Public Knowledge, *Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission's Privacy Rules for the Digital World* at 16-17 (Feb. 2016) ("PK White Paper"), https://www.publicknowledge.org/assets/uploads/blog/article-cpni-whitepaper(1).pdf.

Section 222(d) is a series of exceptions specific to the use of CPNI and, therefore, to the limitations of section 222(c).[95] Its permissive uses of CPNI do not extend to PII that is not also CPNI. And section 222(a) itself describes no permissible uses of "customer proprietary information," not even with customer consent. Thus, if the commenters are correct, although a carrier may use CPNI to bill a customer pursuant to section 222(d)(1), a carrier would violate section 222(a) if it used that broadband customer's name to bill him or her: a broadband customer's name is not CPNI,[96] but it is PII under the NPRM.[97] The Commission, recognizing this problem, claimed that it could expand section 222(d) to cover PII that is not also CPNI despite the clear language of the statute.[98] Yet these commenters neither support the Commission's claimed authority nor dispute that section 222(d) would have to be expanded to permit PII that is not also CPNI to be used for, among other things, the billing of broadband customers.

And section 222(e) requires a carrier to provide subscriber list information in certain circumstances "[n]otwithstanding subsections (b), (c), and (d)." It is, therefore, an exception to subsections (b), (c), and (d). If section 222(a) were a separate source of authority prohibiting the use of customer information, section 222(e) would also have to say that it applied notwithstanding subsection (a). Neither the Commission nor the commenters have indicated how to reconcile sections 222(a) and (e) if the Commission is right.

---

[95] *See* 47 U.S.C. § 222(d) ("Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to *customer proprietary network information* obtained from its customers . . . .") (emphasis added).

[96] *See id.* § 222(h)(1).

[97] *See* NPRM ¶ 62.

[98] *See id.* ¶ 115.

Against the clear structure of the statute, the commenters instead rely on the section title. For instance, Public Knowledge's White Paper states that "Congress's decision to name § 222 'Privacy of Customer Information' makes abundantly clear that Congress intended to broadly protect the privacy of consumers."[99] To the extent the title has any relevance at all, it must be understood to refer to the fact that section 222 deals with information of carriers' customers, including other telecommunications carriers as described in section 222(b).[100] The title is not a substantive provision of the statute, but instead identifies that the provisions of section 222 deal with certain information of customers.

Third, some commenters such as Public Knowledge argue that the legislative history of section 222 shows that Congress "expand[ed] the *general* duty of carriers to protect customer information while significantly reducing the *specific list* of duties."[101] Again, they focus on the fact that the title of the section was changed from "Privacy of Customer Proprietary Network Information" to "Privacy of Customer Information" and the fact that an "In general" introductory subsection was added to the statute.[102] However, the Conference Report explains these changes and demonstrates that they were not intended to create a general authority over all customer information. The introductory subsection and the new title were added because the enacted form of section 222 included section 222(b), regarding proprietary information received from another carrier for the purpose of providing a telecommunications service.[103] These changes do not indicate that Congress was changing its focus from protecting CPNI. In fact, the Conference

---

[99] PK White Paper at 17; *see also id.* at 15.

[100] *See* 47 U.S.C. § 222(b).

[101] PK White Paper at 15.

[102] *See id.*

[103] *See* H.R. Conf. Rep. No. 104-458, at 205 (1996).

Report states that "the new section 222 strives to balance both competitive and consumer privacy interests *with respect to CPNI*."[104] Congress had no intent to include any consumer information within section 222 unless it was CPNI. And the statute Congress enacted only makes sense if it covers CPNI alone and not all PII. The Commission's rules, therefore, cannot stand with respect to PII that is not also CPNI.

B. Commenters' Few Attempts To Ground the Commission's Proposed Rules in Other Statutory Provisions Fail

Verizon has already explained why the Commission cannot ground its authority to issue its proposed rules outside of section 222.[105] Sections 201, 202, 303, and 316[106] are all general provisions that speak broadly of reasonableness and the public interest, but such general statutes do not apply to matters that are specifically addressed in a separate provision of the same Act.[107] Public Knowledge argues that section 631 of the Act, which requires a "cable operator" (or its affiliates) to provide notice to its subscribers before collecting or using "personally identifiable information,"[108] is an independent source of the Commission's authority "for regulating consumer privacy and protecting the proprietary information of consumers online."[109] Of course, section 631 applies only to cable operators and their affiliates, which constitute only a subset of

---

[104] *Id.* (emphasis added).

[105] *See* Verizon Comments at 60-62.

[106] *See* 47 U.S.C. §§ 201(b), 202(a) (prohibiting "unjust or unreasonable" practices); *id.* § 303(b) (permitting the Commission to "[p]rescribe the nature of the service to be rendered by each class of licensed stations" as "public convenience, interest, or necessity requires"); *id.* § 316(a)(1) (permitting the Commission to modify a "station license" if "such action will promote the public interest, convenience, and necessity").

[107] *See Fourco Glass Co. v. Transmirra Prods. Corp.*, 353 U.S. 222, 229 (1957) (section 222 is "the sole and exclusive provision" governing the issue of customer information, and "it is not to be supplemented" by the more general provisions cited in the NPRM).

[108] 47 U.S.C. § 551.

[109] PK White Paper at 20-22.

broadband providers. Moreover, section 631 does not authorize the Commission to issue rules — indeed, the statute provides for a private right of action — and the Commission itself has acknowledged that the provisions of section 631 are "enforced by the courts, and not by the Commission."[110] Even more importantly, section 631 demonstrates that, when Congress intends to regulate the use and disclosure of "personally identifiable information," it knows how to do so. The fact that Congress did not use the term "personally identifiable information" in section 222 confirms that it is limited to CPNI.

Similarly unavailing is the commenters' reliance on section 705,[111] which is an anti-wiretapping provision that prohibits the unauthorized publication or use of communications. The Electronic Frontier Foundation argues that section 705's "broad prohibition against divulgence or publication would serve as a clear statutory bar against carriers from selling consumer data for purposes outside the scope of providing telecommunications services."[112] But section 705 is not a general privacy provision; rather, it prohibits only the unauthorized disclosure of the *contents* of communications, stating that "no person . . . transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof" except to an authorized person.[113] None of the items the Commission proposes to classify as "personally identifiable information" includes the contents of communications. So section 705 provides no independent authority for the Commission's proposed rules.

---

[110] Memorandum Opinion and Order, *Applications for Consent to the Transfer of Control of Licenses and Section 214 Authorizations by Time Warner Inc. and America Online, Inc., Transferors, to AOL Time Warner Inc., Transferee*, 16 FCC Rcd 6547, ¶ 279 (2001).

[111] 47 U.S.C. § 605.

[112] Electronic Frontier Foundation Comments at 3.

[113] 47 U.S.C. § 605(a).

IV. THE COMMISSION SHOULD ADOPT REASONABLE BREACH-NOTIFICATION AND DATA-SECURITY REQUIREMENTS

A. Data-Breach Notifications

As the record shows in this proceeding, the Commission's proposed breach-notification requirements threaten to create a practice of over-notifying consumers about breaches.[114] Specifically, because the Commission's proposal would require consumer notification of any use, disclosure, or access of any customer information, no matter how minimal or non-sensitive, consumers will receive many notifications for "breaches" that will not harm them, that they do not care about, and that do not warrant any action on their part. Under such an approach, the Commission runs the risk of watering-down the significance of breach notifications to such an extent that a consumer will ultimately pay no attention to the notifications — even those that warrant their attention.[115] It is therefore in the interest of consumers, and thus the Commission, to maintain an environment where a notification is sent only when it can be of benefit to the consumer.[116]

To this end, the Commission should modify its proposal and instead require customer notification when "a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed individually identifiable CPNI and where such use, disclosure, or access is likely to cause consumer harm," as proposed by multiple commenters.[117] Additionally, the Commission should adopt a "good faith" exception in cases of accidental breaches where a telecommunications provider's employee unintentionally accesses a consumer's information, and

---

[114] *See* AT&T Comments at 81; Consumer Technology Ass'n Comments at 11.

[115] *See* AT&T Comments at 81.

[116] *See* Jon Leibowitz Comments at 11 (comments of former Chairman of the FTC).

[117] Verizon Comments at 68.

no likelihood of harm to the consumer exists. In such cases, the Commission should exempt telecommunications providers from having to submit breach notifications to consumers.[118]

While certain commenters argue that notice fatigue is not a practical concern,[119] they ignore the practical impact notice fatigue has on consumers. As the FTC staff notes in its comments, "consumers may be overwhelmed by the volume of breach notices they receive."[120] As a result, consumers "could become numb to such notices, so that they may fail to spot or mitigate the risks being communicated to them," as evidenced by a recent study by the Ponemon Institute.[121] Similarly, the Competitive Carriers Association pointed to a study by the USENIX Association indicating that over-notification "would make it less likely that consumers become aware of truly alarming data breaches."[122] Over-notification also has the potential to mislead consumers into distrusting telecommunications providers. When a consumer receives multiple breach notifications from one type of entity — telecommunications providers — and only a few from other types of actors, consumers will incorrectly believe telecommunications providers are mishandling or not protecting their data like other entities,[123] and, in fact, it will be detrimental to the consumer.

---

[118] *See* FTC Staff Comments at 32.

[119] *See* Privacy Rights Clearinghouse Comments at 6.

[120] FTC Staff Comments at 31-32.

[121] *Id.*

[122] Competitive Carriers Ass'n Comments at 44 n.107 (citing Florian Schaub et al., *A Design Space for Effective Privacy Notices, in* 2015 SYMPOSIUM ON USABLE PRIVACY AND SECURITY 3 (USENIX Ass'n, 2015) ("[f]requent exposure to seemingly irrelevant privacy notices results in habituation, i.e., notices are dismissed without even registering their content")).

[123] *See* Mobile Future Comments at 4.

In addition, while certain supporters of the Commission's proposals argue that harm should *not* be the trigger for requiring a notification for the consumer,[124] they ignore the fact that a notification of a breach with no risk of harm serves no purpose. The purpose of notifying consumers of a breach is to make them aware that their information was used or shared in a way that potentially could cause them harm and to inform them that they may need to take action to prevent such harm (such as by changing their password or monitoring their account).[125] Even the Online Trust Alliance notes that a breach notification should not be required "[w]hen there is evidence that there is no risk to the impacted user."[126] While the New America's Open Technology Institute dubiously claims that a consumer should be notified even in instances where "a data breach occurs because of an employee mistake or some other seemingly innocuous circumstance" so as to allow the consumer to take the appropriate protective steps,[127] in reality, the consumer would have no need to protect herself where the data was accessed by mistake. And telecommunications providers have every incentive to take the action needed to protect their customers and to notify them so that they can take action to protect themselves. Thus, notification of breaches that have no potential to harm the consumer would do nothing to protect consumers.

The true outcome of the Commission's proposal would be that companies would be forced to divert resources away from other more important data-security matters, thereby harming the consumer. Proponents of the Commission's proposal claim that telecommunications providers should treat all breaches equally and spend resources notifying consumers of these

---

[124] *See* Privacy Rights Clearinghouse Comments at 6.

[125] *See* NCTA Comments at 91-92.

[126] Online Trust Alliance Comments at 3.

[127] New America's Open Technology Institute Comments at 42.

breaches.[128] But these proponents ignore the reality that investigating a breach and notifying consumers of a breach requires significant resources. By requiring telecommunications providers to spend considerable resources on accidental breaches or non-harmful breaches, there will be fewer resources available to address serious breaches and data-security threats, putting consumers at great peril.[129]

In addition to the quantity of notifications, the Commission's proposal compromises the quality of breach notifications. While certain groups voice their support for the proposal's 10-day notification requirement,[130] they ignore the variety and complexity of breaches that customers may need to be notified about. Many data breaches will take longer than 10 days to assess. Mandating a 10-day deadline would force telecommunications companies to notify consumers before the extent of a breach is fully understood and before the needed time to remedy the breach.[131] As a result, the consumers will be put at a disadvantage by the rigidity of the Commission's time requirement. The notifications will be incomplete, and the consumers will be left in a state of uncertainty. The FTC staff agrees.[132] An approach that would require notice within 30 days and without "unreasonable delay" is a more reasonable and simple approach, and is more consistent with the approaches that have been embraced by many States.[133]

---

[128] *See id.*

[129] *See* State Privacy and Security Coalition Comments at 11-12.

[130] *See* Online Trust Alliance Comments at 3; New America's Open Technology Institute Comments at 43.

[131] *See* Cincinnati Bell Telephone Company Comments at 13.

[132] *See* FTC Staff Comments at 32-33.

[133] *See, e.g.*, State Privacy and Security Coalition Comments at 13-14.

B. Data Security and Encryption

The record in this proceeding is clear: The FCC should not adopt prescriptive data-security requirements. While certain commenters claim prescriptive requirements are needed to protect consumers and their information,[134] these groups ignore the complexities of an ever-changing technological environment. Prescriptive standards that might be state of the art today may be insufficient tomorrow. To keep up with the constant changes in the world of data security, telecommunications providers must be allowed to innovate, rather than adhere to the inflexible standards proposed by the Commission.[135] By stripping telecommunications providers of the flexibility to innovate in their data-security practices, the proposed rules could actually result in a less secure environment.

The record similarly shows that the Commission should not find telecommunications providers strictly liable for all data breaches. Even those commenters generally supporting the Commission's proposal do not favor a strict-liability approach. For example, New America's Open Technology Institute argues that broadband providers have a special duty to protect the confidentiality of customer proprietary information and that "[f]ailing to take *precautions* against data breaches clearly violates that duty."[136] The Commission should abandon strict liability and instead look to the FTC's guidance in crafting security requirements. In their comments, the FTC staff suggested modifying the proposed rules "to require [broadband] providers to 'ensure

---

[134] *See* Consumer Action at 2 ("ISPs must be required to follow strict rules to safeguard consumer information from unauthorized use or disclosure and to take full responsibility for the protection of customer information when it is shared with third parties.").

[135] *See* WTA — Advocates for Rural Broadband Comments at 19 ("[T]he Commission should not stray from the flexible, best practices approach to data security by adopting specific administrative, technical or physical requirements for implementing data security requirements.").

[136] New America's Open Technology Institute Comments at 41 (emphasis added).

the *reasonable* security, confidentiality, and integrity of all customer PI.' "[137] Commenters understand that no entity is wholly immune from a security breach, and, under the Commission's proposed approach, even the most vigilant actor could be liable for an unforeseeable breach.[138] Certain commenters' insistence on imposing strict liability on telecommunications providers for the violations of third-party contractors is similarly misguided.[139] Telecommunications providers "already have every incentive . . . to vet the third parties with whom they contract and to engage in appropriate oversight to ensure that contractual obligations are met."[140]

Revising the Commission's proposed data-security rules in this manner also will ensure that all consumer data is protected appropriately rather than equally. As former FTC Chairman Jon Leibowitz noted, "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."[141] The Commission should not require telecommunications providers to spend resources protecting non-sensitive data in the same manner that it protects highly sensitive data. Certain data-security protections may not be needed for non-sensitive data. As noted by former FTC Chairman Leibowitz, "risk assessments and audits of non-sensitive information divert resources away from

[137] FTC Staff Comments at 27-28.

[138] *See* WTA — Advocates for Rural Broadband Comments at 18 ("The Commission's rules must reflect the reality that no firm or individual is immune from cyber threats and under no circumstance should the Commission take the position that existence of a breach is indicative of poor data security practices.").

[139] *See* American Ass'n of Law Libraries Comments at 4.

[140] Verizon Comments at 67.

[141] Jon Leibowitz Comments at 11.

protecting truly sensitive information and maintaining the security of networks."[142] Encryption and multi-factor authentication similarly are not appropriate in all situations.

While backers of these requirements argue merely that any possible protective measure that could be employed must be employed, or that broadband providers are taking advantage of the consumer,[143] this position ignores the fact that not every protective measure is always appropriate and such a requirement would divert resources that otherwise could have been used to employ more effective means of protecting data.

Indeed, such prescriptive requirements could affirmatively harm consumers, rather than protect them. As the WTA explained, "[s]etting specific guidelines as to multi-factor authentication or other technical measures would provide bad actors with a roadmap of what they need to effectively gain access to systems through social engineering or other methods and would be particularly burdensome for small carriers."[144]

V. THE COMMISSION CANNOT, AND SHOULD NOT, BAN ARBITRATION PROVISIONS IN BROADBAND PROVIDERS' CONTRACTS WITH THEIR CUSTOMERS

As Verizon explained in its comments,[145] the Commission's proposal to prohibit broadband providers from entering into binding arbitration contracts with their customers is both unlawful — particularly in light of the Federal Arbitration Act ("FAA") — and misguided as a

---

[142] *Id.*

[143] *See* New America's Open Technology Institute Comments at 41 ("[Broadband] providers should also have to encrypt their data at rest and, when applicable, in transit. . . . [F]ailing to use encryption to protect private information is unjust and unreasonable, and puts customers at unnecessary risk of data breaches.").

[144] WTA — Advocates for Rural Broadband Comments at 20.

[145] *See* Verizon Comments at 70-80.

policy matter. The comments submitted in favor of the Commission's proposal do not disturb those key conclusions.

First, the comments confirm that the Commission lacks the legal authority to prohibit mandatory arbitration agreements. None of the statutory provisions cited by commenters as a legal basis for the Commission's proposal to ban such agreements gives the Commission that authority.

Nothing in section 201 or section 222 of the Communications Act[146] gives the Commission authority to ban arbitration clauses.[147] Those provisions are general grants of regulatory authority, and they do not address arbitration or dispute resolution and do not indicate in any way that Congress intended for the Commission to regulate this subject. In addition, these provisions cannot be construed to authorize the Commission to ban arbitration, because such an interpretation would contravene both the text of and the policy judgments reflected in the FAA. In interpreting the Communications Act, the Commission must "harmoniz[e]" it with other statutes,[148] including the FAA. Moreover, an interpretation of the Act that *fails* to harmonize it with other statutes is not entitled to *Chevron* deference.[149] Thus, were the Commission to construe its residual regulatory power as authorizing a ban on arbitration clauses, a court would not defer to that interpretation.

---

[146] 47 U.S.C. §§ 201, 222.

[147] *See, e.g.*, American Ass'n for Justice Comments at 6.

[148] *Astoria Fed. Sav. & Loan Ass'n v. Solimino*, 501 U.S. 104, 109 (1991).

[149] *See FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 155-57 (2000); *see also Hoffman Plastic Compounds, Inc. v. NLRB*, 535 U.S. 137, 143-44 (2002).

Likewise irrelevant are sections 206 and 207 of the Communications Act.[150] These sections simply provide a cause of action for individuals to sue common carriers for violations of the Act; they do not reflect a congressional judgment that, even where a customer has agreed to arbitrate, these claims must proceed in court rather than in arbitration. The Supreme Court has specifically and repeatedly rejected the notion that provisions like sections 206 and 207 reflect a congressional judgment sufficient to displace the pro-arbitration text and policy of the FAA.[151]

Nor does section 208 of the Communications Act,[152] which allows persons and entities to bring complaints before the Commission, justify the proposed ban on arbitration agreements.[153] As an initial matter, many arbitration agreements, including Verizon's,[154] do not prohibit individuals from bringing complaints to the Commission. Moreover, the FAA says nothing about a customer's ability to bring complaints to the attention of enforcement agencies like the Commission, which may then undertake an investigation and enforcement action, if it so desires. The FAA simply requires courts to enforce agreements to arbitrate *private* disputes between parties. Section 208 does not contradict that principle.

Nor is it an answer that the FAA "simply supports the enforcement of written arbitration provisions in contracts" and "does not . . . preclude laws or regulations that prevent a party from placing such provisions in their contracts in the first place."[155] The distinction this comment

---

[150] 47 U.S.C. §§ 206-207. *See* American Ass'n for Justice Comments at 6.

[151] *See CompuCredit Corp. v. Greenwood*, 132 S. Ct. 665, 669-70 (2012); *see also Gilmer v. Interstate/Johnson Lane Corp.*, 500 U.S. 20, 29 (1991); *Shearson/American Express, Inc. v. McMahon*, 482 U.S. 220, 228, 238 (1987).

[152] 47 U.S.C. § 208.

[153] *See* Public Knowledge *et al.* Comments at 33.

[154] *See* Verizon Wireless, "Customer Agreement," http://www.verizonwireless.com/b2c/support/customer-agreement.

[155] American Ass'n for Justice Comments at 6.

seeks to draw between the enforcement of arbitration clauses as written (which the FAA clearly requires) and the ability to agree to arbitration clauses in the first place is untenable and contradicts decades of Supreme Court precedent regarding the meaning and purpose of the FAA. The Court has repeatedly explained that the FAA "reflects a legislative recognition of the desirability of arbitration as an alternative to the complications of litigation."[156] The federal policy enshrined in the FAA — a policy that "favor[s] this method of resolving disputes"[157] — would be frustrated by a rule preventing parties from agreeing to arbitrate no less than by a rule declining to enforce such agreements. In *AT&T Mobility LLC v. Concepcion*,[158] the Court explained that the FAA prohibits rules that "stand as an obstacle to the accomplishment of the FAA's objectives."[159] That principle operates to bar such rules even when they are not specifically addressed by the literal terms of the FAA, as was the case with the California rule against arbitration agreements containing class-action waivers that was at issue in *Concepcion*. And that principle applies here: Prohibiting private parties from agreeing in advance to arbitrate disputes plainly would obstruct the accomplishment of the FAA's objectives, the most fundamental of which is "to allow parties to avoid 'the costliness and delays of litigation' " by agreeing to arbitrate any claims that may arise.[160] It is thus no surprise that the federal courts of appeals have held that the FAA preempts regulations that prohibit or limit parties from placing arbitration provisions in contracts.[161]

---

[156] *Scherk v. Alberto-Culver Co.*, 417 U.S. 506, 511 (1974) (internal quotations omitted).

[157] *Rodriguez de Quijas v. Shearson/American Express, Inc.*, 490 U.S. 477, 481 (1989).

[158] 563 U.S. 333 (2011).

[159] *Id.* at 343-44.

[160] *Scherk*, 417 U.S. at 510-11 (quoting H.R. Rep. No. 68-96, at 1, 2 (1924)).

[161] *See Saturn Distrib. Corp. v. Williams*, 905 F.2d 719, 723 (4th Cir. 1990) ("We hold today that § 2 [of the FAA] does preempt state rules of contract formation which single out

Finally, actions or contemplated actions of certain other federal agencies to restrict arbitration agreements are beside the point.[162] The legality of many of these proposals remains contested and unsettled.[163] But whether a particular agency has the authority to prohibit particular kinds of mandatory arbitration provisions depends on the power delegated to the agency by Congress. The Consumer Financial Protection Bureau ("CFPB"), for instance, has proposed to restrict mandatory arbitration provisions in consumer financial-services agreements — but Congress expressly contemplated that, subject to certain conditions and requirements, the CFPB might do so.[164] No comparable provision appears in the Communications Act, and the Act contains no other provision that conceivably could be interpreted as authorizing a prohibition on arbitration clauses in consumer contracts.[165]

---

arbitration clauses and unreasonably burden the ability to form arbitration agreements."); *Securities Indus. Ass'n v. Connolly*, 883 F.2d 1114, 1122-23 (1st Cir. 1989) (holding state regulation prohibiting broker-dealers from requiring customers to enter arbitration agreements was preempted by FAA because the rule would either "inhibit a party's willingness to create an arbitration contract or undermine the contract's enforceability (if the party proceeds notwithstanding the edict)").

[162] *See* American Ass'n for Justice Comments at 3-5; Nat'l Ass'n of Consumer Advocates *et al.* Comments at 7-8.

[163] *Compare D.R. Horton, Inc. v. NLRB*, 737 F.3d 344, 360 (5th Cir. 2013), *with Lewis v. Epic Sys. Corp.*, — F.3d —, 2016 WL 3029464, at *4 (7th Cir. May 26, 2016) (reaching conflicting outcomes on legality of National Labor Relations Board rulings invalidating mandatory arbitration provisions in employment contracts).

[164] *See* 12 U.S.C. § 5518(b).

[165] In particular, the Seventh Circuit's conclusion in *Lewis* that the National Labor Relations Act ("NLRA") precluded mandatory arbitration clauses hinged on the NLRA's express protection of " 'concerted activities for the purpose of collective bargaining or other mutual aid or protection.' " 2016 WL 3029464, at *1 (quoting 29 U.S.C. § 157). There is no similar provision in the Communications Act.

Second, many commenters express the view that arbitration clauses are undesirable as a matter of public policy.[166] The key point is that Congress has considered the same question and reached the opposite policy judgment in enacting the FAA.[167] But it is also important to note that many of the policy arguments advanced by commenters lack support and contradict empirical studies, as well as particular aspects of arbitration agreements like Verizon's. For instance, commenters argue (without citation to any authority) that private arbitration is "inherently biased" because of a purported "repeat player" advantage.[168] But empirical studies — including the study conducted by the CFPB that is cited by several commenters — have found no evidence to support this theory.[169] Similarly, commenters argue (again without citation) that private arbitration is unfairly costly to plaintiffs.[170] In reality, the evidence shows that arbitration is *less* costly than litigation (as well as much faster to resolve disputes),[171] and Justice Ruth Bader Ginsburg has described the rules of the American Arbitration Association as "models for

---

[166] *See, e.g.*, American Ass'n for Justice Comments at 1-3; Consumer Federation of California Comments at 11-12; Nat'l Ass'n of Consumer Advocates *et al.* Comments at 2-4.

[167] *See Concepcion*, 563 U.S. at 339, 351; *see also Ivey v. D.R. Horton, Inc.*, No. 3:08-cv-598-CMC, 2008 WL 2717863, at *2 (D.S.C. July 10, 2008) ("[T]he 'liberal federal policy favoring arbitration agreements' reflects Congress' perspective on the fairness and efficiency of arbitration as a process for dispute resolution.") (quoting *Moses H. Mem'l Hosp. v. Mercury Constr. Corp.*, 460 U.S. 1, 24 (1983))

[168] American Ass'n for Justice Comments at 2.

[169] *See* Consumer Financial Protection Bureau, *Arbitration Study: Report to Congress, pursuant to Dodd-Frank Wall Street Reform and Consumer Protection Act § 1028(a)*, at § 5, p. 67, Fig. 23 (Mar. 2015) ("CFPB Study"), *available at* http://files.consumerfinance.gov/f/201503_cfpb_arbitration-study-report-to-congress-2015.pdf; Christopher R. Drahozal & Samantha Zyontz, *An Empirical Study of AAA Consumer Arbitrations*, 25 Ohio St. J. on Disp. Resol. 843, 909 (2010); Elizabeth Hill, *Due Process at Low Cost: An Empirical Study of Employment Arbitration Under the Auspices of the American Arbitration Association*, 18 Ohio St. J. on Disp. Resol. 777, 785-88 (2003).

[170] *See* American Ass'n for Justice Comments at 3.

[171] *See* Drahozal & Zyontz, 25 Ohio St. J. on Disp. Resol. at 845.

fair cost and fee allocation."[172] In addition, many companies — including Verizon — cover *all* arbitration fees, regardless of the outcome.

Several commenters, citing the CFPB Study, conclude that arbitration simply can never be an effective mechanism for resolving small-dollar-value claims.[173] Again, the evidence does not support that conclusion. It shows that arbitration plaintiffs routinely recover attorney's fee awards of thousands of dollars, providing ample incentive for plaintiffs to bring claims in arbitration where customers actually desire to.[174] Verizon's arbitration agreement, among many others, provides for reasonable attorney's fees for prevailing plaintiffs. Moreover, these commenters overlook the important point that many small-dollar-value cases serve primarily to enrich plaintiff's attorneys rather than consumers, who frequently receive little or no tangible benefit.[175]

Finally, commenters argue that many arbitration agreements are procedurally unfair and take advantage of customers.[176] On the contrary, many companies, including Verizon, go to great lengths to ensure that arbitration procedures are fair and easy for consumers to invoke.[177] In instances in which companies craft biased or one-sided arbitration provisions, courts routinely

---

[172] *Green Tree Fin. Corp.-Alabama v. Randolph*, 531 U.S. 79, 95 (2000) (concurring in part and dissenting in part).

[173] *See, e.g.*, Nat'l Ass'n of Consumer Advocates *et al.* Comments at 3; Smithwick & Belendiuk, P.C. Comments at 4.

[174] *See* Drahozal & Zyontz, 25 Ohio St. J. on Disp. Resol. at 902.

[175] *See, e.g.*, Martin H. Redish et al., *Cy Pres Relief and the Pathologies of the Modern Class Action: A Normative and Empirical Analysis*, 62 Fla. L. Rev. 617, 653-54 (2010).

[176] *See* Consumer Federation of California Comments at 11-12; Smithwick & Belendiuk, P.C. Comments at 7.

[177] *See* Verizon Comments at 79-80.

invalidate them.[178] Commenters argue that consumers do not understand pre-dispute arbitration agreements or their right to opt out,[179] but the evidence in support of this claim — a *post hoc* survey asking consumers if they believed they could sue in court or if they recalled being offered an opt-out opportunity[180] — is weak. And these concerns, even if supported, would not justify a prohibition against all arbitration agreements in contracts between broadband providers and their customers. Moreover, the same charge might be leveled against class actions, where few class plaintiffs are aware of the proceeding or claim relief available to them.[181] That is no basis for prohibiting companies from entering into voluntary agreements with their customers to arbitrate disputes.

CONCLUSION

For the reasons provided above and in Verizon's opening comments, the Commission should ensure that any new privacy and data-security rules it adopts are consistent with the notice-and-choice framework that applies to all other participants in the Internet ecosystem.

---

[178] *See, e.g.*, *Chavarria v. Ralphs Grocery Co.*, 733 F.3d 916, 923-25 (9th Cir. 2013).

[179] *See* Consumer Federation of California Comments at 11-12 (characterizing CFPB Study as finding that "most consumers do not understand pre-dispute arbitration agreements").

[180] *See id.* at 12.

[181] *See, e.g.*, Mayer Brown LLP, *Do Class Actions Benefit Class Members?* at 7 (2013) (finding claim rates ranging from 0.000006% to 12%), https://www.mayerbrown.com/files/uploads/Documents/PDFs/2013/December/DoClassActionsBenefitClassMembers.pdf.

Respectfully submitted,

s/ Karen Zacharia

William H. Johnson
Of Counsel

Karen Zacharia
Catherine M. Hilke
Verizon
1300 I Street, N.W. – Suite 400 West
Washington, D.C. 20005
(202) 515-2438

Scott H. Angstreich
Geoffrey M. Klineberg
Kellogg, Huber, Hansen, Todd,
Evans & Figel, P.L.L.C.
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
(202) 326-7900

Henry Weissmann
Munger Tolles & Olson, LLP
355 South Grand Avenue
35th Floor
Los Angeles, California 90071
(213) 683-9100

Counsel for Verizon

July 6, 2016