Before the
Federal Communications Commission
Washington, D.C. 20554

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

PETITION FOR RECONSIDERATION BY THE UNITED STATES TELECOM ASSOCIATION

Pursuant to 47 C.F.R. § 1.429, the United States Telecom Association ("USTelecom") respectfully petitions for reconsideration of the Commission's *Order* in this proceeding, adopted by a sharply divided 3-2 vote.[1] As discussed below, the Commission should modify key elements of the *Order* and its accompanying regulations to reflect cost-benefit considerations and avoid irrational conflict with the well-established privacy and data security framework applicable elsewhere in the Internet ecosystem.

INTRODUCTION AND SUMMARY

So long as this Commission classifies broadband Internet access as a "common carrier service," it should ensure technological neutrality and avoid consumer confusion by harmonizing its privacy regime with that of the Federal Trade Commission (FTC), under which most participants in the Internet ecosystem operate. The *Order* pays lip service to that objective but falls short, and this Commission should now grant reconsideration to align the two regimes. USTelecom is not challenging those elements of the *Order* that are consistent with the FTC's privacy regime, such as the Commission's decision to streamline outdated provisions of its legacy privacy rules.

[1] Report & Order, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Dkt. No. 16-106, FCC No. 16-148 (Nov. 2, 2016) (*"Order"*). The *Order* was published in the Federal Register on December 2, 2016. 81 Fed. Reg. 87,274.

The *Order* is arbitrary and capricious in a number of respects, but two basic errors stand out. First, on several critical issues, the *Order* dispenses with any cost-benefit analysis: it treats even the most ephemeral privacy interest as though it had infinite weight and simply disregards the economic costs of foreclosing productive uses of information. For example, the *Order* subjects ISPs to a burdensome opt-in regime for marketing uses of *all* web-browsing information on the theory that all such information is equally "sensitive." In contrast, under the FTC's regime, all other Internet companies enjoy much greater flexibility in their use of web-browsing data except where the underlying subject matter itself is sensitive, such as information that reveals medical conditions or personal finance. In rejecting that contextual approach, the *Order* ignores the substantial economic costs of overbroad opt-in requirements as well as the detailed economic analysis that USTelecom submitted on that very subject by former FTC Commissioner (and now Professor) Joshua Wright.[2] As Professor Wright explains, those regulatory costs will exert upward pressure on consumer broadband prices if the *Order* is permitted to take effect.

Second, the *Order* ignores the record facts when it predicates this scheme of asymmetric regulation on the premise that ISPs are nearly omniscient and have greater visibility into consumer data than any other Internet company. That premise is false, as Commissioners Pai and O'Rielly and many commenters have explained. Given the recent rise of encryption and multiple ISP connections per user, any given ISP has rapidly declining visibility into the details of consumers' Internet usage and, in some respects, less visibility than leading social media platforms, search engines, and data brokers. All Internet companies "see" the same types of customer data from different angles, and each has different advantages and limitations in making

[2] Joshua D. Wright, *An Economic Analysis of the FCC's Proposed Regulation of Broadband Privacy* (May 27, 2016) ("*Wright Economic Analysis*") (filed in WC Docket No. 16-106 by the United States Telecom Association on May 27, 2016).

use of the data. The *Order* identifies no sound basis, and there is none, for treating ISPs differently from other major Internet actors or for hamstringing them from putting non-sensitive consumer data to productive use.

These two overarching errors led the Commission to adopt a number of ill-considered rules that it should now reverse. It should align its notice-and-choice rules—including those that apply to consumer data related to voice service—with the FTC's regime. Such rules should distinguish between sensitive and non-sensitive web-browsing and app-usage data, should confine opt-in consent requirements to uses of genuinely sensitive data, should avoid placing unnecessary burdens on incentive-based offers, and should impose no notice-and-consent requirements for any first-party marketing where the relationship is clear. In addition, the Commission should eliminate notice-and-choice obstacles to the mere use of any customer data for internal analytics and service improvements.

To avoid costly administrative burdens, the Commission should also conform its definition of "data breach" to the definitions found in state laws and the FCC's own consent orders, which confine that term to unauthorized disclosure of sensitive information or data that, in combination, would facilitate unauthorized access to an online account. The Commission should further confine any category of "personally identifiable data" to data that is reasonably linkable to actual *persons* and exclude data that is linkable only to devices but not persons. And the Commission should extend the business customer exemption to broadband Internet access services when purchased by businesses such as participants in the E-Rate program.

Although this petition focuses on the factual and policy-oriented shortcomings of the *Order*, USTelecom preserves all legal arguments that it and others have made. These include the arguments (1) that the Commission's reclassification of broadband Internet access services under

Title II was unlawful and that Section 222 is thus irrelevant to those services; (2) that the Commission lacks authority over many ISP privacy and data security practices even if broadband Internet access remains subject to Title II; and (3) that various aspects of the *Order* violate the Communications Act, the Administrative Procedure Act, and the First Amendment.

ARGUMENT

I. THE COMMISSION SHOULD ALIGN ITS NOTICE-AND-CHOICE RULES WITH THE FTC REGIME APPLICABLE ELSEWHERE IN THE INTERNET ECOSYSTEM.

A. The Commission Should Eliminate Its Categorical Opt-In Regime for All Web-Browsing and App Usage Data and Adopt the FTC's More Context-Sensitive Approach.

Consumer information is the fuel of the commercial Internet. Companies like Google, Facebook, and Twitter add incalculable value to the world economy by subsidizing affordable consumer services with the profits earned from productive uses of consumer information. ISPs are no different from any other Internet company in that regard. As Professor Wright explains, the greater the revenues ISPs can earn from the use of consumer data, the lower the subscription fees they will charge in this two-sided market, all else held equal. *Wright Economic Analysis* at 20-22. Thus, "[t]he most tangible cost to consumers" from excessive ISP privacy regulation consists of "higher retail prices for broadband access, as compared to those that would prevail absent such regulation." *Id.* at 21.

Sensitive to these concerns, the federal government, led by the FTC, has always addressed online privacy by carefully balancing the costs of undue regulation against the need to protect consumers from genuine privacy harms. The FTC's regime is as flexible as it is effective, relying largely on industry self-governance backed up by the FTC's own enforcement of statutory prohibitions against unfair or deceptive trade practices. *See* 15 U.S.C. § 45(b) & (n). In the words of a 2012 White House report, that regime relies on "multi-stakeholder processes to

produce enforceable codes of conduct" that market participants can voluntarily incorporate into their privacy policies and thereby make subject to FTC enforcement.[3] As the White House added, "multi-stakeholder processes … can provide the flexibility, speed, and decentralization necessary to address Internet policy challenges" and are thus preferable to "rel[iance] on a single, centralized authority."[4]

The rules adopted here break sharply from that tradition in several key respects. The *Order* recognizes that notice-and-choice rules should vary with the sensitivity of the data involved, as the FTC has long explained. But the *Order* jumps the rails when it concludes that *all* web-browsing and *all* app-usage data are categorically "sensitive" and thus subject to opt-in requirements. *See Order* ¶¶ 181-190. Under that approach, an ISP faces unique regulatory burdens if, for example, it implements an algorithm to serve sports-related advertisements to customers who visit sports websites, even if it shares no customer-specific information with the third-party advertisers.

No U.S. regulatory authority has ever adopted this extreme approach, and for good reason. As Google explains, "consumers benefit" from the wide use of non-sensitive web-browsing information to provide "responsible online advertising, individualized content, and product improvements based on browsing information," and thus "[c]alls by some parties in this proceeding to extend an opt-in consent requirement to all web browsing information are unjustified. The FTC's framework recognizes that while U.S. consumers consider healthcare or financial transactions, for example, to be sensitive information that should receive special

[3] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 24 (Feb. 2012) ("*White House Privacy Framework*"); *see* Verizon Comments 16.

[4] *White House Privacy Framework* at 23-24.

protection, they do not have the same expectations when they shop or get a weather forecast online."[5] Google adds: "[t]he FCC's framework should allow such differentiation based on the nature of web browsing information, regardless of the company collecting the data."[6]

The Commission should now align its rules with the consensus FTC framework and specify that web-browsing and app-usage information is "sensitive" only if the underlying subject matter is sensitive. The *Order* cites several rationales for rejecting that approach, but none is persuasive.

First, the *Order* suggests that an opt-in regime will impose minimal costs because ISPs will be "incentivized to provide and improve access to their notice and choice mechanisms" and can easily persuade consumers to opt in to unobjectionable uses of their data. *Order* ¶ 194. This notion—that opt-in is simply a more consumer-friendly version of opt-out—contradicts established academic research, which the *Order* ignores. Most consumers are happy to share information with online service providers in exchange for free or discounted services.[7] But in the absence of financial inducements, most consumers take the path of least resistance and click "no" when presented with opt-in notices. As Professor Wright explains, most do so *not* because they object to the use of their information, but because they (1) simply do not wish to take the time to read and digest a privacy notice and (2) do not internalize the social costs of that non-choice for the Internet ecosystem, which relies heavily on the free flow of consumer information

[5] Letter from Austin Schlick (Google) to Marlene Dortch (FCC), WC Docket No. 16-106, at 1 (Oct. 3, 2016).

[6] *Id.*

[7] "Indeed, one study found that, on average, Americans assigned a value of almost $1,200 per year to the package of free, ad-supported services and content currently available to them[.]" *Wright Economic Analysis* at 15-16 (internal quotation marks omitted). In addition, "[m]ore than 85 percent of respondents said they preferred [that] ad-supported Internet model instead of paying for online content." Digital Advertising Alliance, *Zogby Poll: Americans Say Free, Ad-Supported Online Services Worth $1,200/Year; 85% Prefer Ad-Supported Internet to Paid* (May 11, 2016), http://digitaladvertisingalliance.org/press-release/zogby-poll. The "[s]urveys" on which the *Order* relies (*e.g.*, ¶¶ 87, 194) ignore these revealed consumer preferences and, in any event, do not distinguish between ISP and non-ISP actors.

to subsidize low-cost or no-cost services. *Wright Economic Analysis* at 16-19. In contrast, an opt-*out* regime does not produce similar inefficiencies because the small minority of consumers who do "care greatly about" uses of their non-sensitive data will "invest the time to read, understand, and make an informed decision regarding the privacy policies with which they are presented." *Id.* at 17.

Indeed, if the *Order's* opt-in regime were broadly applied, it would stop the modern digital economy in its tracks and transform many "free" Internet services into smaller, subscription-based enterprises. "Any *individual* consumer confronted with an opt-in choice could skip reading the applicable privacy policy and decline by default, expecting that he or she could free-ride on the service provider's use of *other* customers' information to subsidize low-cost services. The problem is that most of those other customers would have that same preference, click 'no,' and jam the engine powering today's Internet."[8] As Professor Wright adds, the victims of such overbroad opt-in requirements are ordinary consumers, who must pay "higher retail prices for broadband access" than they would pay if, like countless others in the Internet ecosystem, ISPs could defray the costs of retail services with advertising revenues earned on the other side of this two-sided market.[9] The *Order* nowhere addresses these concerns; indeed, it does not once cite Professor Wright's extensive analysis even though it is directly on point.

Second, the *Order* argues that a categorical opt-in rule for all web-browsing data is necessary because distinguishing between "sensitive and non-sensitive categories [of data] is a fundamentally fraught exercise." *Order* ¶ 187. But the rest of the Internet ecosystem conducts

[8] AT&T Reply Comments 19; *see Wright Economic Analysis* at 19 (discussing this "important externality at play in the user decision to share information").

[9] *Wright Economic Analysis* at 21; *see also* Cincinnati Bell Comments 12.

that "exercise" countless times each minute, as the *Order* appears to acknowledge. *Id.* ¶ 188. And the exercise is hardly "fraught." When ad networks and other online providers serve advertisements on the basis of browsing history, their algorithms simply avoid placing ads that target sensitive subject matter. For example, Google explains that, "[w]hen showing you personalized ads, we will not associate an identifier from cookies or similar technologies with sensitive categories, such as those based on race, religion, sexual orientation, or health."[10] In deciding which categories should remain off-limits, online providers typically rely on guidelines issued by industry self-regulatory organizations such as the Network Advertising Initiative. ISPs are just as capable as any other company of following the guidance of these organizations.[11]

The *Order* notes that there are several such organizations and that they sometimes draw different lines between sensitive and non-sensitive data elements. *Order* ¶ 188. But that fact is unremarkable and, indeed, desirable: it reflects an ongoing and highly visible search for consensus among the very types of multi-stakeholder organizations whose role the White House has lauded.[12] Occasional line-drawing debates are not an excuse to abandon line-drawing altogether and over-classify all web-browsing data as "sensitive" by default. In concluding otherwise, the Commission majority abdicated its obligation to conduct a cost-benefit analysis, effectively assigning dispositive weight to any privacy interest, no matter how negligible, and no weight at all to the substantial costs of an overbroad opt-in regime.

[10] Google, *About Google Ads*, https://support.google.com/adsense/troubleshooter/1631343 (last visited Dec. 21, 2016); *see also* Letter from James J.R. Talbot (AT&T) to Marlene Dortch (FCC), WC Docket No. 16-106, at 3 (Oct. 17, 2016) ("This process involves correlating non-content web address or app information (e.g., visit to a sports website) with a pre-established "white list" of permissible interest categories (e.g., sports lover) available from the IAB. The list of interest categories can be refined as needed to exclude any sensitive categories.").

[11] *See*, *e.g.*, Digital Advertising Alliance Comments 4; Future of Privacy Forum Reply Comments 4.

[12] *See White House Privacy Framework* at 23-24.

Moreover, the *Order*'s characterization of all web-browsing data as "sensitive" ignores not only the FTC's longstanding regime, but also the FTC's specific recommendations to the Commission. In its comments, the FTC supported a more targeted opt-in approach focused on genuinely sensitive information, consisting of "(1) content of communications and (2) Social Security numbers or health, financial, children's, or precise geolocation data." FTC Staff Comments 20. Carefully developed over many years, that approach "reflect[s] the different expectations and concerns that consumers have for sensitive and non-sensitive data." *Id.* 22. In contrast, more expansive opt-in requirements, such as those adopted in the *Order*, "could hamper beneficial uses of data that consumers may prefer[.]" *Id.*

Third, the *Order* claims that ISPs should be subject to uniquely onerous privacy regulation on the theory that, compared to all other Internet companies, ISPs have more comprehensive visibility into consumers' online conduct. *See Order* ¶¶ 185-186. That claim, too, is empirically false, as numerous commenters have explained, including some who support strict privacy regulation.[13] The *Order* brushes off the major and growing limitations on each ISP's visibility into consumer data, such as encryption of most web traffic and the tendency of consumers to switch continuously among different ISPs as they carry their devices from one network to the next.[14] Then, in claiming that *non*-ISP actors have much less visibility than ISPs,

[13] *See, e.g.*, EPIC Comments 16 ("The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem. Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. … Privacy rules for ISPs are important and necessary, but it is obvious that the more substantial privacy threats for consumers are not the ISPs."); Security and Software Engineering Research Center (S^2ERC) at Georgetown University Comments 3-4 ("At times, edge providers may have a broader and more detailed understanding of consumer information as few consumers rely on only a single [ISP]. Edge providers can collect information across all networks a customer uses.").

[14] *Compare Order* ¶¶ 29, 186 *with* Peter Swire et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* (Ga. Tech. Inst. for Info. Sec. & Privacy, May 2016); CenturyLink Comments 5-12; Verizon Comments 17-24; AT&T Comments 13-30; CTIA Comments 114; T-Mobile Comments 5-7; Comcast Comments 26-29. The Commission claims that even when web traffic is encrypted, an ISP can "infer" consumer information from unencrypted data such as top-level URLs and amount of data usage. *Order* ¶ 33.

the *Order* focuses myopically on what *individual websites* can see in isolation and nearly ignores what is seen, collected, and used by ad networks, app developers, browsers, mobile operating systems, and social media sites. *E.g.*, *Order* ¶ 185. As the FTC has explained, however, "operating systems and browsers may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles" of individual consumers.[15]

In short, as Commissioner Pai observes, the *Order* reflects "not data-driven decision-making, but corporate favoritism":

> [The] *Order* tries to justify [regulatory asymmetry] by arguing that ISPs and edge providers see vastly different amounts of your online data. It recounts what it says is a vast sea of data that ISPs obtain. It then says that "By contrast, edge providers only see a slice of any given consumers Internet traffic." A "slice." Really? ... The volume and extent of personal data that edge providers collect on a daily basis is staggering.

Pai Dissent 210. Commissioner O'Rielly adds: "The fact that consumers use multiple platforms to access the Internet, coupled with the increasing prevalence of encryption, significantly undermines the order's claims that broadband providers have unique or unparalleled access to customers and their information." O'Rielly Dissent 214-215.

For the same reasons, the *Order* falls flat when it bases ISP-only restrictions on a false analogy between web-browsing history and traditional "call detail information" on the legacy telephone network. *Order* ¶ 181. All commercial entities with access to call-detail data were generally telecommunications carriers subject to Section 222, and there were no unregulated companies collecting the same information for marketing purposes. Consumer expectations

---

Such information is generally not very sensitive and pales in comparison to the detailed information collected by edge providers on each end of these communications. *See* Future of Privacy Forum Comments 9-19; AT&T Reply Comments 16-25; CTIA Comments 113-14; Comcast Comments 29-34; T-Mobile Comments 6.

[15] *See* FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, at 56 (Mar. 2012) ("*2012 FTC Privacy Report*").

about the data uses on that closed network thus have no bearing on their quite different expectations about the use of data on the open Internet, where unregulated online companies routinely make extensive use of the very same data that the *Order* hamstrings ISPs—and them alone—from using.[16]

Fourth, the *Order* implies (at ¶ 36) that ISPs face less retail competition than other leading Internet companies and are thus less subject to competitive checks on their data practices. That suggestion, too, is meritless. Although the *Order* asserts without support that some fixed-broadband customers "do not have the benefit of robust competition" (*id.*), the record contains unrebutted evidence that many broadband markets are indeed highly competitive.[17] In any event, competition cannot justify the radical regulatory asymmetry imposed by this *Order* because broadband markets in general are certainly no more concentrated than various other parts of the Internet ecosystem, which are subject to the FTC's more flexible privacy regime. The *Order* does not contend otherwise. There is likewise no basis for the *Order*'s unexplained suggestion (at ¶ 36) that ISPs benefit from unique "switching costs" greater than those applicable to these other Internet actors. To the contrary, Internet companies with the greatest visibility into consumer data may benefit from equal or greater switching costs.[18]

---

[16] *See* AT&T Comments 2-3, 9-10; USTelecom Comments 3-6; CTIA Comments 110-111; *see also* O'Rielly Dissent 213.

[17] *See* Verizon Comments 22-23, 28; AT&T Comments 46-49 & n.101; CTIA Comments 114-115. Although the *Order* states that "51 percent of Americans still have only one option for a provider of fixed broadband at speeds of 25 Mbps download/3 Mbps upload," *Order* ¶ 36, that is an arbitrary and meaningless statistic, as broadband providers compete on the basis of many variables, not only raw throughput speeds, and consumers perceive nothing talismanic in the 25 Mbps metric. In any event, there are few if any geographic markets in which USTelecom's members are the "one option" for such services, and they therefore could not logically be subject to special regulation under this rationale even if it otherwise had merit.

[18] *See 2012 FTC Privacy Report* at 56 (suggesting that consumers "might have limited ability to block or control … tracking" by a mobile operating system unless they "chang[e] th[at] operating system" by purchasing a new phone and abandoning their existing OS-specific apps). Similarly, consumers often find it very difficult to switch web-based email accounts (thereby abandoning their prior email address used by friends and family) or prominent social network sites (particularly given the role of strong network effects).

Finally, turning from substance to rhetoric, the *Order* trots out familiar "gatekeeper" jargon to justify its irrational regulatory dichotomy. *See, e.g.*, *Order* ¶¶ 6, 28, 30, 36. That "tired refrain," as Commissioner O'Rielly aptly calls it (Dissent at 214), plays two distinct but equally flawed roles in the *Order*. First, the *Order* uses the term as a shorthand for the misconception rebutted above—that ISPs, as physical conduits, "see" more consumer data than any operating system, browser, or ad network can. Second, citing the *Open Internet Order*, this *Order* uses "gatekeeper" as a synonym for "terminating access monopoly"—*i.e.*, as a rationale for treating ISPs as regulated monopolists "even in the absence of 'the sort of market concentration that would enable them to impose substantial price increases on end users.'"[19] But the use of that concept here is incoherent. In the very narrow circumstances where it applies at all,[20] the "gatekeeper"/"terminating monopoly" concept addresses only the supposed ability of telecommunications carriers to charge high interconnection rates to entities that are *not its customers*, such as interconnecting carriers. It has no bearing on the retail competition that forces any carrier to deal fairly with *its own customers*.

B. The Commission Should Adopt a More Targeted Definition of "Content."

In addition to web-browsing and app-usage data, the Commission's list of "sensitive" information categories includes the "content" of online communications. USTelecom has no objection to including such a category if properly defined, but the Commission should scale back the *Order*'s overbroad definition of "content." The *Order* defines that term to include not only actual content, but also "any … part of a communication that is highly suggestive of the

[19] *Order* ¶ 36 (quoting Report & Order on Remand, *Protecting and Promoting the Open Internet*, 30 FCC Rcd at 5633, ¶ 84 (Mar. 12, 2015) ("*Open Internet Order*").

[20] *See, e.g.*, Jonathan E. Nuechterlein & Christopher S. Yoo, *A Market-Oriented Analysis of the "Terminating Access Monopoly" Concept*, 14 COLO. TECH. L.J. 21, 23 (2015) (terminating monopoly phenomenon poses no policy concern "except in very limited circumstances"), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2698393.

substance, purpose, or meaning of a communication." *Order* ¶ 102. That definition is so nebulous that it could be read to include almost any online activity, such as the innocuous fact that a customer visited a sports website because she is interested in sports and thus has the "purpose" of reading about them. The Commission should thus narrow its definition to include only the actual content of communications. Of course, even if information does not qualify as "content," it should still be treated as sensitive if it reveals otherwise sensitive facts, such as medical or financial information.

C. The Commission Should Reject "Heightened" Opt-In Requirements for Incentive Programs.

The *Order* effectively discourages ISPs from giving customers financial incentives to opt into marketing-oriented uses of their data, both (1) by imposing unusually "heightened" notice-and-consent requirements, even for non-sensitive data, and (2) by announcing that the Commission will "closely monitor" the use of such incentives and "take action, on a case-by-case basis," against ISPs that offer any incentives that the Commission deems "predatory" or "coercive" in some undefined sense. *See Order* ¶¶ 301, 303; *see also* 47 C.F.R. 64.2011. As Commissioner O'Rielly explains, this approach is over-prescriptive and will deter a variety of pro-consumer measures, such as offers of discounts subsidized by productive data uses. *See* O'Rielly Dissent 218; *see also* Verizon Comments 45-53. On reconsideration, the Commission should confirm that such offers are generally desirable and pro-consumer and will not be subject to special scrutiny.

D. The Commission Should Eliminate Regulatory Obstacles to Ordinary First-Party Marketing.

Under the FTC's longstanding policy, "most first-party marketing practices are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice,"

even in the form of opt-out consent.[21] For example, if Amazon wishes to use its customers' browsing information to send them an advertisement for an entirely new type of Amazon service, it may do so outside of any notice-and-choice framework. The *Order* rejects that approach for ISPs and allows them to conduct first-party marketing without a notice-and-choice mechanism only for "communications services commonly marketed with the telecommunications service to which the customer already subscribes," such as those "commonly bundled together with the subscriber's [existing] service." *Order* ¶¶ 204-205.

As Commissioner O'Rielly notes, "there is no rational reason" to depart from the FTC's treatment of this issue. O'Rielly Dissent 217. The *Order* should thus be revised to "extend[] inferred consent to the marketing of *all* products and services offered by broadband providers and affiliates as long as the affiliated relationship is clear to consumers." *Id.* (emphasis added). Consumers fully expect to receive such first-party communications, and "if broadband providers cannot market new products and services on the same terms as online companies—or even other brick and mortar businesses—there will be less incentive to invest and develop new services." *Id.* at 217-218 (internal quotation marks omitted).

The *Order* also mixes apples and oranges when it invokes the Do Not Call and CAN-SPAM rules as support for its more restrictive approach (*Order* ¶ 200). Those rules enable consumers to reduce the *volume* of commercial messages they receive via telephone calls and emails. But those rules have no bearing on *which* messages will fill (for example) the advertising space on webpages—and, in particular, whether those messages will be more relevant or less relevant to particular consumers. And no matter what first-party marketing rule

[21] *2012 FTC Privacy Report* at 40; *see also id.* at iv, 39. The main exception to this general rule involves the use of sensitive information. This section addresses only first-party marketing based on non-sensitive information.

the Commission adopts, consumers are always free to "opt out of receiving all solicitations by asking that they be added to the provider's existing do not call, do not email, and/or do not solicit list."[22]

Nothing in section 222 prevents the Commission from treating first-party marketing by ISPs the same way that the FTC treats such marketing by everyone else. Section 222(c)(1)(B) permits a carrier to infer consent when it markets a service that is "necessary to, or used in, the provision of" telecommunications services already provided to a customer. In 1999, the Commission concluded that this provision is sufficiently flexible to permit a highly deregulatory approach to first-party marketing. In particular, a service that is *not* currently provided to a customer can be considered "necessary to, or used in, the provision of" a telecommunications service that *is* currently provided to that customer if those two services are "reasonably understood by customers as within the existing service relationship."[23] That condition should be deemed satisfied if the customer understands—for example, through common branding—that the services are offered by the same company or its affiliates. Indeed, the Commission concluded that wireless carriers may infer consent when they use CPNI to market any and all "information services" offered by them or their affiliates.[24] The Commission should adopt that approach here, too, and extend it to wireline as well as wireless ISPs. As belt-and-suspenders, the Commission

[22] Letter from William H. Johnson (Verizon) to Marlene H. Dortch (FCC), WC Docket No. 16-106 (Sept. 29, 2016) ("*9/29/2016 Verizon Ex Parte*").

[23] Order on Recon. and Pet'ns for Forbearance, *Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 14 FCC Rcd 14409, ¶ 43 (1999); *see also id*. ¶ 45 (focusing on whether customers "expect that their service provider can and will offer these services along with the underlying telecommunications service").

[24] *Id.* at ¶ 43 ("In the CMRS context, carriers should be permitted to use CPNI, without customer approval, to market information services and CPE to their CMRS customers."); *accord* 47 C.F.R. § 64.2005(b)(1).

could simultaneously forbear from any arguably contrary requirements imposed by Section 222.[25]

E. The Commission Should Eliminate Regulatory Obstacles to the Use of Customer Data for Internal Analytics and Product Improvement.

The *Order* also subjects ISPs to irrationally restrictive notice-and-choice requirements when using sensitive customer information simply to conduct internal analytics, improve network performance, or develop and provide services that are necessary to or used in the provision of telecommunications services, such as technical support for customers that encounter connection problems due to their web-browsing history. The *Order* acknowledges that ISPs use many types of customer data to "conduct internal analyses" and "develop and improve their products and services and to develop or improve their offerings or marketing campaigns generally, apart from using [information] to target specific customers." *Order* ¶ 205. All such information uses should thus be exempt from any notice-and-choice framework. In a single sentence, however, the *Order* limits that exemption to non-sensitive information and thus implicitly requires ISPs to obtain opt-in consent to these wholly benign uses of any information deemed "sensitive." *See Order* ¶ 205. That limitation, which the *Order* makes no effort to justify, makes no sense and once again reflects an inattention to cost-benefit concerns.

Broadband ISPs routinely use "sensitive" customer information, including precise geo-location data, for internal analytics and to develop and improve their services. *See 9/29/2016 Verizon Ex Parte* 1. This activity comes within the meaning of "necessary to, or used in, the provision of … service" and is thus eligible for inferred consent treatment. *See* 47 U.S.C.

[25] *See* Letter from James J.R. Talbot (AT&T) to Marlene H. Dortch (FCC), WC Docket No. 16-106, at 4 (Oct. 4, 2016) (explaining that forbearance criteria under 47 U.S.C. § 160 are satisfied); *AT&T Inc. v. FCC*, 452 F.3d 830 (D.C. Cir. 2006) (holding that statute authorizes "conditional forbearance" from legal requirements that may or may not apply).

§ 222(c)(1)(B). Such activity poses no discernible privacy concerns because the information at issue is already within the possession of the service provider and is not used to target individual consumers. But because the *Order* limits the inferred consent regime to "non-sensitive" data and has classified (for example) precise geo-location information as "sensitive," the *Order* hamstrings ISPs from using such critical information to enhance the value of their services to consumers. The costs of suppressing these benign data uses are substantial, and they outweigh any negligible privacy interests that opt-in treatment could possibly serve. The Commission should thus extend its inferred consent regime to cover the use of *any* customer information for internal analytics and product-improvement purposes.

F. The Commission Should Confirm That Notice-and-Choice Requirements Are Inapplicable to Initial Steps in the Creation of De-Identified and Aggregate Data.

As the *Order* recognizes, de-identified and aggregate data are properly excluded from its broadband privacy rules, including notice-and-choice requirements. *Order* ¶¶ 106-121. Of course, to create such data in the first place, an ISP must first take personally identifiable information and anonymize it to create aggregate or otherwise de-identified data sets. The *Order* nowhere suggests that ISPs must discharge any notice-and-choice obligations when "using" personally identifiable data in this technical sense as an initial step in creating aggregate or de-identified data. To avoid any question on the issue, however, the Commission should confirm that ISPs have no such obligations.[26]

[26] *See* Second Report and Order and Further Notice of Proposed Rulemaking, *In the Matter of Implementation of the Telecommunications Act of 1996*, 13 FCC Rcd 8061, ¶ 149 (1998) (making similar point concerning voice rules).

II. THE COMMISSION SHOULD CORRECT OTHER ASPECTS OF THE *ORDER* THAT MAY IMPOSE NEEDLESS COSTS.

A. The Commission Should Narrow Its Definition of "Data Breach."

The *Order* defines "data breach" to encompass "any instance" in which an unauthorized person has gained access to any "customer proprietary information," which broadly includes any CPNI and any "personally identifiable information," defined as "any information that is linked or reasonably linkable to an individual or device."[27] Under this set of definitions, a typical ISP might suffer many insignificant "data breaches" each day—for example, whenever an employee states a customer's name aloud in a crowded retail store or inadvertently discloses a list of customer cellphone numbers unaccompanied by names or addresses. For each such "breach," the *Order* "require[s] breach notification unless a carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach." *Order* ¶ 263.

In practice, that requirement, combined with the overbroad definition of "breach," will induce ISPs to go through the motions of "investigating" countless trivial "breaches" to document that they in fact pose "no harm to customers." Like other activity designed solely to check a regulatory box, these investigations will impose needless costs on ISPs and ultimately their customers. Additionally, to the extent these rules lead to over-notification, they will disserve consumers in a second respect as well. As the FTC aptly notes, consumers who receive too many notices eventually become numb to them and "fail to spot or mitigate the risks being communicated to them." FTC Staff Comments 31-32.

The Commission should amend its definition of "data breach" to avoid these concerns. All other data breach notification laws—even those that incorporate a harm-based notification

[27] 47 C.F.R. § 64.2002(c), (f), (m); *see Order* ¶ 261. The Commission uses the term "[b]reach of security" in its regulations as synonymous with "data breach," and we do the same here.

trigger—more narrowly define the information subject to breach-notification rules as information whose disclosure is reasonably likely to cause harm. For example, a typical state breach law limits notification requirements to unauthorized disclosure of sensitive information or data that, in combination, would facilitate unauthorized access to an online account.[28] Indeed, the Commission has followed that very approach in its own orders directing ISPs to ensure adequate data security, defining the relevant data categories as "either one of the following":

> (1) an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social Security number; (B) driver's license number or other government-issued identification card number; or (C) account number, credit or debit card number, in combination with any required security code, access code, PIN, or password that would permit access to an individual's financial account; or (2) a user name or email address, in combination with a password or security question and answer that would permit access to an online account.[29]

The Commission gave no reason for departing from that approach in the *Order*, and its much broader definition of covered information imposes needless costs. On reconsideration, the Commission should conform its definition of "data breach" to the consensus approach, which narrowly targets the types of information whose disclosure is reasonably likely to cause harm.

B. The Commission Should Root Any Notion of "Emotional Harm" in Objective Common Law Standards.

The *Order* states that a breach can trigger reporting and notification requirements even if it threatens no financial harm and raises only a risk of "emotional harm." *Order* ¶ 266. The concept of "emotional harm," however, is so subjective that anyone could assert it in response to any disclosure of virtually any information, no matter how objectively harmless. At a minimum,

---

[28] *See, e.g.*, Cal. Civ. Code § 1798.82(h); Fl. Stat. § 501.171(g); N.Y. Gen. Bus. Law § 899-AA; Tex. Bus. & Com. Code § 521.002(a).

[29] *In the Matter of Cox Communications, Inc.*, File No. EB-IHD-14-17829, ¶ 2(s) (Nov. 5, 2015); *see also In the Matter of AT&T Services, Inc.*, File No. EB-TCD-14-16243, ¶ 2(s) (Apr. 8, 2015). As discussed below, USTelecom preserves its legal claim that the Commission lacks authority under Section 222(a) to address non-CPNI data.

therefore, the Commission should impose limiting principles on this concept. It should take its cue from the Supreme Court, which recently held that "whether an intangible harm constitutes injury in fact" depends in part on "whether [the] alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[30] Here, the Commission should clarify that, to be cognizable for breach disclosure purposes, any "emotional" harm should, at a minimum, constitute the type of legal injury cognizable under traditional tort law. Without that limitation, ordinary breaches involving non-sensitive information and posing no reasonable risk of harm to consumers—*e.g.*, a sales agent accidentally accessing the wrong customer's records—could be construed as reportable breaches based on idiosyncratic and purely subjective notions of emotional harm.

C. The Commission Should Confine the Term "Personally Identifiable Data" to Information That Is Reasonably Linkable to *Persons*.

The *Order* defines the class of protected "personally identifiable information" as "any information that is linked or reasonably linkable to an individual *or device*." 47 C.F.R. § 64.2002(m) (emphasis added), *see Order* ¶¶ 89-94. The words "or device" should be eliminated from that definition. As Commissioner O'Rielly explains, "[i]f a device cannot be linked to a specific individual, information that may be linked to the device would fall outside the scope of the statute and should not be subject to these rules."[31] The *Order* makes no coherent response to this point. It states only: "While some commenters argue that we should not include information linkable to a device in the definition of PII, we find that such identifiers are often and easily linkable to an individual[.]" *Order* ¶ 91 (footnote omitted). That is a non-

[30] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016).

[31] O'Rielly Dissent 214 (internal quotation marks, brackets, and ellipsis omitted) (noting that section 222(c)(1) is limited to "individually identifiable" CPNI).

sequitur. Insofar as such identifiers *are* linkable to an individual, it is unnecessary to include the words "or device" in the definition of PII. Including those words anyway thus accomplishes nothing beyond expanding that definition to include device identifiers that are *not* linkable to personally identifiable information and thus should remain unaffected by this regulatory scheme.[32]

D. The Commission Should Extend the Business Customer Exemption to Broadband Internet Access Services Purchased by Businesses.

The *Order* properly exempts enterprise customers from its privacy rules for voice services because they actively negotiate their terms of service. *Order* ¶¶ 306-309. The *Order* nonetheless withholds "a business exemption for BIAS services purchased by enterprise customers" on the premise that "BIAS services by definition are 'mass market retail service[s],' and as such we do not anticipate that it will be typical for purchasers to negotiate the terms of their contracts." *Id.* ¶ 308. That premise is mistaken. For example, major E-Rate and Rural Health Care participants purchase what the Commission has characterized as mass market BIAS services,[33] yet they often use formal bidding processes and have heavily negotiated contracts. The relevant issue here is not whether a given service is often sold to mass market customers, but whether a given purchaser of that service is a business customer. If the answer to that question is yes, prescriptive privacy regulations are as unnecessary as they are burdensome. The business customer exemption should thus extend to BIAS as well as voice services.

III. THE *ORDER* IS UNLAWFUL.

[32] *See, e.g.*, Verizon Comments 40-42 (describing Verizon's anonymous identifiers).

[33] *Open Internet Order*, ¶ 189 ("To be clear, 'mass market' includes broadband Internet access services purchased with support of the E-rate and Rural Healthcare programs, as well as any broadband Internet access service offered using networks supported by the Connect America Fund (CAF).").

Although this petition focuses on the *Order*'s policy flaws, USTelecom respectfully refers the Commission to the legal arguments presented in the petitions for reconsideration filed by CTIA and NCTA. USTelecom will not repeat those arguments in full, but urges the Commission to heed them when considering this petition.

First, the *Order* pervasively violates the Administrative Procedure Act because, as discussed above, it bases critical regulatory decisions on unsound logic, disregard of record evidence, and/or inattention to cost-benefit considerations.[34] Second, and for similar reasons, the *Order*'s marketing and other use restrictions violate the First Amendment.[35] For example, the *Order*'s sweeping definitions of "sensitive" data categories are unconstitutionally over-inclusive because they include many online activities that are not genuinely sensitive. *See* Section I.A, *supra*. The *Order*'s use restrictions also do little to promote any genuine privacy interest because they are unconstitutionally *under*-inclusive in the sense that all other Internet companies will continue making pervasive use of the exact same customer information that the *Order* restricts ISPs alone from using. *See, e.g.*, AT&T Comments 94-95; CTIA Comments 85-87.

The Commission further lacks statutory authority to adopt these restrictions on ISP data practices. To begin with, the Commission erred in reclassifying broadband Internet access in 2015 as a common carrier service, thereby stripping the FTC of authority it had exercised for the prior two decades (*see Order* ¶ 24). USTelecom thus urges the Commission to reverse that

[34] *See, e.g.*, *Michigan v. EPA*, 135 S. Ct. 2699 (2015) ("Agencies have long treated cost as a centrally relevant factor when deciding whether to regulate. Consideration of cost reflects the understanding that reasonable regulation ordinarily requires paying attention to the advantages *and* the disadvantages of agency decisions."); *id.* at 2707 ("[n]o regulation is 'appropriate' if it does significantly more harm than good"); *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) (to satisfy APA, agency "must examine the relevant data and articulate a satisfactory explanation for its action, including a rational connection between the facts found and the choice made") (internal quotation marks omitted).

[35] *See* Laurence Tribe and Jonathan Massey, *The Federal Communications Commission's Proposed Broadband Privacy Rules Would Violate the First Amendment* (May 27, 2016) (attached to letter of the same date from CTIA, NCTA, and USTelecom); AT&T Comments 91-100; Verizon Comments 29-40.

classification decision and remove this impediment to the FTC's authority. In the process, the Commission will necessarily acknowledge that ISP privacy practices are not subject to section 222, which applies only to "telecommunications carrier[s]."

In any event, so long as the 2015 reclassification decision stands, the Commission still lacks statutory authority to adopt these new regulations for the reasons that Commissioner O'Rielly explains in dissent (at 212-214). First, information widely available to the rest of the unregulated Internet ecosystem—as most such information here is—cannot be treated as "proprietary" under *any* provision of Section 222, including Section 222(a) ("proprietary information") and 222(c) ("consumer proprietary network information"). As Commission O'Rielly explains, "proprietary information is information that a person or entity owns to the exclusion of others, and thus it is not proprietary if other individuals or entities can access the information and use it for their own commercial purposes. … Unlike traditional voice calls where the only parties that had access to call records were those already subject to section 222(c)—the local exchange carrier and in some instances the interexchange carrier—multiple parties that are unregulated by section 222 have access to an end user's online activities." O'Rielly Dissent 213 (internal quotation marks omitted). That information thus "fall[s] outside the scope of section 222(c)." *Id.*

Second, "there is no independent authority in section 222(a) to regulate privacy or data security, regardless of the technology," and therefore "the categories of information that the [*Order*] ma[kes] up within section 222(a)—'customer proprietary information' and its subset 'personally identifiable information'—are outside the scope of the provision." *Id.* at 212-213. The *Order* likewise errs in invoking section 201(b)—which prohibits unjust and unreasonable prices and practices "in connection with" telecommunications services—to fill the jurisdictional

holes of section 222. *See Order* ¶¶ 368-370. That tactic both disregards the congressional policy choices reflected in the jurisdictional limitations of section 222[36] and contradicts the Commission's obligation to observe "a limiting principle [for section 201(b)] consistent with the structure of the statute and its other provisions."[37] In Commissioner O'Rielly's words, "if data protection falls within the ambit of 201(b)," one "can only imagine what else might be a practice 'in connection with' a communications service."[38]

[36] *See, e.g., Bloate v. United States*, 130 S. Ct. 1345, 1354 (2010).

[37] *Maracich v. Spears*, 133 S. Ct. 2191, 2200 (2013) (interpreting phrase "in connection with" in the Driver's Privacy Protection Act of 1994).

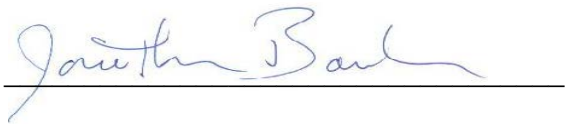
[38] Notice of Apparent Liability, *TerraCom, Inc. and YourTel America, Inc.*, 29 FCC Rcd 13325, 13353 (2014) (dissenting statement of Commissioner O'Rielly); *see also* USTelecom Comments 32-33. The *Order*'s efforts (at ¶¶ 371-72) to support these rules under various Title III provisions and under Section 706 are even more implausible. *See* AT&T Comments 110-113.

CONCLUSION

For the reasons discussed above, the Commission should reconsider the *Order* and should grant this Petition.

Respectfully submitted,

United States Telecom Association

By: 

Jonathan Banks.
B. Lynn Follansbee

607 14th Street, NW, Suite 400
Washington, D.C. 20005
(202) 326-7300

January 3, 2017