Before the
**FEDERAL COMMUNICATIONS COMMISSION**
Washington, DC 20554

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

To: The Commission

**COMMENTS OF T-MOBILE USA, INC.**

Cathleen Massey
Luisa Lancetti
Michelle Rosenthal
**T-Mobile USA, Inc.**
601 Pennsylvania Avenue, NW
Suite 800
Washington, DC 20004
(202) 654-5900

May 27, 2016

## TABLE OF CONTENTS

Before the
**FEDERAL COMMUNICATIONS COMMISSION**
Washington, DC 20554

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

To: The Commission

**COMMENTS OF T-MOBILE USA, INC.**

T-Mobile USA, Inc. ("T-Mobile")[1] submits these comments in response to the Notice of Proposed Rulemaking ("NPRM")[2] in the above-referenced proceeding.

## I. INTRODUCTION AND SUMMARY

T-Mobile appreciates and understands the importance of consumer privacy and consumer trust. As the "Un-carrier," T-Mobile has consistently developed new and innovative services to address customer needs, while recognizing that consumers expect appropriate protections for their most personal data. In this area and others, T-Mobile's commitment to the needs of customers, and its aggressive efforts to compete against other providers in the mobile marketplace to win and retain customers, generates tremendous consumer value.

The Commission's proposed rules, however, would undermine rather than promote consumer interests. Customers value privacy, and they also recognize the benefits of the current Internet ecosystem, in which the use of some data, subject to existing privacy protections,

---

[1] T-Mobile USA, Inc. is a wholly-owned subsidiary of T-Mobile US, Inc., a publicly traded company.

[2] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* Notice of Proposed Rulemaking, 31 FCC Rcd 2500 (2016) ("NPRM").

informs the provision of services they want and demand. The NPRM's proposal, if adopted, would constrain T-Mobile's ability to innovate and deliver new and convenient services to consumers that reduce "pain points," in turn impairing T-Mobile's continued ability to disrupt the wireless marketplace – without corresponding consumer protection benefits.

T-Mobile agrees that the practices of mobile broadband Internet access service ("BIAS") providers[3] should protect consumers' privacy and security. But it is in no way inconsistent with a robust level of privacy and security protection for such practices to be dictated by consumers, competition, and generally applicable consumer protection regimes that apply to all other players within the Internet ecosystem. Rigid prescriptive rules, like those proposed in the NPRM, simply cannot keep up with the dynamic Internet marketplace. Ultimately, the NPRM relies on arbitrary distinctions and ignores current consumer expectations, practical realities, and competitive impacts. The Commission should not dictate customer choices in this manner.

Moreover, the NPRM ignores the language and limitations in Section 222 of the Communications Act[4] in ways that impermissibly seek to expand the Commission's jurisdiction. The Commission proposes to bring within its reach control over virtually any customer information a BIAS provider holds about a consumer, including any personally identifiable information ("PII"). Section 222, however, is limited to customer proprietary network information ("CPNI") – a class of information far narrower than that which the Commission seeks to regulate here. And the Commission cannot rely on other provisions of the Communications Act to reach beyond CPNI and impose the rules proposed here. But regardless

[3] These comments at times refer to BIAS providers alternatively as Internet service providers ("ISPs").

[4] 47 U.S.C. § 222.

of the scope of its jurisdiction, the Commission still could not adopt the proposed rules, as they would run afoul of the First Amendment.

Even if they were lawful, the proposed rules would harm consumer interests. They would prevent ISPs like T-Mobile from serving customers in the ways they expect and demand, and that are best tailored to meet their needs. Eschewing the "total services approach" the Commission took with respect to CPNI in the telephony era,[5] the framework proposed here would strip ISPs of their ability to seamlessly offer comprehensive services to their customers, including not only voice and data services, but also related services. T-Mobile is concerned about numerous aspects of the NPRM. In these comments, however, T-Mobile focuses on features of the proposed rules it finds particularly troubling, including the following:

- *The Unlawful Scope of Information Covered.* The expansive category of information covered by the proposal, which fails to take into account its relative sensitivity, the actual potential for consumer harm related its use and disclosure, or the limits on the Commission's legal authority;[6]

- *Information Overload and Over-Notification.* Repetitive and overly detailed proposed customer notification requirements that would result in significant information overload and over-notification, muting the value of transparency and engendering customer confusion;

- *The Overly Restrictive Approval Framework.* An impractical customer approval framework that would restrict many beneficial uses and disclosures of data by requiring opt-in approval for the vast majority of uses and disclosures of customer data, even in cases where there is little or no privacy risk to consumers; and

---

[5] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8080-81 ¶¶ 24-25 (1998) ("*1998 CPNI Order*").

[6] The Commission's legal authority to adopt broadband privacy rules will become even more suspect should the D.C. Circuit reverse the Commission's reclassification of mobile broadband as a telecommunications service in the Open Internet proceeding. *See Protecting and Promoting the Open Internet*, 30 FCC Rcd 5601(2015), appeal pending sub nom., *United States Telecom Ass'n v. FCC*, Case No. 15-1063 (D.C. Cir., filed Mar. 23, 2015).

- *The Prescriptive and Unreasonable Data Security Requirements.* Data security requirements, including potentially a strict liability standard, for an expansive category of data that would impose substantial burdens regardless of any potential harm to consumers.

This unwise and prescriptive framework would apply exclusively to ISPs, and *not* to other providers in the Internet ecosystem, which would remain subject to the more workable and reasonable framework overseen by the Federal Trade Commission ("FTC"). This approach would result in competitive disparities and consumer confusion and would not serve the public interest. Given that the proposed rules are based on flawed legal interpretations, pose substantial operational challenges, and ultimately would not serve consumers, the Commission should abandon its pursuit of the regime contemplated by the NPRM. Instead, it should pursue its goals in a manner consistent with the FTC's framework, as set forth by the joint industry proposal discussed herein.[7]

## II. THE NPRM OVERSTATES ISPS' CAPABILITIES, UNDERESTIMATES THE COMPLEXITY OF THE INTERNET ECOSYSTEM, AND FAILS TO SHOW THAT THE PROPOSAL WOULD BENEFIT CONSUMERS

The Commission's proposal is predicated on a fundamental misunderstanding of the Internet ecosystem and a plethora of false assumptions. Specifically, the NPRM presumes that ISPs have exclusive access to consumer data unavailable to edge providers. The Commission also asserts that its proposal is consistent with consumer expectations. Finally, the NPRM asserts that the proposed rules will benefit consumers, without demonstrating as much or conducting any type of cost-benefit analysis. The Commission should not and cannot base burdensome, prescriptive rules on these flawed and factually inaccurate assumptions.

[7] *See infra* Section III.C.

### A. ISPs Do Not Have Exclusive Access to Consumer Data or Even Greater Access than Many Other Internet Marketplace Participants

The proposal is founded on the allegedly unique access enjoyed by BIAS providers. According to the Commission, BIAS providers "have the ability to capture a breadth of data that an individual streaming video provider, search engine or even e-commerce site simply does not."[8] This underlying premise is false.

BIAS providers' access to user data is neither unique nor comprehensive. A recent paper by privacy expert Peter Swire explained in great detail the technical and marketplace realities of the Internet ecosystem.[9] According to Swire, developments such as consumers' use of multiple ISPs and devices and the increasing prevalence of encryption and proxy services have eroded whatever expansive access that BIAS providers once might have had to their users' traffic:

> [T]he evidence does not support a claim that ISPs have "comprehensive" knowledge about their subscribers' Internet activity, for encryption and other technological reasons. Similarly, ISPs lack "unique" insights into users' activity, given the many contexts where other players in the ecosystem gain insight but ISPs do not, and the leading role in cross-context and cross-device tracking played by non-ISPs.[10]

When traffic is encrypted, ISPs lack the ability to see users' content and detailed URLs.[11] Today, *all* of the top 10 most visited websites and 42 out of the top 50 websites online are encrypted, and encryption is trending upward, with a substantial majority of Internet traffic

---

[8] NPRM ¶ 4.

[9] Peter Swire et al., *Online Privacy and ISPS: ISP Access to Consumer Data is Limited and Often Less than Access by Others* (The Institute for Information Security & Privacy at Georgia Tech, (Feb. 29, 2016), http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf.

[10] *Id.* at 123.

[11] *Id.* at 3.

expected to be encrypted by the end of 2016.[12] Moreover, a growing number of Internet users utilize proxy services, such as Virtual Private Networks, which block ISPs' ability to see even the domain name that the user is visiting.[13] On the other hand, it is widely recognized that many edge providers have the ability to track user Internet activity across multiple websites, despite the NPRM's assumption that ISPs have unique capabilities.[14]

The Commission should not ignore these technical and marketplace realities simply to justify ISP-specific rules. Indeed, the FTC – the primary data privacy and security regulator in the United States – has rejected the notion that ISPs warrant privacy mandates beyond those applied to other large platform providers within the Internet ecosystem, such as operating system and browser providers.[15] Moreover, assuming *arguendo* that ISPs *were* different from edge

---

[12] *Id.* at 3, 28.

[13] *Id.* at 3.

[14] *See* NPRM ¶ 4. Virtually all major websites utilize some form of analytics that enable the website provider to understand who is visiting the site, how often, and from what other pages. As demonstrated in a recent Princeton study, the top 5 third party analytics providers, as well as 12 of the top 20, are Google-owned domains. Steven Englehardt & Arvind Narayanan, *Online tracking: A 1-million-site measurement and analysis*, at 9, Princeton University (Draft: May 18, 2016), http://randomwalker.info/publications/OpenWPM_-1_million_site_tracking_measurement.pdf. Google therefore has the ability to track users across websites and monetize that information. Similarly, any page that has a Facebook "like" button embedded in it will share information about the user's interaction with a central point – Facebook. Because of the scale of these providers, they are uniquely positioned in their ability to track individual users across different devices. *See* Ad Tech Daily, Press Release, *Adobe Announces Cross-Device Co-op to Enable People-Based Marketing* (Mar. 29, 2016), http://adtechdaily.com/2016/03/29/adobe-announces-cross-device-co-op-enable-people-based-marketing/.

[15] *See* FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, at 56 (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf ("FTC Privacy Report") (noting that "ISPs are just one type of large platform provider" and that "any privacy framework should be technology neutral"); *see also id.* at 56 n.270. Moreover, while the FTC Privacy Report discussed concerns about potential tracking capabilities of large platform providers, including but not limited to ISPs, it did not state such providers should be subject to a strict opt-in regime. *See id.* at 56

providers, the NPRM makes no attempt to tailor its proposed rules to those purported differences. In fact, the NPRM seeks to regulate BIAS practices with respect to data that *any* business (for example, a retailer) may hold about its customers,[16] thus quickly disregarding its underlying justification for the proposed rules – *i.e.*, that ISPs are unique and therefore require more prescriptive regulation.

### B. The NPRM Misunderstands Consumer Expectations

Nor are the proposed rules consistent with consumer expectations or needs. Rather, the NPRM departs from the framework that applies more broadly today to the Internet ecosystem – and thus the consumer experience. In fact, the proposed rules represent a substantial departure from the current approach to privacy on the Internet, which provides the basis for current consumer expectations and which will continue to govern the vast majority of consumers' online interactions.

Critically, the proposal fails to take into account the fact that customer expectations and preferences differ based on the sensitivity of the information used and shared.[17] Consumers *expect* some kinds of information to be used for various purposes, including marketing.[18]

---

[16] Specifically, countless consumer-facing businesses other than BIAS providers may hold customer information such as a customer's name, address, contact information, and transactional information. Such businesses' use and disclosure of such information generally are subject to the FTC's deception and unfairness authority. Yet, in this proceeding, the NPRM would apply prescriptive rules to BIAS providers' treatment of such information, in many cases requiring opt-in consent, even though there is absolutely nothing about such information that is uniquely related to BIAS.

[17] Tellingly, in a recent survey, more than 83% of Internet users said that data protections should vary based on the data's sensitivity. *See* Comments of Progressive Policy Institute, WC Docket No. 16-106 (filed May 27, 2016) ("PPI Comments") (submitting recent survey by Public Opinion Strategies and Peter D. Hart ("POS Survey")).

[18] *See, e.g.*, Accenture, News Release, *U.S. Consumers Want More Personalized Retail Experience and Control over Personal Information, Accenture Survey Shows* (Mar. 9, 2015), https://newsroom.accenture.com/industries/retail/us-consumers-want-more-personalized-retail-

Moreover, consumers care most about *what* data is gathered and used about them – namely, *sensitive* data that is used in ways that would surprise them – without regard to *who* holds such data. While the NPRM claims to provide consumers with choice,[19] in reality it sets the baseline too high and fails to tailor its proposals to actual consumer expectations, or to base them on targeted research – potentially prohibiting practices most consumers would prefer.[20] The NPRM also contends that consumers have special expectations with regard to their broadband providers, but fails to cite any actual support for the proposition.[21] In fact, as a recent consumer survey shows, consumers do not distinguish between their BIAS provider's and edge providers' respective access to their information.[22] Thus, rather than meeting consumers' expectations, the proposal would cause substantial consumer confusion, with highly restrictive rules applying to

---

experience-and-control-over-personal-information-accenture-survey-shows.htm (finding that nearly 60% of consumers want real-time promotions and offers, and "many consumers are willing to share some personal details with retailers" while still wishing to retain greater control over other classes of data).

[19] *See, e.g.*, NPRM ¶¶ 14, 16, 18.

[20] T-Mobile agrees with the views of policymakers who have emphasized the importance of tailored rules. *See* Maureen K. Ohlhausen, Commissioner, FTC, Remarks at Public Policy Briefing at the George Mason University School of Law: The FTC, The FCC, and BIAS, at 6 (Mar. 30, 2016) ("In establishing the proper baseline of prohibited practices, regulators must avoid bias. If regulators set the baseline too low, it would not stop harmful practices that most consumers oppose. Too high, and it would prohibit services many consumers would prefer. Indeed, too high a privacy baseline – a biased baseline – imposes the privacy preferences of the few on the many.").

[21] Moreover, the NPRM fails to address its disruption of consumer expectations of uniform data treatment *post*-acquisition. Consumer expectations are based on the type of data at issue and do not change across service, platform, and medium. This is particularly so with data that is collected in identical ways, *e.g.*, through registration in a web form or making a purchase at a retail store.

[22] *See* PPI Comments (submitting POS Survey findings that 90% of Internet users believe all Internet companies should operate under the same set of rules and regulations and that only 12% believe that the extent of data protection should vary based on the type of Internet company that uses the data). If anything, consumer expectations cut the opposite direction. *See id.* (consumers believe search engines, browsers, and social networks have more access to their data than ISPs).

BIAS, while edge providers and others remain free to use the very same customer information. As a result, highly restrictive BIAS privacy regulation will not actually result in greater customer privacy for the expansive amount of information proposed to be subject to new rules. Non-BIAS entities will continue to use and share that information, mostly subject to inferred or opt-out consent under the FTC's regime.

As described further below, the NPRM also proposes regulatory distinctions that bear no relation to consumers' expectations or the potential for harm. For example, the proposed rules would treat the first-party marketing of communications-related services differently from the first-party marketing of non-communications-related services. This distinction simply is not consistent with consumers' expectations – fostered by the existing CPNI rules – that a company providing one set of services will be able to offer discounted bundles involving other offerings. [23]

The NPRM's discussion of consumer expectations with respect to the sharing of information with third parties is also flawed. According to the NPRM, "customers view the use of their personal information by their broadband provider differently than disclosure to or use by a third party for a variety of reasons."[24] But the NPRM bases this conclusion entirely on a 14-year old order that does not address broadband providers and fails itself to identify any

[23] Under the "total service approach" rules, regulated entities can "use CPNI to market new product offerings within the carrier-customer service relationship, on the basis of the customer's implied consent." *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, et al.*, Third Report and Order and Third Notice of Proposed Rulemaking, 17 FCC Rcd 14860, 14863 ¶ 2 (2002) ("*2002 CPNI Order*") (citation omitted). In that vein, the FTC framework does not require choice for first party marketing of non-sensitive data. FTC Privacy Report at 40.

[24] NPRM ¶ 129 (citation omitted).

"research."[25] The NPRM also asserts that "studies from the Pew Research Center show that the vast majority of adults deem it important to control who can get information about them,"[26] but the NPRM overstates these studies and their application here.[27] The studies do not support the Commission's specific proposals, nor do they support rules that treat ISPs differently than other online entities.

Ultimately, the NPRM denies informed consumers the ability to make their own decisions about the use and sharing of their information in the same manner as they have for years. Instead, the NPRM assumes that consumers are better off if the Commission makes such decisions for them.[28] Such determinations are inconsistent with consumer expectations today and would hamper ISPs from keeping pace with the other major players in the Internet ecosystem in meeting customer preferences.[29]

---

[25] *See 2002 CPNI Order*, 17 FCC Rcd at 14883 ¶ 51 (asserting that "the record unequivocally demonstrates that, in contrast to intra-company use and disclosure of CPNI, there is a more substantial privacy interest with respect to third-party disclosures").

[26] NPRM ¶ 129 (citation omitted).

[27] The Pew studies are not specific to BIAS providers; they also address the activities of edge providers such as Google and Facebook, which the NPRM does not cover. Moreover, the studies do not provide the granularity necessary to support the specific proposals here. Rather, they express merely the general (and utterly unsurprising) view that customers place some value on their privacy. And they do not acknowledge the trade-offs that customers routinely make with respect to their data, which provide concrete evidence regarding their wishes and expectations with regard to their privacy. This includes, for example, the posting of extremely personal information on a social media website, giving a retail store employee an email address to get promotions, or even saving credit card information to an e-commerce website so it can easily be accessed during a subsequent purchase.

[28] Most egregiously, and as discussed further below, the NPRM considers removing some choices from consumers altogether. *See, e.g.*, NPRM ¶ 24 (inquiring whether certain uses of data should be "prohibited altogether"); *id.* ¶ 266 (considering a *per se* prohibition on deep-packet inspection); *id.* ¶ 272 (asking for recommendations from commenters on potential catch-all prohibitions of any unenumerated activities).

[29] It also would prevent ISPs from innovating in ways that themselves drive changes in customer preferences, as many edge providers have done. For example, at its introduction, Google's

### C. The NPRM Fails to Demonstrate that the Proposed Rules Are Necessary or Will Benefit Consumers

The NPRM also fails to identify a problem with BIAS provider practices that needs to be remedied, or to demonstrate that the existing privacy framework or the marketplace is not protecting consumers. The NPRM asserts without evidence that "[a]bsent legally-binding principles, [broadband] networks have the commercial motivation to use and share extensive and personal information about their customers."[30] This statement is stunning in its tacit dismissal of the prime force that protects customers in the vast majority of industries – *i.e.*, market competition. T-Mobile is keenly aware that if consumers are dissatisfied with T-Mobile's service or its practices, they can and do easily switch to another provider.[31] Any claim that legally binding principles are the only safeguards against "commercial motivation" to mistreat consumers is flatly wrong. ISPs have every incentive to earn and keep the trust of their customers without regulation. Unlike other players within the Internet ecosystem, ISPs' primary revenue source is the consumers who purchase their services. Indeed, unlike many online

---

Gmail service faced pointed criticism based on its practice of scanning email content in order to target ads placed in the window of the email service. Today, Gmail reportedly has one billion users. *See* Ross Miller, *Gmail now has 1 billion monthly active users*, The Verge (Feb. 1, 2016), http://www.theverge.com/2016/2/1/10889492/gmail-1-billion-google-alphabet. Had prescriptive regulation prohibited this use of data, a billion consumers could have been without this free service option.

[30] NPRM ¶ 3.

[31] Indeed, T-Mobile has taken various steps to eliminate so-called "switching costs." *See, e.g.*, T-Mobile, Switch Carriers Without Early Termination Fees, http://www.t-mobile.com/offer/-switch-carriers-no-early-termination-fee.html (last visited May 25, 2016) (explaining how T-Mobile covers switching fees, allowing greater consumer choice by lowering transaction costs to changing). T-Mobile's changes have reverberated among its mobile competitors, only heightening the company's incentives to ensure that its practices cater to customer demands. This is in contrast to the obstacles consumers face when switching among many of their edge providers, which often have unique roles in the public sphere. Abandoning a social network, for example, is not a reasonable option for consumers who want to continue to engage in online expression.

scenarios in which it is unclear who is accessing and using data, consumers know how to find their ISP, learn of its privacy practices, and make their concerns known. Moreover, the NPRM never asserts – nor could it – that ISPs have failed to respect their customers' privacy under the existing framework. In fact, it is noteworthy that in the many years during which the FTC claimed authority over broadband providers, not one of over 100 privacy and data security cases brought by that agency was directed against a broadband provider.[32]

The NPRM also assumes that prescriptive privacy rules are better for consumers than flexible ones. As recognized by both the White House and the FTC, they are not. In espousing "general principles that afford companies discretion in how they implement them," the White House emphasized that "flexibility will help promote innovation" and "encourage effective privacy protections by allowing companies, informed by input from consumers and other stakeholders, to address the privacy issues that are likely to be most important to their customers and users, rather than requiring companies to adhere to a single, rigid set of requirements."[33] It further observed that "United States Internet policy has generally avoided fragmented, prescriptive, and unpredictable rules that frustrate innovation and undermine consumer trust"[34] –

---

[32] The FTC has brought several non-privacy-related cases against ISPs. *See Wrecking the Internet to Save It? The FCC's Net Neutrality Rule: Hearing Before the H. Comm on the Judiciary*, 115th Cong. 18-20 (2015) (statement of Joshua Wright, Comm'r, FTC) (noting FTC actions against AT&T, TracFone, AOL, CompuServe, and Prodigy). However, the FTC appears to have brought only one enforcement action against an ISP that even resembled a privacy matter; the case involved a rogue ISP engaged in fraudulent activities. *See* FTC, Press Release, *FTC Shuts Down Notorious Rogue Internet Service Provider, 3FN Service Specializes in Hosting Spam-Spewing Botnets, Phishing Web sites, Child Pornography, and Other Illegal, Malicious Web Content* (June 4, 2009), https://www.ftc.gov/-news-events/press-releases/2009/06/ftc-shuts-down-notorious-rogue-internet-service-provider-3fn.

[33] White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 2 (Feb. 23, 2012) ("White House Privacy Report").

[34] *Id.* at 24.

conventional wisdom the Commission now second-guesses.[35] The FTC likewise has emphasized the importance of a flexible approach to privacy practices. It designed its privacy framework "to be flexible to permit and encourage innovation," allowing companies to "implement the privacy protections of the framework in a way that is proportional to the nature, sensitivity, and amount of data collected as well as to the size of the business at issue."[36] In sum, while the NPRM purports to offer "flexible" proposals as well,[37] its proposals are anything but.

The NPRM also fails to undertake a cost-benefit analysis to determine what exactly the rules, if adopted, would provide to consumers and at what corresponding cost. As described herein, the proposed rules would impose very significant costs and restraints on broadband providers, including but not limited to increasing ISPs' costs (and therefore prices to consumers) and causing customer confusion. But the NPRM fails to sufficiently take these costs into account. Nor does it consider whether the proposed requirements are tailored to address actual or potential consumer harm. Indeed, in many regards, the proposal fails entirely to account for the likelihood of consumer harm. For example, as described below, because the unduly expansive definition of "customer proprietary information" ("CPI" or "customer PI") does not account for the sensitivity of the data involved or the risk of harm,[38] consumers will be inundated

---

[35] Indeed, even setting aside the harms of fragmentation, the underpinning wisdom of the FCC's approach is questionable in light of studies linking prescriptive privacy regimes with concrete economic harms. *See, e.g.*, Avi Goldfarb and Catherine E. Tucker, *Privacy Regulation and Online Advertising*, Mgmt. Sci. 57.1 (Aug. 5 2010) (contrasting the effects of European Union prescriptive privacy regulation with the then-comparatively more tailored U.S. regime, and finding that the EU's regime resulted in a potentially innovation-deterring decrease in curation effectiveness).

[36] FTC Privacy Report at 9.

[37] *See, e.g.*, NPRM ¶¶ 148, 167.

[38] *See generally id.* ¶ 57 (proposing to define CPI broadly to include any information that falls into CPNI or PII the BIAS provider acquires in connection with the provision of PII); *see also id.*

with notices, requests for consent, and breach notifications, with no way to distinguish between harmful and non-harmful activity. The proposed rules will impose greater costs than benefits, ultimately disserving consumers.

Given that the NPRM fails to identify a true need or consumer benefit requiring its proposed rules, and the general impracticality and burden of such rules, the proposed rules would not only be bad policy if adopted, but also (as explained below) would run afoul of both the First Amendment and the Administrative Procedure Act.

### D. The Commission Should Better Reflect the Expertise of the FTC, the Administration, and Stakeholders in Contemplating Any New Framework

The Commission appropriately has looked to existing sources and the expertise of the FTC to address the complex technical, economic, consumer protection, and legal questions presented in this matter.[39] But rather than following the leads of these experts, the FCC seeks to depart from the wisdom they offer. It should not.

There is a wealth of information on which the Commission can and should rely on creating its privacy framework. The FTC held three roundtables and numerous meetings in the lead-up to the FTC's 2012 Privacy Report to address these complex privacy issues. Moreover, the FTC issued a staff report, sought comment on that report, received over 400 comments, and revised its framework to address many of those comments, including by eliminating most restrictions on first-party marketing.[40] The NPRM asserts that its proposal is consistent with this

---

¶ 60 (proposing to define PII broadly to include any information that is linked or linkable to an individual).

[39] *See id.* ¶ 27 ("Our proposals build on the Commission's prior decisions and existing Section 222 rules; other federal privacy laws; state privacy laws; and recognized privacy best practices….").

[40] *See* FTC Privacy Report at 15-16, 22.

FTC framework, but in fact it sharply diverges from that approach in many fundamental ways. In some cases, it misapplies the FTC's principles and precedents. Perhaps most significantly, the FTC explicitly *rejected* the notion that ISPs should be regulated in a manner different from other large platform providers, noting that "ISPs are just one type of large platform provider" and asserting that "any privacy framework should be technology neutral."[41] In addition, as noted above, the White House has issued its own report, which also endorses a uniform, flexible approach to online privacy regulation.[42]

T-Mobile respectfully urges the Commission to pause to more fully consider these expert views, as well as the experience of providers in the Internet ecosystem. To that end, it should in the first instance pursue a consensus framework, such as that set forth by the American Cable Association, Competitive Carriers Association, CTIA, National Cable & Telecommunications Association, and USTelecom, which is grounded on longstanding FTC principles.[43] Alternatively, to the extent the Commission believes additional efforts to protect consumers online are required, it should work with the National Telecommunications & Information Administration and the FTC to launch an ecosystem-wide multi-stakeholder process to identify what, if any, additional protections are required.

---

[41] *Id.* at 56. Despite the FCC's frequent declarations that its privacy regulations will mirror those of the FTC in theory, the NPRM undercuts this notion in practice. *See, e.g.*, NPRM ¶¶ 154-55 (claiming the FCC will follow FTC guidance on de-identification and aggregation); *id.* ¶¶ 158-59 (immediately seeking comment on non-FTC factors for defining "not reasonably linkable" under new FCC regulations).

[42] White House Privacy Report at 2.

[43] *See* Letter from Meredith Attwell Baker, President and CEO, CTIA, et al., to Tom Wheeler, Chairman, FCC (Mar. 1, 2016) ("Industry Framework"). The proposed framework specifically sets forth guidelines and principles, which, like the NPRM, cover notice, choice, data security and breach notification. The Industry Framework would protect consumer privacy in a way that is consistent with other privacy laws that apply to companies providing services online. *Id.* at 1.

## III. THE SCOPE OF CUSTOMER INFORMATION COVERED BY THE PROPOSED RULES IS LEGALLY IMPERMISSIBLE AND OTHERWISE IMPRACTICAL

The NPRM's proposal paints with far too broad a brush, applying the proposed rules to virtually all information a BIAS provider may hold about a customer. This framework contravenes statutory limits to the Commission's authority and poses substantial implementation challenges and burdens and would negatively impact customers and BIAS providers alike.

### A. The Commission Has No Statutory Authority to Expand the Scope of Section 222 Beyond CPNI

The NPRM's proposed rules are unprecedented in scope. If adopted, they would apply not only to CPNI but also could apply to virtually any customer information a BIAS provider may hold relating to a consumer that does not constitute CPNI, including any PII, a broadly-defined term in the NPRM. The Commission attempts to achieve this result via a grossly overbroad and legally unsustainable reading of Section 222.

Section 222(a) merely states a general principle that is implemented through other provisions, including Sections 222(b) and 222(c).[44] CTIA explained as much in its Petition for Partial Reconsideration of the Commission's *Order on Reconsideration* in its Lifeline reform and modification docket.[45] The core points of the analysis – which T-Mobile hereby incorporates by reference – are as follows:

(1) Section 222(a) is not a standalone grant of authority – rather, it merely identifies the categories of information to which Section 222 applies;

---

[44] Just as Section 222(c) fleshes out carriers' obligations with respect to customer information, other provisions address carriers' obligations with regard to the other entities mentioned in Section 222(a). *See* 47 U.S.C. §§ 222(b) (carrier proprietary network information), 273(d)(2) (equipment manufacturer proprietary information).

[45] *See generally* Petition of CTIA – The Wireless Association® for Partial Reconsideration, WC Docket Nos. 11-42, 09-197, 10-90 (filed Aug. 13, 2015) ("CTIA Petition").

(2) In the case of customer information, the operative provision is Section 222(c), which is expressly limited in scope to CPNI, as that term is defined in Section 222(h)(1), and, more specifically, to *individually identifiable* CPNI;[46]

(3) if Section 222(a) required carriers to protect customer information other than CPNI, then neither Section 222(e)'s directive that carriers disclose subscriber list information nor the other disclosure exceptions in Section 222(d) would make sense; and

(4) Section 222's legislative history confirms that Congress affirmatively *eliminated* from the relevant House and Senate bills catch-all provisions that would have given the Commission broader authority to regulate customer information more generally.[47]

For these reasons, Section 222(a) is nothing more than a general introductory provision; it cannot be read to assign the Commission broad authority over a new, separate, and undefined category of information.[48]

---

[46] Section 222(c)(1) only mandates protection of individually identifiable CPNI. 47 U.S.C. § 222(c)(1) (a telecommunications provider "shall only use, disclose, or permit access to individually identifiable customer proprietary network information"). Section 222(h) limits CPNI to "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship," and certain information contained in bills. *Id.* § 222(h)(1)(A)-(B). Thus, any proposed rules should only apply to information that (1) meets the Section 222(h)(1) definition of CPNI *and* (2) is "individually identifiable."

[47] *See* CTIA Petition at 6 (discussing H.R. REP. NO. 104-204, Pt. 1, at 23 (1995); S. REP. NO. 104-123, at 24 (1995)).

[48] Notably, Section 222(h) defines CPNI in a very specific manner. *See generally* 47 U.S.C. § 222(h)(1). It defies logic and canons of statutory construction to suggest that Congress would define CPNI so specifically yet leave undefined a broader catch-all of "customer proprietary information," that includes but is not limited to CPNI, for the Commission to interpret however it wants in any given context. *See, e.g., Whitman v. Am. Trucking Assns., Inc.*, 531 U.S. 457, 468 (2001) ("Congress ... does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions – it does not, one might say, hide elephants in mouseholes.") (citation omitted); *Main St. Legal Servs. v. NSC*, 811 F.3d 542, 551 (2d Cir. 2016) (statutory subsection followed by subsection particularizing duties "cannot reasonably be construed as a congressional delegation of independent authority").

### B. The Commission's Proposed Inclusion of PII Violates Section 222 and Otherwise Is Unworkable

The Commission nevertheless contends that Congress's use of the term "proprietary information" in Section 222(a) authorizes it to create a new, potentially limitless category of protected data that appears nowhere in the statute, *i.e.*, "customer proprietary information" or "CPI".[49] CPI, as defined by the Commission, includes (1) CPNI and (2) PII, a term that, again, appears nowhere in Section 222 (and that drops the critical term "proprietary" from the analysis).[50] Section 222(a), however, does not give the FCC authority over carriers' handling of consumer data beyond CPNI.[51]

Significantly, Congress used the term "proprietary information" rather than "personal information" or "personally identifiable information" in Section 222(a). This choice reflects Congress's intent to regulate only the service-related customer information uniquely available to carriers by virtue of the customer-carrier relationship, *i.e.*, CPNI.[52] By contrast, PII – such as, for instance, a customer's name, address, and phone number – is available from a variety of

---

[49] Nor, as described below, can Section 222(a) be used to support the various proposals within the NPRM.

[50] NPRM ¶ 57. The NPRM defines PII to include "any information that is linked or linkable to an individual," *id.* ¶ 60, while acknowledging that "not all of the ... listed examples of PII [in the NPRM] are necessarily collected by BIAS providers currently," and that some of them "may never be collected." *Id.* ¶ 62 n.117.

[51] The term "proprietary information" was used in 222(a) to reference CPNI, addressed in Section 222(c), as well as non-consumer-related proprietary information of carriers and equipment manufacturers, addressed in Sections 222(b) and 273(d)(2), respectively. *See* 47 U.S.C. §§ 222(a)-(c), 273(d)(2); *see also* CTIA Petition at 4.

[52] 47 U.S.C. § 222(h)(1)(A). This principle was also embedded in the Commission's CPNI rules that predated Section 222. *See 1998 CPNI Order*, 13 FCC Rcd at 8070 ¶ 7 (citation omitted) ("The *Notice* [*of Proposed Rulemaking*] stated that the Commission's existing CPNI requirements were intended to prohibit AT&T, the BOCs, and GTE from using CPNI obtained from their provision of regulated services to gain a competitive advantage in the unregulated CPE and enhanced services markets.").

sources and thus is not unique to the customer-carrier relationship.[53] In fact, any company – or any person for that matter – can find consumer information (personal or otherwise) on the Internet, often for free through a website such as Spokeo or, for a fee, from data brokers.[54] Moreover, Congress specifically required the publication of certain kinds of PII when it included the Section 222(e) requirement that subscriber list information (defined to include names, numbers, and addresses) be provided by carriers *to any person upon request* for the creation of public directories, and did not specify any privacy or security rules for such subscriber list information. This is hardly indicative of Congressional intent to authorize the Commission to regulate the privacy and security of such information.

Further, where Congress has sought to regulate "personally identifiable information" in other provisions of the Communications Act, it has done so explicitly – including both before and after Congress enacted Section 222 in 1996.[55] Had Congress wanted to address PII at the time it enacted Section 222, it knew how and would have used the term PII. Instead, it chose not to do so, further undercutting the Commission's expansive reading of that provision.

---

[53] Whereas "personal information" and "personally identifiable information" can be held by multiple persons and commercial entities without losing its character as PII, "proprietary information" is data that a person or entity owns to the exclusion of others. A BIAS subscriber cannot claim that information is "proprietary" if other individuals or entities can access the information and use it for their own commercial purposes. Even if Section 222(a) provided authority for a category of information broader than CPNI, which it does not, such information still would not include PII and other personal information, for the reasons described here.

[54] *See* FTC, *Data Brokers: A Call for Transparency and Accountability*, at 8-9, 13 (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[55] Section 631(c)(1) of the Communications Act, which Congress enacted in 1984, provides that, with certain exceptions, a cable operator "shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned ...." 47 U.S.C. § 551(c)(1). Likewise, Section 338(i)(1)(A), which Congress enacted in 2004, directs satellite carriers to advise subscribers of "the nature of personally identifiable information collected or to be collected with respect to the subscriber ...." *Id.* § 338(i)(1)(A).

Even if the Commission had the authority to expand Section 222 to cover PII, the NPRM's proposed definition is essentially boundless. The Commission proposes to define PII as "any information that is linked or linkable to an individual."[56] This concept incorporates no limiting principle – the Commission instead "propose[s] to define PII broadly because of the interrelated nature of different types of personal information and the large risks posed by unauthorized uses and disclosures," without discussing exactly what those risks might be, or why they are "large."[57] The absence of real guidance as to what does and does not constitute PII will impose unreasonable costs and other burdens on BIAS providers without any clear concomitant benefit to their customers.[58]

The NPRM cites several sources for its proposed approach, but either takes those sources out of context or simply misreads them. The FTC, for example, applies a *reasonable* linkability standard to de-identified data, and it excludes data that is not reasonably linkable from its policy framework for PII.[59] The Commission, in contrast, omits the "reasonable" modifier, expanding dramatically the class of information that could be covered by its rules.

Furthermore, the Commission provides no clarity as to what is or is not PII under the new rules. What the Commission *does* supply is an "illustrative, non-exhaustive" laundry list of over

[56] NPRM ¶ 60. According to the NPRM, information is "linked" or "linkable" to an individual "if it can be used on its own, in context, or in combination to identify an individual or to logically associate with other information about a specific individual." *Id.* ¶ 61.

[57] *Id.* ¶ 60.

[58] Moreover, as described in Section IV.B below, if the Commission impermissibly applies Section 222 to a broader set of information than CPNI, it must also apply Section 222's limitations, including with respect to de-identified and aggregate customer information, to the same set of information.

[59] *See* FTC Privacy Report at 20. Similarly, Department of Education regulations define "personally identifiable information" as information that would allow a "*reasonable person* ... who does not have knowledge of the relevant circumstances, to identify the student with *reasonable certainty*." 34 C.F.R. § 99.3(f) (emphasis added).

30 types of information it has deemed to be PII, drawn from a collection of specified and unspecified sources.[60] The proposed definition of PII, in short, amounts to a "we know it when we see it" standard, presumably to be applied by the FCC in specific contexts and cases, chilling business innovation and potentially resulting in enforcement actions for behavior that a BIAS provider could not reasonably have ascertained to have been unlawful beforehand. As such, the definition is impermissibly vague.[61]

This lack of specificity also renders the proposal unlawful in other ways. The Commission's rules and policies "must give fair notice of conduct that is forbidden or required."[62] As discussed above, the definition of PII provides no notice of the conduct being targeted, let alone notice that could be deemed "fair" under any standard.

The NPRM also is wrong to dismiss the relevance of Section 222's subscriber list information exception in the broadband context. In the telephone era, that exception reflected customers' recognition that publicly available information such as their names, postal addresses, and telephone numbers would not be subject to the same protections as truly sensitive data, such

---

[60] NPRM ¶ 62 (citations omitted) ("In order to provide such guidance, we look to a number of sources, including our prior orders, NIST, the FTC, the White House's proposed Consumer Privacy Bill of Rights, and other federal and state statutes and regulations."). The NPRM also notes that "several of [the listed] data elements may overlap with our proposed interpretation of the terms of the CPNI definition." *Id.* ¶ 62. As shown above, the statutory definition of CPNI excludes PII, so any given piece of data must be one or the other – it cannot be both.

[61] *See FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012); *see also Trinity Broadcasting of Fla., Inc. v. FCC*, 211 F.3d 618, 632 (D.C. Cir. 2000), quoting *General Elec. Co. v. EPA*, 53 F.3d 1324, 1333-34 (D.C. Cir. 1995) ("Where ... the regulations and other policy statements are unclear, where the petitioner's interpretation is reasonable, and where the agency itself struggles to provide a definitive reading of the regulatory requirements, a regulated party is not on notice of the agency's ultimate interpretation of the regulations, and may not be punished.").

[62] *Fox*, 132 S. Ct. at 2317 (citation omitted); *see also Trinity Broadcasting*, 211 F.3d at 632, quoting *General Elec. Co.*, 53 F.3d at 1333-34.

as their social security numbers. Broadband customers today recognize similar distinctions with respect to contemporary public information (such as IP addresses). Further, the fact that broadband providers do not publish directories of customer information today does not mean they may not do so in the future. As discussed above, many websites and public records offer such information. The Commission cannot insist that Section 222 *can* be applied to broadband and simultaneously assert that exemptions from the definition of CPNI[63] *cannot*.

### C. The Commission Cannot Promulgate Privacy and Data Security Rules on BIAS Providers through Other Provisions of the Communications Act

The Commission also cannot rely on Sections 201, 705, 706, or Title III provisions of the Communications Act as authority for the proposed rules.[64] Because the NPRM relies principally on Section 222, at this time we address these other provisions only briefly:[65]

- *Section 201(b).* Congress established the parameters of consumer privacy protections in Section 222, and the Commission cannot expand those protections through the more general mandate in Section 201(b). Indeed, the Commission has acknowledged as much, stating that "Congress established a comprehensive new framework in Section 222, which balances principles of privacy and competition in connection with the use and disclosure of CPNI and other customer information."[66]

- *Section 705*. As the NPRM recognizes, Section 705 addresses issues surrounding piracy and the unlawful interception of content.[67] It cannot provide authority for the dramatically expansive privacy rules proposed in the NPRM, which concern issues other than the content of the communications at issue.

---

[63] *See* 47 U.S.C. § 222(h)(1) (CPNI "does not include subscriber list information").

[64] NPRM ¶¶ 304-311.

[65] T-Mobile concurs with the fuller response to these issues in the comments filed in this docket by CTIA. *See* Comments of CTIA, WC Docket No. 16-106, at 59-73 (filed May 26, 2016) ("CTIA Comments").

[66] *1998 CPNI Order*, 13 FCC Rcd at 8073-74 ¶ 14; *see also* H.R. REP. NO. 104-458, at 205 (1996) (Conf. Rep.) (Joint Explanatory Statement of the Committee of Conference) (describing Section 222 as "striv[ing] to balance both competitive and consumer privacy interests with respect to CPNI.").

[67] 47 U.S.C. § 605; NPRM ¶ 307.

- *Section 706.* The Commission cannot rely on Section 706 because, as shown in these comments and others, the proposed rules are not tailored to promote the acceleration of broadband deployment and are, in fact, likely to have the opposite effect, as the proposed regime is likely to hamper BIAS providers' ability to compete and to confuse and frustrate consumers.[68] Section 706 only empowers the Commission to use regulation in ways that "remove barriers to infrastructure investment."[69] The proposed requirements, however, will instead undermine investment.[70] Moreover, the so-called "virtuous cycle" is inapplicable here. That cycle is based on the assumption that users are declining to adopt broadband based on privacy-related concerns. The empirical evidence, however, proves otherwise, especially for mobile broadband service.[71]

- *Section 303(b).* Section 303(b) gives the Commission the authority to "from time to time, as public convenience, interest, or necessity requires ... [p]rescribe the nature of the service to be rendered by each class of licenses [radio] stations ...."[72] The proposed rules, however, relate to the treatment of CPNI, not "the nature of the service" rendered by BIAS providers. Section 303(b) does not authorize the Commission to take whatever action it likes with respect to radio licenses.

- *Section 303(r).* Section 303(r) gives the Commission the authority to impose regulations that are "necessary to carry out the provisions of this chapter ...." Courts have established that Section 303(r)'s "catch-all" authority must be tethered to the use of otherwise delegated authority which, as shown above, does not exist here.[73] Nor, for the reasons discussed herein, can the Commission

---

[68] To the extent Section 706 does provide the FCC authority to address privacy and data security, and it is determined that online privacy and data security concerns indeed inhibit broadband deployment, then it would be arbitrary and capricious for the FCC to apply privacy and data security rule only to BIAS providers and not edge providers.

[69] 47 U.S.C. § 1302(a).

[70] Moody's credit rating agency referred to the NPRM as a "negative" for investors in broadband companies. *See* David Shepardson, *U.S. FCC Internet Privacy Proposal Could Harm Broadband Providers – Moody's*, Reuters (Mar. 15, 2016), http://www.reuters.com/-article/usa-fcc-internet-moodys-idUSL2N16N0UA ("Ratings agency Moody's Investors Services said on Tuesday that a proposal by U.S. communications regulators to impose privacy restrictions on broadband providers … was 'credit-negative.'").

[71] John B. Horrigan and Maeve Duggan, *Home Broadband 2015*, Pew Research Center (Dec. 21, 2015), http://www.pewinternet.org/2015/12/21/home-broadband-2015/; *see also* Brian Whitacre and Colin Rhinesmith, *Broadband Un-Adopters*, Telecommunications Policy, at 5 (2015) (only .018 and .007 of consumers are broadband un-adopters and never-adopters).

[72] 47 U.S.C. § 303(b).

[73] *See, e.g., Motion Picture Ass'n of Am., Inc. v. FCC*, 309 F.3d 796, 806 (D.C. Cir. 2002).

demonstrate that the proposed rules are necessary to achieve its objective in this proceeding.

- *Section 316.* Section 316 only gives the Commission the authority to modify the actual terms of station licenses.[74] No licenses or modifications are at issue here, so the statute is irrelevant.

* * *

In sum, the Commission does not have the authority to adopt its proposed broadband privacy rules. This should come as no surprise: When Congress enacted Section 222, it neither envisioned nor intended that the Commission would apply the statute to a service other than voice telephony. Indeed, the statute is replete with voice-related terminology and repeatedly refers to telecommunications services, which at the time were not understood to include Internet access.[75] The Commission should not resort to legal gymnastics to achieve what nevertheless will be an unlawful result.[76] Rather, any new privacy regulations for BIAS providers must be limited to CPNI, as that term is defined in Section 222(h).[77]

---

[74] 47 U.S.C. § 316.

[75] Section 222 refers to, for example, "call[s]," "call location information," "local exchange carriers," "telephone exchange service," "telephone toll service," and "telemarketing." The provision's only Internet-related reference is in Section 222(d)(4), which creates an exception for "call location information concerning the user ... of an IP-enabled voice service." 47 U.S.C. § 222(d)(4). Congress created that exception in 2008 only to ensure that first responders could receive information necessary to locate callers who used Internet-enabled voice services. H.R. RPT. NO. 110-442 (2007). This amendment, of course, was not intended to dramatically expand the scope of the statute to include all BIAS.

[76] Some have argued that Section 222 commands the Commission to impose the proposed rules. The NPRM, however, relies on an incorrect interpretation of Section 222 and, whenever convenient, departs from the statute's limitations to capture a breadth of data and practices not actually covered by Section 222. Thus, any suggestion that Section 222 compels these proposed rules is misguided, even assuming *arguendo* that Section 222 could apply to BIAS.

[77] If, on the other hand, the Commission is deemed to have the statutory authority to adopt its proposed rules, then it can and should adopt the industry privacy proposal previously submitted by CTIA, USTelecom, NCTA, the American Cable Association, and the Competitive Carriers Association. *See* Industry Framework.

## IV. THE PROPOSED RESTRICTIONS ON THE USE AND DISCLOSURE OF CUSTOMER INFORMATION ARE UNLAWFUL AND IMPRACTICABLE AND WILL ELIMINATE BENEFICIAL PRODUCTS AND SERVICES

### A. The Proposed Tiered Approval Regime Outstrips Commission Authority, Radically Departs from Existing Framework, and Ignores Real Consumer Expectations

The NPRM states that the proposed rules, "like the existing CPNI rules, are intended to directly advance both the substantial public interest in consumer privacy as well as Section 222's mandate to protect customer confidentiality, while not being more extensive than necessary to serve those interests, according to the criteria of *Central Hudson*."[78] The NPRM further asserts that the "proposed rules correspond with well-established rules in the voice context … imposing no more restrictions than are necessary to protect customer privacy and control."[79] The NPRM is wrong on both accounts.

Because, as described above, Section 222(a) does not provide the Commission with standalone authority, it cannot be the basis for FCC rules. Thus, the Commission must limit any privacy regulations rules that implement the "[p]rivacy requirements for telecommunications carriers" set forth in Section 222(c)(1).[80] The proposal, however, not only exceeds the limits of Section 222, but it in fact offers only illusory benefits to consumer privacy and thus fails entirely to advance a substantial public interest. It sets the baseline for broadband privacy too high, at great expense and in a manner far more extensive than necessary to achieve any incremental

[78] NPRM ¶ 302 (citing *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557 (1980)).

[79] *Id.*

[80] 47 U.S.C. § 222(c)(1).

benefit. As a result, that framework disregards Section 222 and actually runs afoul of *Central Hudson* and the First Amendment.[81]

The Supreme Court has noted that "[p]recision of regulation must be the touchstone" in the case of broad limits on speech, which "so closely touch[] on our most precious freedoms."[82] Here, where the proposed speech is lawful and not misleading, the regulation must directly advance a substantial government interest and be no more extensive than necessary to serve that interest.[83] But the proposed opt-in requirement for virtually all forms of customer information does not materially advance *any* government interest. As described below, the NPRM's proposed approval framework will stifle innovation, confuse consumers, and hamper BIAS providers' ability to provide a seamless consumer experience. Therefore, it does not materially advance consumer interests and certainly is more extensive than necessary to serve that interest.[84]

The proposed approval framework also is bad policy. In the mobile broadband space, consumers expect and demand a flexible user experience that promotes privacy while enabling

---

[81] *See Central Hudson* at 569-70 (complete suppression of speech ordinarily protected by the First Amendment must be no more extensive than necessary); *see also US WEST v. FCC*, 182 F.3d 1224 (10th Cir. 1999) (vacating a Commission order on First Amendment grounds, when the agency had restricted use and disclosure of CPNI for marketing by requiring companies to obtain opt-in consent).

[82] *Edenfield v. Fane*, 507 U.S. 761 (1993) (quoting *NAACP v. Button*, 371 U.S. 415, 438, (1963). Moreover, the Supreme Court particularly disfavors regulations that, as here, target one specific type of speaker even while others who are similarly situated are not subject to the restriction. *See Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011). In the case, the invalidated law singled out pharmacies' use of personal data for marketing. The Supreme Court found that, in a case targeting particular forms of speech by particular speakers, a stricter standard than the *Central Hudson* test should be applied.

[83] *Central Hudson* at 564.

[84] T-Mobile concurs with CTIA's analysis concluding that the proposed approval regime runs afoul of the First Amendment. *See* CTIA Comments at 73-93.

access to robust mobile services. A *Consumer Reports* survey found that 66% of consumers were irritated by being asked several times for the same information; and speed of issue resolution is key for consumers.[85] Regulations that frustrate provider efforts to respond to these concerns frustrate consumers. After years of familiarity with the existing privacy framework governing the entire Internet ecosystem, mobile consumers generally are not surprised when non-sensitive and readily available information held about them is used and disclosed, without opt-in consent, in ways that do not harm them and more often than not *benefit* them. The Commission's proposal fails to establish a coherent consent framework that is commensurate with consumer expectations.[86]

### 1. The Proposal to Require Opt-In Consent for Most Uses and Disclosures of Customer Information Would Fail Consumers

The proposed rules would dramatically expand opt-in consent requirements for most types of consumer data. As an initial matter, this proposal would not have withstood a cost-benefit analysis had the Commission performed one. And even absent such an analysis, it is simply unreasonable to think that most types of customer information should be subject to a restrictive opt-in requirement. The opt-out framework that now applies to the Internet ecosystem has prompted the development of innovative new services that benefit consumers, while still allowing them to make informed choices about how their data is used. In contrast, sweeping opt-in mandates would hamstring BIAS providers' ability to develop and deploy services to

[85] Consumer Reports, *Your Call Is Important to Us: The problem with customer service* (July 29, 2015), http://www.consumerreports.org/cro/magazine/2015/07/the-problem-with-customer-service/index.htm; Talkdesk, *What Customers Want from Support Contact Centers* (Aug. 25, 2015), https://www.talkdesk.com/resources/infographics/what-customers-want-from-support-contact-centers ("problems solved quickly" was top choice of consumers).

[86] *See generally* PPI Comments (submitting POS survey).

consumers, and thus will make consumers worse off without providing additional benefit.[87] In some cases, the restrictive rules could even force BIAS providers to roll back beneficial services and innovations customers are enjoying today.

Given the breakneck speed of innovation in the mobile broadband environment (and elsewhere), new services are offered constantly, and consumers will quickly become fatigued by the sheer number of opt-in requests, including for many data uses that do not give rise to any potential harm. Consumers today neither expect nor wish to opt in for each and every use or disclosure of their non-sensitive customer information for which consent is not inferred.[88] They understand that the use and disclosure of their information on the Internet generally is governed by privacy policies of the websites they visit and the services they use, and that they have choices about many such uses. In that light, an opt-in requirement could be confusing to the extent consumers do not distinguish between rules for data use by BIAS providers, OS providers, and edge service providers.[89] Consumers neither expect nor want to be barraged with notices

---

[87] *See, e.g.*, Maureen K. Ohlhausen, Commissioner, FTC, Remarks at the Free State Foundation Eighth Annual Telecom Policy Conference: Privacy in the Internet Ecosystem, at 8 (Mar. 23, 2016) ("[O]pt in mandates unavoidably *reduce* consumer choice. First, one subtle way in which a privacy baseline might be set too high is if the default opt in condition does not match the average consumer preference. If the FCC mandates opt in for a specific data collection, but a majority of consumers already prefer to share that information, the mandate unnecessarily raises costs to companies and consumers. Second, opt in mandates prevent unanticipated beneficial uses of data.").

[88] The NPRM refers to "implied approval" (*see, e.g.*, NPRM ¶ 110), whereas the proposed rules refer to "inferred" approval. *See* Proposed Section 64.7002(a). Given that these terms appear to be used interchangeably in the NPRM, we use the term "inferred" to refer to this concept.

[89] *See* Statement of Commissioner Rosenworcel ("consumers can be confused by these distinctions"); Jim Halpert, *Why Privacy Pros Should Care About the FCC's Broadband Privacy Rules*, IAPP (Apr. 5, 2016), https://iapp.org/news/a/why-privacy-professionals-should-care-about-the-fccs-broadband-privacy-rulemaking/ ("Consumers are unlikely to understand if asked to consent to ISP uses of information that the consumer choices apply only to the ISP and would have no bearing on use of consumer data elsewhere in the Internet ecosystem.").

and choices on a case-by-case basis regarding unsurprising uses of their non-sensitive information. Indeed, the only surprise in store for consumers is the one promised by the NPRM's consent proposal – namely, the frequency with which they would be asked to permit specific uses of their information.[90] And again, consumers do not expect that their broadband provider operates in a different manner as providers of other Internet services with respect to how their information is used and disclosed. Thus, consumers do not, and would not, expect to provide opt-in consent for uses of their non-sensitive information.

For these reasons, the Commission should abandon its default opt-in proposal. Instead, consistent with the FTC's guidance [91] and previous FCC thinking,[92] it should afford providers flexibility to adapt to changing consumer expectations by providing consumers with easy-to-use choice mechanisms governing any non-contextual use or disclosure of their information. Opt-in should be reserved very sensitive information whose use or disclosure would surprise consumers, and because that determination may change with time and circumstances, the rules must be flexible enough to account for such change.

[90] *See* NPRM ¶ 106 n.186 (recognizing that consumers' ability to exercise choice can be eroded through "notice fatigue").

[91] *See, e.g.*, FTC Privacy Report at 50 ("Industry is well positioned to design and develop choice mechanisms that are practical for particular business models or contexts, and that also advance the fundamental goal of giving consumers the ability to make informed and meaningful decisions about their privacy.").

[92] In the past the FCC has explicitly declined to impose specific privacy rules because it did "not wish to artificially constrain the still-developing market for location-based services…." *Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices*, 17 FCC Rcd 14832, 14832 ¶ 1 (2002).

### 2. The Proposal to Allow Opt-Out Consent Only for Marketing Communications-Related Services Poses Operational Challenges

The NPRM's proposal to allow providers to rely on notice and the opportunity to opt out in the narrow case of marketing communications-related services also poses compliance challenges.[93] In particular, the combination of the Commission's narrow definition of "communications-related services"[94] and its unduly broad definition of CPI (which is not qualified by the sensitivity or proprietary nature of such information)[95] would result in troubling confusion. The NPRM's approach fails to serve consumers, as it considers telecommunications service in a vacuum, rather than recognizing that consumers want products and services that meet their day-to-day needs, regardless of whether they meet an arbitrary and technical definition of "communications-related services."

Moreover, the proposed "opt-out" regime departs dramatically from the way the Internet works (and works well) today. The NPRM proposes to require a BIAS provider to solicit customer approval when the provider first intends to use or disclose the customer's information in a manner that requires consent.[96] The Commission further proposes that the notification include "the types of customer PI for which the provider is seeking customer approval to use, disclose or permit access to; the purposes for which such customer PI will be used; and the entity or types of entities with which such customer PI will be shared."[97] This prescriptive approach, however, is simply unnecessary – as noted above, consumers know where to go to learn more

[93] As described above, it also relies on a distinction that largely is arbitrary to the consumer.

[94] *See* NPRM ¶ 72.

[95] As described above, the FCC's application of rules to CPI is neither lawful nor practicable.

[96] *See* NPRM ¶ 140.

[97] *Id.*

and to exercise the choices they have with respect to the use and disclosure of their information by their ISP.

### 3. The Proposed Inferred Consent Category Is Far Too Narrow, As Many Uses of Non-Sensitive Information Need Not Require Additional Approval

Also troubling is the NPRM's very narrow "inferred consent" category. The Commission appears to recognize that uses of customer data to diagnose and quickly address any problems with a broadband provider's network do not pose a risk to consumer privacy.[98] However, consumers expect other uses of their information that benefit them and/or the public interest, and such uses should not be subject to separate opt-in consent. For example, providers should be free to use customer information for fraud prevention outside of BIAS. Mobile telecommunications providers have the technological capabilities to offer much-needed and pro-consumer services. These services, among other things, can confirm that a consumer is in the country or geographic location where his or her credit card was used or where money was withdrawn from his or her account. Such uses of information serve consumers and do not pose any real privacy risks. Here, an opt-in requirement itself could impose harm, as the customer simply may not recognize the benefits available and thus may not choose to utilize the service. As a result, the consumer may be subject to annoyance (*e.g.*, when transactions the consumer tries to make are declined) or, worse, fraud.

Consistent with the FTC's findings and First Amendment jurisprudence, the FCC also should not restrict first-party marketing. The FTC has found that "the first-party collection and use of non-sensitive data ... creates fewer privacy concerns than practices that involve sensitive

[98] *See id.* ¶ 113.

data or sharing with third parties" [99] and thus do not require active consent.[100] Such restrictions do not serve a compelling government interest,[101] and therefore are constitutionally unsound.

In addition, consistent with the FTC's framework, providers should be free to use non-sensitive customer information for other innocuous and consumer-friendly purposes, including affiliate sharing, as long as the affiliate relationship is reasonably clear to consumers.[102] Consumers expect such uses of their information whether or not it's a communications-related or broadband-specific service and neither expect nor desire to be inundated with notices about their ability to opt in or decline.

#### 4. The Proposed Rules May Unduly Complicate BIAS Providers' Use of Vendors to Provide Seamless, Cost-Effective, and High-Quality Service to Consumers

The Commission's proposed consent framework also appears to be problematic for BIAS providers' use of third-party vendors for a variety of functions essential for helping maintain the quality of service consumers expect. The NPRM appears to have attempted to allow reliance on vendors through inferred consent, but the inferred consent is far too narrow to account for the ways in which carriers may use vendors. For example, proposed Section 64.7002(a) arguably would permit carriers to disclose customer PI to third parties without a customer's consent *only*

[99] FTC Privacy Report at 15-16 (citation omitted).

[100] *See id.* at 40 ("[M]ost first-party marketing practices are consistent with the customer's relationship with the business and thus do not necessitate consumer choice.").

[101] In fact, the FTC has said that first party marketing should only require affirmative express consent when it is "*designed to target* consumers based on sensitive data – including data about children, financial and health information, Social Security numbers, and certain geolocation data" because "the risks to consumers may not justify the potential burdens on general audience businesses that *incidentally collect* and use sensitive information." *Id.* at 47-48.

[102] *See id.* at 43.

for very narrow purposes, including to provide BIAS and bill for the service.[103] Other disclosures to vendors appear to require *opt-in* consent.[104]

The proposed framework's limitations on sharing customer information with vendors are unnecessary and may threaten the ability of BIAS providers to provide quality services through a seamless customer experience. Broadband providers already face strong incentives to include contractual provisions in their vendor agreements and oversee their vendors to ensure that they protect customer information and use it only for the services performed on behalf of the provider, and vendors are themselves regulated.[105] The proposal could have the unintended consequence of reducing the utility of using vendors to provide many routine services if those services fall outside the narrow category of uses permitting "inferred" consent. Again, this impact would come without a corresponding benefit to consumers.

[103] Other purposes include to protect the BIAS provider or uses; for marketing and other services only at a customer's initiation; public safety and emergency purposes; and as required by law. *See* Proposed 47 C.F.R. § 64.7002(a).

[104] Neither proposed Section 64.7002(b) (permitting use of CPI for marketing of additional BIAS services in the category to which the customer already subscribes) nor proposed Section 64.7002(e) (requiring opt-in or opt-out approval for disclosure of CPI to affiliates for marketing of communications-related services) would apply to third-party vendors.

[105] If vendors are telecommunications carriers, they will be subject to the same rules as their principal(s); if they are not, they will be subject to the FTC's authority and other applicable privacy laws; and in addition to federal regulation, they would be subject to state laws and in many cases self-regulatory regimes. These mandates will protect consumers without forcing broadband providers to burden their customers with unnecessary approval requests, or subjecting consumers to any meaningful risk that their information will be disclosed without their consent.

### B. The Commission Must Respect Congressional Limitations on Section 222

Even if the Commission unlawfully ignores Section 222's limitation to CPNI[106] and applies the proposed framework to a broader set of customer information, it must still give effect to statutory exemptions for data that is not individually identifiable or is aggregated.

#### 1. Section 222 Precludes Application of the Proposed Rules to De-Identified Data of Any Type

The NPRM asks for comment on how de-identified but non-collective data should be treated under Section 222 and the Commission's rules.[107] In particular, the Commission asks whether Section 222 requires it to conclude that "all CPNI should be considered individually identifiable [and thus cannot be disclosed] unless it meets the definition of aggregate,[108] *i.e.*, is both de-identified and collective."[109] The answer to this question is clearly no.

As a preliminary matter, such a regulation would not be supported by the statute's language. Specifically, Section 222 defines CPNI as

> (A) Information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by a customer of the telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
>
> (B) Information contained in the bills pertaining to [certain telecommunications services] received by a customer of a carrier.[110]

---

[106] *See supra* Section III.A.

[107] NPRM ¶ 165.

[108] Under Section 222(c)(3), carriers may use, disclose, or permit access to aggregate customer information. Section 222(h)(2) defines aggregate customer information as "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed. 47 U.S.C. §§ 222(c)(3), (h)(2).

[109] NPRM ¶ 165.

[110] 47 U.S.C. § 222(h)1(A)-(B).

Nothing in this definition limits CPNI to "individually identifiable" information – rather, the concept of individually identifiable information is a subset of CPNI to which Congress afforded special treatment under Section 222(c)(1).

Section 222(c), however, applies only to a subclass of CPNI – *i.e.*, to that subset of CPNI that is "individually identifiable."[111] Accordingly, any information that does not identify an individual – *i.e.*, information that is de-identified – cannot and should not be covered under the proposed rules, regardless of aggregation. Even when such information is CPNI, it by definition is not "*individually identifiable*" CPNI. Congress elected to include particular language in one section of the Act, and exclude it in others. Thus, principles of sound statutory construction require the Commission to limit any proposed rules on choice (as well as notice, data security and breach notification) to the class of CPNI protected by Section 222(c)(1) – which does *not* cover de-identified data.

Moreover, there is no reason to draw de-identified data within the scope of the proposed rules given the routine safeguards and solutions that are available to providers to protect consumers from re-identification of such data. The FTC has determined that reasonably de-identified data are not "reasonably linkable" if the data holder (i) takes measures to ensure that the data is de-identified; (ii) publicly commits not to try to re-identify the data; and (iii) contractually prohibits downstream recipients from trying to re-identify the data.[112] These

---

[111] *See* Reply Comments of T-Mobile USA, Inc., WC Docket No. 13-306, at 2 (filed Mar. 4, 2014) ("T-Mobile WC Docket No. 13-306 Reply Comments"); 47 U.S.C. § 222(c)(1) (applying protections to "*individually identifiable* customer proprietary network information") (emphasis added).

[112] FTC Privacy Report at iv, 21 (discussing appropriate steps to minimize reasonable linkability of information); *see also* Letter from Maneesha Mithal, Associate Director, Division of Privacy & Identity Protection, FTC to Reed Freeman, Counsel to Netflix, Inc. (Mar. 12, 2010),

protections are sufficient to protect and meet the legitimate privacy expectations of consumers, and there is no reason for the Commission to depart from the FTC's expert guidance here.

Finally, the use or sharing of de-identified data (whether aggregated or not) provides a variety of significant public interest benefits. For example, such data provides the ability to, among other things: (1) monitor and contain the spread of infectious diseases; (2) improve health research; (3) improve traffic patterns and transportation infrastructure; (4) analyze disaster recovery efforts; and (5) monitor socio-economic conditions.[113] Use of de-identified data also gives ISPs the ability to provide subscribers with relevant advertising and associated discounts. De-identification is also an important data security measure – one that the NPRM's overreaching efforts would ironically discourage. Thus, restrictions on the use or sharing of de-identified data – particularly the inclusion of such use and sharing in an opt-in regime – puts all of these benefits at risk, and does so without advancing the interests of consumers or the protection of privacy generally.[114]

---

https://www.ftc.gov/sites/default/files/documents/closing_letters/netflix-inc./100312netflixletter.pdf (closing investigation in light of Netflix's assurances of contractual and operational safeguards to prevent anonymized data it releases from being used to re-identify consumers); T-Mobile WC Docket No. 13-306 Reply Comments at 3-7. Similar conclusions have been reached by other policy makers and academics alike. *See id.* at 6 n.24 and the comments cited therein. For instance, according to the Future of Privacy Forum, "today's sophisticated anonymization tools can make re-identification unlikely and difficult even with publicly [available] data sources at hand." *Id.* at 6-7 (citation omitted). As a result, "the risk of privacy harm from re-identification is significantly lower than many risks we take without concern, such as throwing out our trash." *Id.* at 7 (citation omitted).

[113] T-Mobile WC Docket No. 13-306 Reply Comments at 7-8.

[114] Nor would restrictions on use of de-identified data stop consumers from receiving targeted advertising, as the proposal would not affect the ability of edge providers and countless other players within the Internet ecosystem to deliver such advertising.

### 2. The Commission's Proposed Restrictions on the Use and Disclosure of Aggregate Information Are Inconsistent with Section 222(c) and Would Be Unduly Burdensome

Aggregate information is, by definition, not individually identifiable. It thus falls outside the scope of Section 222(c)(1). In addition, Section 222(c)(3) explicitly *permits* the use and disclosure of aggregate CPNI without subscriber consent. The Commission has long recognized that this exception "affords important commercial benefits for carriers and customer[s] alike, without impacting customer privacy concerns."[115] The NPRM likewise recognizes the commercial benefits of the aggregate CPNI exception.[116] Given the extensive amount of commerce that relies on aggregate data and the lack of associated privacy harms, restrictions on its use – especially restrictions that asymmetrically disadvantage only one class of actors – should be rejected.

Notwithstanding the above, the NPRM proposes to impose its own modified and more restrictive version of the FTC's three-pronged reasonable linkability test on carrier use of aggregate data without a subscriber's consent.[117] Congress did not deem these restrictions necessary when it enacted Section 222, and the NPRM has not provided any reasonable showing why they are needed now.[118] The NPRM does not, for example, specify what "technology

---

[115] *1998 CPNI Order*, 13 FCC Rcd at 8169 ¶ 149.

[116] *See* NPRM ¶ 155 (noting that "aggregate, non-identifiable customer information can be useful to BIAS providers and the companies they do business with, and not pose a risk to the privacy of consumers").

[117] The proposed restrictions are, essentially, the three prongs discussed in Section III.B, plus a requirement that the holder of the aggregated data "exercise[] reasonable monitoring to ensure that [its] contracts [restricting third-party disclosure] are not violated." NPRM ¶ 154.

[118] In fact, the FTC does not impose its own linkability test to aggregated data; that the NPRM now proposes to do so demonstrates the hollowness of the FCC's purported adherence to the principles of the FTC's regime. In reality, the NPRM has applied a distorted and more restrictive version of those requirements.

changes" it is referring to as a reason for this change, or why they pose a meaningful risk that aggregate data could be linked to a customer. Also, the NPRM claims that "[t]here is a rich scientific literature on re-identifying data that has been de-identified," but offers little evidence of this aside from two academic papers discussed briefly in a single footnote of the NPRM.[119] While the Commission's predictive judgments are entitled to deference, such judgments must be based on something more than the mere speculation the Commission has offered here.[120] In any event, the Commission's predictive judgments cannot be entitled to deference, where, as here, they exceed the agency's authority.

In any case, aggregate data does not raise the same privacy concerns as other kinds of data. During the aggregation process, data are stripped of individual customer identities and characteristics. Once aggregated, the data are simply summary statistics and cannot be reverse-engineered to identify the individuals from whom the information was derived. This is precisely why Congress deemed such information disclosable under Section 222(c)(3). In fact, the FTC has recognized that aggregation is an *appropriate method used to de-identify data*, and nothing about the process reveals a subscriber's personally identifiable data to third parties without his or her consent.[121] Application of the multi-pronged de-identification test to aggregate data thus is

---

[119] *Id.* ¶ 157 n.263.

[120] *See Sorenson Communications Inc. v. FCC*, 755 F.3d 702, 708 (D.C. Cir. 2014) (citations omitted) ("Though 'an agency's predictive judgments about the likely economic effects of a rule' are entitled to deference, 'deference to such ... judgment[s] must be based on some logic and evidence, not sheer speculation.' The Commission may hoist the standard of common sense, of course, but the wisdom of agency action is rarely so self-evident that no other explanation is required."); *FiberTower Spectrum Holdings, LLC v. FCC*, 782 F.3d 692, 700 (D.C. Cir. 2015), quoting *Ctr. For Auto Safety v. Fed. Highway Admin.*, 956 F.2d 309, 314 (D.C. Cir. 1992) ("An agency action is arbitrary and capricious if it rests upon a factual premise that is unsupported by substantial evidence.").

[121] *See* FTC Privacy Report at 21 ("Depending on the circumstances, a variety of technical approaches to de-identification may be reasonable, such as deletion or modification of data

regulatory overkill that would impose unnecessary burdens on BIAS providers and undermine the beneficial use of such information to the detriment of competition.

## V. THE PROPOSED TRANSPARENCY OBLIGATIONS WOULD CAUSE "NOTICE FATIGUE" AND CONSUMER CONFUSION, REDUCING CUSTOMERS' AWARENESS OF RELEVANT PRIVACY PRACTICES IN A MANNER THAT ALSO IS UNLAWFUL

T-Mobile believes strongly in providing transparency to all on how it collects, uses, and discloses consumer data. T-Mobile already takes an accessible multi-layered approach to transparency, providing consumers with both easy-to-read privacy policy highlights[122] and more information for those wanting additional details[123] – all absent any prescriptive FCC regulatory edict. We also provide just-in-time notices in many contexts, where appropriate, and further information on our website. Our approach is a response to the competitive market and to consumers' finite time and attention – and there is no evidence that this approach is insufficient, or fails to meet consumer needs and expectations. T-Mobile has learned from experience that today's busy consumers often have limited ability to fully review the hundreds of privacy policies that apply to the apps, websites, and services they use, and prefer simpler notices that provide meaningful information. The proposed notification framework would push these limits.

---

fields, the addition of sufficient 'noise' to data, statistical sampling, *or the use of aggregate or synthetic data*.") (emphasis added) (citation omitted).

[122] T-Mobile, *T-Mobile Privacy Policy Highlights* (Nov. 25, 2015), http://www.t-mobile.com/-company/website/privacypolicy.aspx.

[123] T-Mobile, *T-Mobile Privacy Policy* (Nov. 25, 2015), http://www.t-mobile.com/company-/website/privacypolicy.aspx#fullpolicy (also providing direct links to the Spanish-language version of T-Mobile's privacy policy, and to the aforementioned highlights).

### A. The Proposed Obligations Risk Inundating Consumers and Drowning Out Meaningful Notice

The Commission's proposed obligations risk flooding consumers with multiple uncurated notices – a deluge that would inhibit rather than heighten consumers' ability to focus on actual unwanted or harmful uses of their sensitive data.[124] This problem would become especially acute in light of the additional notices the proposed rule would require providers to send in order to use and disclose even non-sensitive data.[125] The sharp uptick in notifications contemplated by the NPRM would place unwieldy logistical demands on consumers, and in the process risk reducing the attention afforded to *all* privacy-related disclosures, decreasing overall user awareness without providing more meaningful consumer information.

For example, under the NPRM's proposal, a BIAS provider would be required to disclose "[how it] uses, and under what circumstances it discloses, *each type* of CPI that it collects[.]"[126] This mandate is apt to prompt even *longer* privacy policies, including a substantial amount of data that may not convey any useful information about the privacy risks to consumers.[127]

The potential for privacy policy bloat is an especially egregious harm given the costs already imposed by voluminous privacy policies. In 2008, current FTC Chief Technologist Lorrie Cranor estimated that if it took approximately 8-12 minutes for a person with a high

---

[124] The NPRM would also impose unnecessary burdens on providers, including by requiring point-of-sale notices. *See* NPRM ¶ 87.

[125] The NPRM, for example, contemplates an array of possible notifications without delineating sensitive vs. non-sensitive data. *See id.* ¶¶ 83-85. It also seeks comment on updates via email that may in practice need to be frequently sent to customers. *See id.* ¶ 87.

[126] *Id.* ¶ 83 (emphasis added).

[127] In contrast, the FTC has urged *shorter* privacy notices. FTC Privacy Report at 64.

school education to read the average privacy policy on the Internet's most popular sites,[128] the national opportunity costs for "just the time to read policies" alone – setting aside time devoted to considering whether to use the related offerings – was about $781 billion.[129] That cost, of course, can only have grown as consumers conduct more of their activities online, and the Commission's proposal would contribute to this problem.

Relatedly, the NPRM's proposal on advance notice of material changes is a departure from the FTC's approach, which only focuses on material *retroactive* changes.[130] The NPRM proposes to require very detailed advance notice through multiple means of any material changes to a BIAS provider's practices.[131] Although the proposal applies to only those changes that are *material*, the expansive definition of CPI and the extensive notice requirements contemplated by the NPRM in the first instance serve to undermine that limiting standard.

### B. Prescriptive Transparency Obligations Would Prevent Providers from Adapting to Changing Consumer Expectations

Prescriptive transparency obligations, particularly those that do not apply to other entities in the Internet ecosystem, would prevent providers from adapting to changing consumer expectations and privacy policy trends. For example, such requirements could inhibit BIAS providers from adopting any new Internet-wide norms that develop to simplify notice for consumers. Moreover, BIAS provider privacy policies that diverge from policies utilized in the rest of the online ecosystem may actually reduce consumer understanding. This is not only

---

[128] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: J. of L. & Pol. for the Info. Soc., at 10 (2008).

[129] *Id.* at 2.

[130] FTC Privacy Report at 57-58. The FTC specifically chose not to address prospective changes to companies' data collection and use. Rather, it focused on material changes to uses of data that have already been collected. *See id.*

[131] *See* NPRM ¶ 96.

problematic from a public-policy perspective, but also undercuts any suggestion that the Commission could overcome the strict or even intermediate scrutiny that the First Amendment would mandate in response to compelled ISP speech.

Moreover, the NPRM specifically proposes to require BIAS providers disclose how they use and disclose *each* type of CPI they collect in their privacy notice, and to make such notice available at the point of sale and prior to the purchase of BIAS.[132] Instead, the Commission should enable providers to describe their present and future privacy practices to consumers in clear, non-deceptive terms. Providers need flexibility to optimally deliver the information users truly care about, in a form they can focus on and digest. Context-consumable information is especially important in the mobile context, where limited screen space creates customer annoyance if the reader is forced to page through an exhaustive list. Ultimately, the proposed transparency obligations represent a significant step *backwards* in terms of the trend of how companies inform consumers about their privacy practices.[133]

### C. The NPRM's Proposed Notice Requirements Unlawfully Compel Speech

The NPRM proposes prescriptive privacy notice obligations with respect to how BIAS providers use and disclose essentially any of the customer information they hold. This proposal is not only bad policy, but also unlawful. The NPRM suggests that "adequate disclosure of privacy and security practices is necessary to protect the confidentiality of proprietary information of and relating to customers" and that such prescriptive transparency obligations "do

[132] *Id.* ¶ 83. As a preliminary manner, it would be impossible to satisfy this standard because the NPRM has declined to propose a definitive list of what constitutes CPI.

[133] *See, e.g.*, FTC Privacy Report at 64 (finding that privacy notices should be clearer, shorter, and more standardized); *id.* at 62 ("Privacy statements should account for variations in business models across different industry sectors, and prescribing a rigid format for use across all sectors is not appropriate.").

not constitute unconstitutionally compelled speech under the First Amendment."[134] It also asserts that "adequate transparency is necessary to ensure that BIAS providers' practices are just, reasonable, and not unreasonably discriminatory, and that disclosures are in fact a necessary part of providing just and reasonable service[s]."[135] This is mistaken. Indeed, the proposal would have the agency compel precisely what BIAS providers must state about their privacy practices and in precisely what way, in contravention of the First Amendment.[136] Even if transparency with respect to privacy practices constituted a necessary part of providing just and reasonable services, the way in which the Commission seeks to impose such transparency is not. The

[134] NPRM ¶ 301.

[135] *Id.*

[136] The First Amendment generally forbids regulation that compels speech by private parties. *See generally Pacific Gas & Electric v. Public Utilities Comm'n of Cal.*, 475 U.S. 1 (1986); *Wooley v. Maynard*, 430 U.S. 705, 713-17 (1977); *West Virginia Bd. of Educ. v. Barnette*, 319 U.S. 624, 633-34 (1943). The NPRM contemplates content-based speech mandates that are subject to strict scrutiny. *See United States v. Playboy Entm't Group, Inc.*, 529 U.S. 803, 811-12 (2000) (regulation is content-based when it "'focuses *only* on the content of the speech and [on] the direct impact that speech has on its [readers].'") (quoting *Boos v. Barry*, 485 U.S. 312, 321 (1988)). Even if the proposed rules were subject to intermediate scrutiny, though, they would run afoul of the First Amendment, because the Commission cannot "show[] that the restriction directly and materially advances a substantial state interest in a manner no more extensive than necessary to serve that interest." *Ibanez v. Fla. Dep't of Bus. & Prof'l Regulation*, 512 U.S. 136, 412 (1994). Under intermediate scrutiny, "if the Government could achieve its interests in a manner that does not restrict speech, or that restricts less speech, the Government must do so." *Thompson v. Western States Med. Ctr.*, 535 U.S. 357, 371 (2002). Here, the FTC has for many years ensured that Internet users' privacy interests are protected without the prescriptive disclosures contemplated by the NPRM. Thus, even if one believed that the proposed rules would promote consumers' privacy (and, as detailed herein, they would not), it is beyond dispute that the consumer interests at stake could also be protected in a way that did not similarly encumber providers' speech interests. This fact alone renders the proposed transparency requirements unlawful.

proposed transparency obligations would defeat the goal of actually providing transparency to consumers, and thus also are arbitrary and capricious.[137]

## VI. THE COMMISSION SHOULD NOT OVERRIDE CONSUMER CHOICE

The NPRM asks whether to prohibit outright a variety of practices, including deep packet inspection, financial inducements, and persistent identifiers.[138] Although these questions raise difficult legal, technical, and operational issues, these practices are given only brief and simplistic treatment in the NPRM.

Ultimately, these questions boil down to whether the Commission should save consumers from themselves, substituting its judgment for their own and for that of the evolving market. It should not do so. For instance, the Commission should not prohibit providers from offering discounts in exchange for customer consent to certain uses and disclosures of their information. Recent research strongly suggests that customers in many cases voluntarily elect to make such trade-offs, and that they benefit from the ability to do so; these studies also show that such choices are consumer- and context-specific.[139] Furthermore, a decision to prohibit discounted

---

[137] *Office of Commc'n of United Church of Christ v. FCC*, 779 F.2d 702, 707 (D.C. Cir. 1985) (explaining that the arbitrary and capricious test requires a court to scrutinize the rationality of the agency's action, and that "[r]ational decisionmaking ... dictates that the agency cannot employ means that actually undercut its own purported goals") (citing *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 46 (1983); *Office of Commc'n of United Church of Christ v. FCC*, 707 F.2d 1413, 1441-42 (D.C. Cir. 1983). *See also Safari Club Int'l v. Salazar*, 709 F.3d 1, 14 (D.C. Cir. 2013) (adopting a definition of a term and then ignoring that definition and failing to apply it was arbitrary and capricious).

[138] NPRM ¶¶ 24, 256.

[139] *See* Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, at 2, Pew Research Center (Jan. 14, 2016), http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/ (finding that "there are a variety of circumstances under which many Americans would share personal information or permit surveillance in return for getting something of perceived value"); *see also* FTC Privacy Report at 60 (recognizing that whether a particular piece of data is sensitive lies in the "eye of the beholder" and depends upon a number of subjective considerations).

(or free) broadband service plans premised on targeted advertising[140] could suppress emerging business models that are expanding broadband availability for all citizens.[141] Consumers should be free to decide what they care about and what they value, as long as the choices provided to them are made clear and they have other choices in the marketplace, as they certainly do in the context of mobile broadband service.

In any case, to the extent that the Commission wishes to pursue its inquiry into these business practices, it should host issue-specific workshops to develop a better understanding of these practices. If it decides to proceed, it should then issue a further notice of proposed rulemaking setting forth with *specificity* any rules it proposes and the basis on which it believes such rules are justified and legally permissible. Interested parties would then have a meaningful opportunity to participate in these workshops and analyze the proposals to develop a robust record specific to these issues, obviating the need to make predictive judgments about an extremely complicated set of questions within an already-complicated proceeding.[142]

---

[140] Dissenting Statement of Commissioner Michael O'Rielly) ("There is a trade-off – consumers receive 'free' stuff offered by Internet companies while in return the companies receive other things, such as data to place targeted ads, that consumers may or may not want but, at the same time, may be completely comfortable with in the context of the overall package. Heightening the limitations on the use of information, as contemplated by this item, will impact every other pricing component of Internet access and eventually edge providers.").

[141] *See* Doug Brake, Daniel Castro, Alan McQuinn, *Broadband Privacy: The Folly of Sector-Specific Regulation*, at 6, ITIF (Mar. 2016), http://www2.itif.org/2016-broadband-privacy-folly.pdf ("An example to consider is the new LinkNYC service, which is transforming payphone booths into free gigabit Wi-Fi kiosks around New York City. The new service has been heralded as giving free, super-fast Internet access to the public, but looking at the privacy policy and the partner companies, it is clear that this offering is premised on data collection and targeted advertising.") (citations omitted).

[142] *See supra* Section II.

## VII. THE DATA SECURITY AND DATA BREACH NOTIFICATION OBLIGATIONS, AS PROPOSED, WOULD CAUSE UNINTENDED AND POTENTIALLY HARMFUL CONSEQUENCES

The NPRM asserts that "Section 222 leaves no doubt that every telecommunications carrier has a duty to protect its customers' proprietary information."[143] It observes that the Commission has referred to Section 222(a) as imposing security obligations on telecommunications carriers and has implemented security and breach obligations on CPNI under Section 222(c).[144] The NPRM concludes that "the same authority justifies the revised breach notification requirements … that carriers notify customers, law enforcement, and the Commission of breaches of customer PI that is not CPNI."[145] T-Mobile agrees that Section 222 "leaves no doubt" about the existence of a duty to protect, but Section 222 also "leaves no doubt" that this duty is limited to CPNI.[146] Thus, while T-Mobile appreciates that data security is critical, the Commission cannot lawfully apply any data security and breach notification obligations to practices and breaches involving any information beyond CPNI.[147]

Moreover, as described below, the specific data security and breach notification proposed by the Commission are unnecessary, create operational and practical problems, and would not serve consumers. They thus are arbitrary and capricious.[148]

---

[143] NPRM ¶ 303.

[144] *Id.*

[145] *Id.*

[146] *See supra* Section III.A.

[147] Because, as described above, Section 222(a) does not provide the Commission with standalone authority, it cannot be the basis for FCC rules. Thus, as noted above, the Commission must limit any privacy regulations to CPNI, and any rules must implement, at most, the "[p]rivacy requirements for telecommunications carriers" set forth in Section 222(c)(1).

[148] *Northwest Envtl. Advocates v. Nat'l Marine Fisheries Serv.*, 460 F.3d 1125, 1150 (9th Cir. Wash. 2006) ("While we certainly must respect the agency's technical decisions, where those

### A. The Commission Must Afford BIAS Providers Flexibility in How They Secure Customer Information

T-Mobile agrees that providers should establish, implement, and maintain reasonable data security programs. These should include reasonable physical, technical, and administrative security safeguards to protect customer information from unauthorized access, use, and disclosure. Prescriptive data security rules, however, will have unintended consequences because they cannot be adapted to the different network architectures implemented by each BIAS provider, fail to consider the dynamic nature of future networks as enabled by Network Function Virtualization (NFV) or Software Defined Networks (SDN), and necessarily cannot anticipate the changing threat environment.

Providers must have the flexibility to allocate resources in accordance with the assessed risk to the provider and its customers, particularly as technology and the threat environments evolve. Importantly, providers need to focus on how best to use resources to reduce the likelihood of harm to their customers and any FCC rules similarly should be based on the potential for mitigating actual consumer harm.

Although the discussion in the NPRM appears to contemplate a reasonableness standard[149] similar to the approach the FTC has taken,[150] the actual proposed rule, as drafted,

---

decisions enable the agency to ignore reality, we need not acquiesce."); *Alliance for Cannabis Therapeutics v. Drug Enforcement Admin.*, 930 F.2d 936, 940 (D.C. Cir. 1991) ("Impossible requirements imposed by an agency are perforce unreasonable.").

[149] *See, e.g.*, NPRM ¶¶ 217, 219.

[150] *See* FTC Privacy Report at 21 n.108 ("The Commission's approach in data security cases is a flexible one. Where a company has offered assurances to consumers that it has implemented reasonable security measures, the Commission assesses the reasonableness based, among other things, on the sensitivity of the information collected, the measures the company has implemented to protect such information, and whether the company has taken action to address and prevent well-known and easily addressable security vulnerabilities.").

seems to take a strict liability approach.[151] That approach is entirely unreasonable given the complexities and challenges of data security. It may, for example, cause BIAS providers to take extremely costly measures to secure customer information that are not cost-effective or helpful to consumers – including, for example, information that already is publicly available. These additional costs, which will generate no corresponding benefit, will of course ultimately be borne by consumers. While a "bear any burden" approach to data security might sound appealing in theory, the law routinely and pervasively recognizes that it is far better to apply a "reasonableness" standard that balances benefits and costs than to adopt mandates with no limiting principles, particularly given rapidly changing technology. Likewise here, consistent with the FTC's approach to data security, the FCC should adopt a reasonableness standard, rather than taking a strict liability approach.

Even under a data security standard properly calibrated to reasonableness, the Commission should not set prescriptive requirements and minimum standards, as the NPRM has proposed. The practices the NPRM proposes to mandate are practices that BIAS providers can and should consider adopting *voluntarily*.[152] But providers must be permitted and encouraged to engage in risk-based analysis, and to adjust protections in light of the nature and scope of their activities, the sensitivity of the data, and the size and complexity of their relevant data operations. Inevitably, minimum standards and prescriptive data security rules will inhibit providers from focusing resources on measures they deem best to protect consumers in any given circumstance, *i.e.*, reasonable measures under the circumstances. They will also prevent ISPs from adapting their practices as technical and marketplace realities evolve.

---

[151] *See* Proposed Rule 47 C.F.R. § 64.7005(a) ("A BIAS provider *must ensure* the security, confidentiality, and integrity of all customer PI….") (emphasis added).

[152] *See* NPRM ¶ 174.

Indeed, although the NPRM suggests that the proposed minimum standards are "flexible"[153] the NPRM proposes, or at least seeks comment on, various *specific* administrative, technical, and physical requirements. For example, the NPRM's discussion of authentication requirements asks whether the Commission should require multi-factor authentication, mandate password protection, and adopt specific authentication procedures for particular scenarios.[154] This type of prescriptive requirement fails to consider the cost to the BIAS provider of implementing and operating such a system for authentication. It also does not consider the impact to the consumers who would need to understand the proper use and protection of secondary tokens or biometric data. In addition, distribution of tokens, protection of biometrics, and the additional protection of these types of secondary authentication mechanisms will create additional complexity for both the BIAS provider and the consumer. The fact that the NPRM even asks a series of questions about how providers would meet its minimum standards demonstrates the significant challenges to implementation.[155]

Moreover, the proposed data security requirements are unnecessary. BIAS providers have strong incentives to keep their customers' information, and particularly their customers' sensitive information, secure. The NPRM does not – and could not – dispute such incentives, and accordingly fails to provide any reason why the marketplace is not currently working to

[153] *Id.* ¶ 175.

[154] *See id.* ¶¶ 194, 196, 198.

[155] The proposed data security requirements are especially problematic and prescriptive given the broad definition of CPI to which the rules apply.

ensure reasonable data security. Nor does (or can) the Commission explain why the FTC's approach to data security has been insufficient to protect consumers.[156]

### B. The Proposed Data Breach Notification Obligation Will Result in Over-Notification and Consumer Confusion

The proposed data breach notification obligation, which would apply to both BIAS providers and providers of other telecommunications services,[157] also would have unintended consequences. Most notably, it would result in over-notifying consumers who will not be able to determine which, if any, of the breaches pose actual risk to them and their information.[158] Further, if consumers receive numerous breach notices from their providers of BIAS and telecommunications services – and many more than they receive from providers of other online services subject not to FCC rules, but to state data breach notification standards[159] – they will develop the mistaken impression that BIAS and telecommunications service providers do not adequately protect and secure their information. As a result, the Commission's obligation may actually undermine BIAS use, rather than promote adoption and deployment.

#### 1. The Commission Must Apply Reasonable Limits to Any Breach Notification Obligations

Even with impeccable data security safeguards and efforts, incidents involving unauthorized access to data will occur. Many incidents do not pose any risk to consumers and

---

[156] Again, it is telling that the FTC, which has brought numerous data security cases, never brought a data security case against a BIAS provider when it viewed such providers as being subject to its authority.

[157] *See* NPRM ¶ 233.

[158] The NPRM correctly notes the real risk of over-notification. *See, e.g., id.* ¶ 23.

[159] Notably, BIAS providers are subject to these state requirements – even without any new requirements from the FCC, BIAS providers will be required to notify their customers of data breaches under state law. Thus, it's not clear how layering an additional FCC data breach notification requirement actually helps to protect consumers.

may not even involve a bad actor obtaining access to customer information, let alone sensitive customer information. Any breach notification requirement must account for when consumers actually are put at risk and when they were not. The FCC's proposal, however, fails to do so. It is overbroad with respect to what would be considered a breach (*i.e.*, "*any* instance in which a 'person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information'"),[160] particularly given the broad scope of the NPRM. The Commission should not underestimate how many notices BIAS providers might be required to send to consumers and the Commission under an ill-advised rule. And almost all of these notices may disclose incidents that never even posed the potential of harm to consumers.[161]

To mitigate these risks, to the extent that there is any justification for FCC-specific data breach notification obligations instead of relying on state law, the Commission should limit any notification requirement in several ways. First, it should limit the definition of breaches to cases in which a person *intentionally* and without authorization accesses, uses, or discloses customer information.[162] Inadvertent employee mistakes, for example, simply do not pose a risk to consumers and therefore should not be considered a reportable security breach.[163] Second, the Commission must include a trigger for breach notification that is based on a likelihood of harm to ensure that consumers are alerted to breaches only when there is some risk to them.[164] A harm

---

[160] NPRM ¶ 75 (emphasis added) (citation omitted).

[161] For example, a provider should not be required to report a breach if an employee inadvertently accesses non-sensitive data about the wrong customer, such as a name or number.

[162] Of course, for the reasons described above, the Commission cannot and should not reach the broad scope of information it seeks to in the NPRM, including with respect to any data breach notification obligation.

[163] *See* NPRM ¶ 76.

[164] *See id.* ¶ 237.

trigger should focus, for example, on the sensitivity of any breached information, as it makes no sense to require notification where a breach was limited to non-sensitive information that may already be publicly available, such as a consumer's name.[165] Notifications involving breaches that pose no harm – which cannot offer the consumer any meaningful steps to take in response – serve only to confuse customers and corrode faith in providers' practices based on misconceptions as to the consequences of a purported "breach."

Separately, the Commission must ensure that providers actually can comply with any breach notification obligation it ultimately adopts. The NPRM's proposal fails in this regard. As currently contemplated, the rules at times would require notifications that are not currently deliverable.[166] Any rules must be flexible to accommodate a variety of business practices and offerings, so that ISPs are not compelled to collect and store *more* information from customers without a corresponding benefit.

Regardless of what standard the Commission may ultimately adopt, it must establish additional reasonable exceptions to notification obligations. As discussed above, in no event should reportable breaches include good-faith acquisitions or disclosures of information where such information is not used improperly or further disclosed.[167]

---

[165] The Commission should allow providers to make a good faith determination about whether any given breach presents a likelihood of harm to consumers.

[166] For example, providers often have limited (if any) personal information about prepaid customers, and may in fact lack sufficiently accurate contact information to notify them in the event of a breach in the manner the NPRM proposes. In particular, the NPRM proposes a detailed set of information to be included in every such notice. *See* NPRM ¶ 243. Thus, to the extent that prepaid consumers could be contacted by voicemail or SMS messaging only, it may not be practical to offer such details through this method. In this context, providers generally also lack any sensitive information whatsoever about such prepaid customers.

[167] *See, e.g., id.* ¶ 76 (noting that some state statutes exempt from the definition of breach the good-faith acquisition of covered data by an employee or agent of the company where such

### 2. The Commission Must Afford Providers More Time to Report Breaches

The Commission also must provide a longer timeline to report a breach that meets whatever reporting threshold the Commission adopts.[168] An overly aggressive reporting timeline would result in breach notifications that are inaccurate, incomplete, and potentially unnecessary. It also risks the company's ability to respond to consumer and security needs in the wake of a breach.

Breach responses and investigations take time and tremendous resources. There can be little disagreement that a first priority after discovery of any given breach is to investigate, identify, and remedy any vulnerabilities. Then, the company will continue to investigate the extent of the breach, also ensuring that there are no further vulnerabilities. The company subsequently must validate the identity of all individuals who were exposed by the data breach – which may be especially difficult if the data breached does not directly identify specific consumers but may be considered "linkable" under the Commission's rules[169] – and it must confirm all contact information for affected individuals. As this investigative and fact-gathering process unfolds, the company learns new information each day, and initial assessments regarding the scope of the breach and the number of consumers affected may prove inaccurate or incomplete as time goes on.

---

information is not used improperly or further disclosed and asking whether the FCC should do the same or whether doing so is "unnecessary or otherwise unadvisable").

[168] The NPRM proposes (i) mandatory notification to the FBI and Commission within seven days, and at least three days before notifying consumers; and (ii) mandatory notification to consumers within 10 days. *Id.* ¶ 234. Meanwhile, the shortest timeline in a state breach notification statute requires notification within 30 days. Fla. Stat. § 501.171.

[169] *See supra* Section III.D.

Moreover, breach response itself consumes substantial company resources, well beyond those required to notify consumers consistent with any state and federal regulatory requirements. For example, a breached company must activate and prepare enough customer service representatives to communicate with and address the concerns of potentially affected consumers. The breached company may also contract for, and procure, identity theft protection services for its affected customers. An aggressive notification timeline, like the one proposed in the NPRM, could potentially leave providers with an impossible choice – either ignore what consumers may need post-breach or divert resources to such efforts rather than to the investigation of the breach.[170] Taken in conjunction with the overbroad scope of data incidents to which the rules would apply, this would consume significant unnecessary customer time and resources and pose a substantial burden on providers, without advancing consumer interests.

Even without an aggressive regulatory requirement, companies strive to report breaches to customers as soon as possible to maintain a trusted relationship with, as well as protect, their customers. Companies also have a further incentive to report a breach as soon as possible before the press reports on the breach to avoid embarrassment and mitigate any public and consumer confusion. Flexibility, however, is important to ensure that any information provided to consumers is as accurate as possible. Otherwise, breach notifications may provide consumers with a false impression of the nature and scope of any given breach, whether the notification turns out to be an overstatement or understatement of the risk to consumers. This will be further exacerbated if follow-up notifications are needed to correct inaccuracies.

[170] As a practical manner, many of the same people within a company involved in investigating a breach, including technical, legal, and business teams, also are involved in managing the company's response to said breach, including ensuring that customers have resources available to them to understand the breach, any risk to them, and what steps they can take to mitigate any such risk.

## VIII. THE FCC HAS NO LEGAL BASIS FOR ADDRESSING ARBITRATION AND ALTERNATIVE DISPUTE MECHANISMS

The NPRM seeks comment on arbitration and alternative dispute resolution, including whether the Commission should "prohibit BIAS providers from compelling arbitration in their contracts with customers."[171] The Commission, however, has no legal authority to do so. Federal law establishes a strong presumption in favor of arbitration clauses, which are valid and enforceable under the Federal Arbitration Act ("FAA")[172] barring explicit "contrary congressional command" in a separate federal statute.[173] Congressional intent must be "discernible from the text, history, or purposes of the statute" to override the FAA.[174] When a federal statute "is silent on whether claims under the Act can proceed in an arbitrable forum, the FAA requires the arbitration agreement to be enforced."[175]

The Communications Act does not override the FAA. The Communications Act makes no reference to arbitration provisions in agreements for telecommunications services. Under the Supreme Court's recent *CompuCredit* jurisprudence, this silence ends all inquiry into the Commission's (lack of) authority.[176] Further, the Communications Act's legislative history offers no grounds for outlawing arbitration, and there is no basis to argue that arbitration is in "inherent conflict"[177] with the Act's "underlying purpose."[178]

---

[171] NPRM ¶¶ 273-275.

[172] 9 U.S.C. § 2 (arbitration provisions are "valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract").

[173] *Moses H. Cone Mem'l Hosp. v. Mercury Constr. Corp.*, 460 U.S. 1, 31 (1983).

[174] *Shearson/Am. Express, Inc. v. McMahon*, 482 U.S. 220, 227 (1987).

[175] *CompuCredit Corp. v. Greenwood*, 132 S. Ct. 665, 673 (2012).

[176] *Id.*

[177] *McMahon*, 482 U.S. at 227.

## IX. OTHER ASPECTS OF THE PROPOSAL WOULD CAUSE SUBSTANTIAL IMPLEMENTATION CHALLENGES

Many other aspects of the NPRM also would create substantial implementation challenges, and thus too would be arbitrary and capricious. For example, the proposal asks whether to require BIAS providers to "provide their customers with access to *all* customer information in their possession, including *all* CPNI, and a right to correct that data."[179] Regardless of whether it is even technically possible to provide such access to "*all* customer information," including "*all* CPNI," it is not valuable to a consumer to have access and the ability to correct the vast majority of this information. Moreover, the NPRM's proposed application of the framework to *former* customers, as well as *applicants* for service, poses additional challenges. In fact, to comply with such requirement, a BIAS provider may need to maintain enough information regarding a former customer to provide such former customer with access rights. This would seem inconsistent with the principle of (and any requirement regarding) data minimization and could further burden providers' efforts to secure the data they hold. This concept, along with many other proposals in the NPRM, would fail to serve consumers, but would do so at a high cost and burden to BIAS providers.[180]

---

[178] The Commission would not receive deference if it attempts to regulate arbitration, and the agency's actions consequently would be invalidated. Interpretation of the FAA is outside of the Commission's purview, and courts have wisely refrained from granting deference to agencies addressing questions controlled by statutes the agency in question does not administer. *See, e.g.*, *Metro. Stevedore Co. v. Rambo*, 521 U.S. 121, 137 n.9 (1997).

[179] NPRM ¶ 205 (emphasis added).

[180] T-Mobile offers this example as just one of many of the other challenges posed by the NPRM's broad application to virtually all customer data combined with the proposed prescriptive requirements. T-Mobile expects that the record will contain additional examples beyond those discussed in these comments.

## X. CONCLUSION

As described herein, the NPRM proposes complicated and burdensome rules that exceed the Commission's legal authority, rely on a misunderstanding of the Internet ecosystem, and would confuse and harm consumers rather than protect their privacy. T-Mobile therefore urges the Commission to reconsider its proposal in its entirety in a manner consistent with these comments.

Respectfully submitted,

*/s/*

Cathleen Massey
Luisa Lancetti
Michelle Rosenthal
**T-Mobile USA, Inc.**
601 Pennsylvania Avenue, NW
Washington, DC 20004
(202) 654-5900

May 27, 2016