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

REPLY IN SUPPORT OF PETITION FOR RECONSIDERATION BY THE UNITED STATES TELECOM ASSOCIATION

The United States Telecom Association ("USTelecom") respectfully files this reply in support of its petition for reconsideration ("petition" or "PFR") of the Commission's *Order*.[1] Like the *Order* itself, the oppositions to the petition avoid genuine engagement with the reasons we have given for aligning the Commission's privacy regime with that of the Federal Trade Commission. The oppositions are thus meritless for the same reason that the *Order* is a textbook case of arbitrary and capricious decision-making. The Commission should now do what it should have done already: conduct a genuine cost-benefit analysis and revise its rules to avoid unfounded inconsistency with the FTC's well-established and generally applicable framework.

I. THE OPPOSITIONS PRESENT NO BASIS FOR DENYING RECONSIDERATION OF THE *ORDER'S* NOTICE-AND-CHOICE RULES.

The *Order* saddles ISPs with uniquely expansive opt-in burdens when they seek to make productive use of online information, including information that has never before been considered "sensitive." For example, because other Internet companies are subject to the FTC's more flexible regime, they confront no opt-in requirement when they serve sports-related ads to consumers who visit sports-related websites. But the *Order* subjects ISPs, and them alone, to an opt-in requirement for

[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"*). Although USTelecom focuses here on the respects in which the *Order* is arbitrary and capricious, it preserves all other legal challenges to the *Order* and respectfully refers the Commission to the filings made by the other parties seeking reconsideration.

marketing-related uses of *any* web-browsing information, whether it involves sensitive subject matter or not. The *Order* thus impairs the ability of ISPs to compete with others in the digital advertising market space, an area where they are not market leaders.[2]

As our petition explains, the Commission adopted that asymmetrical notice-and-choice regime without addressing objections by USTelecom and others that the costs of its uniquely expansive opt-in requirement are substantial and far outweigh the negligible benefits.[3] For example, USTelecom submitted an exhaustive analysis by former FTC Commissioner (now Professor) Joshua Wright analyzing the social costs of overbroad opt-in requirements.[4] As Professor Wright explained, opt-in is not a costless, consumer-friendly version of opt-out that ISPs can readily accommodate, as the *Order* and its defenders assume. *Order* ¶ 194; New America Opp. 10; Center for Democracy & Technology "CDT" Opp. 12-13. Instead, overbroad opt-in rules generate costly market failures because, when consumers decline to opt in, most do so out of inertia or indifference rather than any considered objection and fail to internalize the larger social costs of that non-choice for the rest of the Internet ecosystem. As a result, overbroad opt-in requirements exert upward pressure on retail broadband prices by shutting off a potentially significant source of revenues on the other side of this inherently double-sided market.[5]

---

[2] Peter Swire, Justin Hemmings & Alana Kirkland, The Institute for Information Security and Privacy at Georgia Tech, *Online Privacy and ISPs: ISP Access to Consumer Data Is Limited and Often Less Than Access By Others* (Feb. 29, 2016).

[3] *See, e.g.*, USTelecom Comments 8-16; AT&T Comments 51-61, 88-90.

[4] 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).

[5] *Wright Econ. Analysis* 20-22. Free Press asserts that ISPs should be forbidden to "double-dip" by supplementing subscription revenues with revenues based on productive uses of non-sensitive customer information. Opp. 12. Under that logic, newspapers and magazines would be forbidden to sell ad space because they also charge subscription fees. Free Press appears unfamiliar with two-sided market dynamics, in which revenue reductions in one market impose upward pricing pressure in the other.

The *Order* acknowledges none of these concerns; indeed, it does not even cite Professor Wright's analysis. For that reason and others, it violates the Commission's basic APA obligation to "examine the relevant data and articulate a satisfactory explanation for its action," *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983), and "answer[] objections that on their face appear legitimate," *Mistick PBT v. Chao*, 440 F.3d 503, 512 (D.C. Cir. 2006).

The *Order*'s defenders now ignore all of these concerns as well. Like the *Order* itself, their opposition briefs do not mention Professor Wright's analysis even though it plays a central role in our petition for reconsideration. Nor do the oppositions address the social costs—including higher broadband prices—of imposing overbroad opt-in rules on broadband providers. Nonetheless, without a trace of irony, the oppositions argue that our petition should be denied on the ground that it "simply rehash[es] arguments that have been fully considered by the Commission." CDT Opp. 1; *see also* New America Opp. 1; Free Press Opp. 4. That is not a coherent basis for denying reconsideration where a petitioner's very complaint is that the Commission did *not* "fully consider" arguments and thus violated the APA's central requirement of reasoned decision-making.[6] The Commission should act now to correct that shortcoming rather than wait for judicial compulsion to take its APA obligations seriously.

More generally, the oppositions offer no meaningful response to any of our arguments for aligning the Commission's notice-and-choice rules with the FTC's. For example, some oppositions argue that the Commission should give itself a pass for departing from the FTC's regime because the *Order* accepts "the FTC's guidance and enforcement regime in many significant ways." CDT Opp. 16. It is true that the *Order* accepts *in concept* the FTC's longstanding position that opt-in requirements should be reserved for uses of "sensitive" information. But the *Order* departs radically from the FTC's regime by concluding that *all* web-browsing and *all* app-usage data are categorically "sensitive" and should thus be

[6] In any event, even where the Commission *has* "fully considered" the arguments in a petition for reconsideration, its rules "simply permit" and "do not require" the dismissal of the petition on that ground. Order Granting Stay Petition in Part, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, FCC No. 17-19, at ¶ 11 (Mar. 1, 2017) (emphasis omitted).

subject to opt-in requirements. *See Order* ¶¶ 181-190. That position is as baseless as it is unprecedented. As Google has explained, "extend[ing] an opt-in consent requirement to all web browsing information [is] unjustified" because, as "[t]he FTC's framework recognizes," consumers "do not have the same expectations when they shop or get a weather forecast online" as they do when they engage in "healthcare or financial transactions."[7]

That FTC-overseen distinction between "sensitive" and "non-sensitive" web-browsing information underlies the privacy regime applicable to the rest of the Internet ecosystem (including the companies that provide the overwhelming majority of Internet advertising today). The opponents thus ignore reality when they suggest that applying the same distinction to ISPs will give rise to new and intractable implementation problems. *See, e.g.*, CDT Opp. 20. As we have explained, other Internet companies implement that distinction countless times a minute on the basis of transparent industry-wide guidelines, and they do so in ways that protect the privacy of sensitive data. PFR 7-8. The opponents do not respond to those points, let alone identify any basis for concern that ISPs will be somehow less capable of implementing the sensitive/non-sensitive distinction than any other category of Internet companies.[8] Further, contrary to the argument made by CDD, this argument holds for children's information, as well as other sensitive information, as ISPs, like other Internet companies, are able to offer distinct protections, such as opt-in consent, to use children's information.[9] CDD Opp. 7-8.

---

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

[8] Contrary to CDT's suggestion (Opp. 20), we do not purport to have identified "the outer bounds of sensitive information" by citing well-recognized categories of sensitive information. Our point is simply that the Commission should align its regime with the FTC's so that any given category of information will be either sensitive or non-sensitive for *all* participants in the Internet ecosystem rather than sensitive for some and non-sensitive for others. Similarly, the Commission should clarify that information qualifies as the (presumptively sensitive) "content of communications" only if it is treated as such for other ecosystem participants. *See* PFR 13.

[9] As CDD acknowledges, there is no disagreement that children's information should be considered sensitive. ISPs will continue to operationalize the treatment of children's information the same way as other online providers.

Some opponents implausibly contend that, no matter what the policy merits of alignment with the FTC, section 222 *requires* "differential treatment for telecommunications providers." New America Opp. 11; *see also* Free Press Opp. 10-11. It does no such thing. It requires opt-in consent ("express prior authorization") in only two contexts: access to "call location information" for cellular and VoIP telephone calls and certain uses of "automatic crash notification information." 47 U.S.C. § 222(f). In all other contexts, the Commission has always exercised discretion to impose less burdensome choice mechanisms, including opt-out.[10]

There is similarly no basis for woodenly extending the Commission's legacy opt-in rules for telephone call detail information on the theory that "[w]eb browsing and app usage history are the digital equivalent to call history." Public Knowledge Opp. 4. As we have explained, that analogy is facile because consumers' expectations about the closed telephone network bear no resemblance to their expectations about the open Internet—where, as they are aware, countless Internet companies collect their web-browsing information in order to serve them relevant advertisements. PFR 10-11. For the same reason, Free Press is wrong in asserting that "[e]dge providers' scope of access to their customer's information is immaterial" to the ISP-specific rules presented here. Opp. 9. Customers expect a broad range of online companies to collect non-sensitive online information for marketing purposes, they do not distinguish between ISPs and other online companies for that purpose, and appropriate privacy rules are ultimately rooted in such expectations.[11] Indeed, the irrational inconsistency of the current marketing

[10] *See, e.g.*, Third Report and Order, *Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 17 FCC Rcd 14860, ¶¶ 5-9 (2002).

[11] *See, e.g.*, FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, at 24, 38-39 (Mar. 2012) *("2012 FTC Report")*. A recent consumer survey confirms that 94 percent of consumers agree with the statement that "[a]ll companies collecting data online should follow the same consumer privacy rules so that consumers can be assured that their personal data is protected regardless of the company that collects or uses it." Public Opinion Strategies & Peter D. Hart, Memorandum to Progressive Policy Institute, at 2 (attached to Letter from Will Marshall, Progressive Policy Institute, to Marlene Dortch, FCC, WC Docket No. 16-106 (May 26, 2016)).

rules with the FTC regime—their selective application to ISPs but not to other participants in the Internet ecosystem—dooms them under both the APA and the First Amendment.[12]

The opponents fare no better when they recite the *Order*'s discredited claim that ISPs have categorically greater visibility into online activities than any "edge" provider. *E.g.*, CDT Opp. 11; Consumers' Union ("CU") Opp. 3; New America Opp. 8. That position ignores (1) the rapidly increasing prevalence of encryption, which limits the visibility of ISPs but not edge providers; (2) users' tendency to shift continuously among different Wi-Fi and cellular networks; and (3) "[t]he volume and extent of personal data that edge providers collect," which is "staggering." Pai Dissent 210; *see also* O'Rielly Dissent 214-215. Public Knowledge is also wrong to suggest (Opp. 6) that a 2012 FTC report blessed the *Order*'s position on this issue. That FTC report in fact explained that "ISPs are just one type of large platform provider" with access to customer information; that "operating systems and browsers" such as Android and Chrome are also large platform providers and "may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles"; and that consumers "might have limited ability to block or control such tracking" unless, for example, they "chang[e] their operating system."[13] The FTC further emphasized "that any privacy framework should be technology neutral" as between these types of "large platform provider[s]." *2012 FTC Report 56.* Indeed, Acting FTC Chairman Maureen Ohlhausen recently confirmed that the *Order* challenged here "does not serve

[12] *See* PFR 22 & n.35; *see generally Greater New Orleans Broadcasting Ass'n v. United States*, 527 U.S. 173, 193-94 (1999) ("in commercial speech cases, decisions that select among speakers conveying virtually identical messages are in serious tension with the principles undergirding the First Amendment"); *Transactive Corp. v. United States*, 91 F.3d 232, 237 (D.C. Cir. 1996) ("A long line of precedent has established that an agency action is arbitrary when the agency offered insufficient reasons for treating similar situations differently.").

[13] *Id.* at 56. The report is also five years old and thus predates widespread encryption.

consumers' interests" insofar as it "create[s] two distinct frameworks—one for Internet service providers and one for all other online companies."[14]

More unpersuasive still are claims that ISPs face less competition than other Internet companies or benefit from greater switching costs and are thus somehow less receptive to consumer privacy preferences. *E.g.*, CDT Opp. 12; CU Opp. 4. As we have explained (PFR 11-12), the leading social networks, browsers, and operating systems in fact enjoy less competition and higher switching costs than many ISPs do, yet they are subject to the FTC's more flexible regime. Nor can the opponents plug that empirical hole with facile "gatekeeper" rhetoric. *E.g.* New America Opp. 6-7.[15] Again, to the limited extent the "gatekeeper" construct is meaningful at all, it applies only where telecommunications carriers deal with interconnecting entities that are *not its customers.* PFR 12. It has no coherent application to the relationships between an ISP and its own retail customers. *Id.* If anything, ISPs have unusually strong incentives to deal fairly with end users on notice-and-choice issues because ISPs face competition thus creating a business imperative to maintain subscribers' goodwill.

In sum, the Commission should align its notice-and-choice regime with the FTC's by distinguishing between sensitive and non-sensitive web-browsing and app-usage data. As discussed in our petition, the Commission should align that regime with the FTC's in several additional respects as well. First, it should eliminate any suggestion that ISPs will trigger special regulatory concerns when they use incentive-based offers to *encourage* customers to opt in to productive uses of their information. *See* PFR 13. Second, it should remove regulatory obstacles to ordinary first-party marketing by extending "inferred consent to the marketing of *all* products and services offered by broadband providers and

[14] Joint Statement of Acting FTC Chairman Maureen K. Ohlhausen and FCC Chairman Ajit Pai on Protecting Americans' Online Privacy (Mar. 1, 2017), https://www.ftc.gov/news-events/press-releases/2017/03/joint-statement-acting-ftc-chairman-maureen-k-ohlhausen-fcc.

[15] In a similar vein, New America argues that ISPs should be treated differently on the theory that "[c]onsumers do not need any particular edge provider to access the internet, but they do need a BIAS provider." Opp. 7. This, too, is specious. New America could just as easily argue for stricter privacy regulation of mobile operating systems because "consumers do not need any particular ISP to access the internet, but they do need an operating system."

affiliates as long as the affiliated relationship is clear to consumers," O'Rielly Dissent 217 (emphasis added), rather than only an artificial subset composed of "communications services commonly marketed with the telecommunications service to which the customer already subscribes," *Order* ¶ 205. The oppositions do not seriously engage in the substance of either issue.

Finally, the Commission should confirm that ISPs confront no notice-and-choice obligations when they use any customer information—including sensitive information—for internal analytics, product-improvement, and similar purposes. *See* PFR 16-17. CDT criticizes this request, not because it disagrees with our position, but because it believes that the *Order* already clearly supports it. CDT Opp. 16. But as we have explained, paragraph 205 of the *Order*, which CDT does not cite, contains a stray sentence suggesting that notice-and-choice rules might still apply to *sensitive* information in this context.[16] Because CDT agrees that notice-and-choice rules should not apply even to sensitive information for these purposes, it presumably would have no objection to a clarifying statement from the Commission on that point.

II. THE OPPOSITIONS PRESENT NO BASIS FOR OPPOSING THE OTHER RELIEF SOUGHT IN USTELECOM'S PETITION

Apart from notice-and-choice, USTelecom's petition seeks reconsideration on a number of additional issues as well. For example, it asks the Commission to narrow its definition of "data breach," which currently encompasses "any instance" in which an unauthorized person gains access to "any information" linked to person or device. PFR 18 (citing 47 C.F.R. § 64.2002(c), (f), (m)). As we have explained, that definition is untenably overbroad because, if applied literally, a typical ISP might suffer many trivial "data breaches" every day. As a practical matter, the definition might induce ISPs to conduct costly and pointless "investigations" for every such breach, no matter how obviously harmless, simply to check a regulatory box. *Id.* at 18-19. Our petition thus asks the Commission simply to conform its

[16] *See Order* ¶ 205 ("This exception also allows carriers to conduct internal analyses of *non-sensitive* customer PI to develop and improve their products and services and to develop or improve their offerings or marketing campaigns generally[.]") (emphasis added).

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. No opposition takes issue with our petition on that point. *Cf.* CDT Opp. 18-19 (supporting current "standard" without addressing USTelecom's definitional point).

As discussed in our petition, the Commission should revise its data-breach rules in two additional respects. First, it should clarify that purely "emotional harm" (*see Order* ¶ 266) can trigger reporting and notification requirements only if it would constitute the type of legal injury cognizable under traditional tort law, rather than idiosyncratic and purely subjective notions of emotional harm.[17] Contrary to New America's suggestion (Opp. 15), we are not arguing that emotional harm should never trigger any notification requirement; we are simply observing that the concept requires sensible limiting principles provided by generally applicable state law. Second, the Commission should 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. *See* PFR 20-21. Devices have no privacy interests; people do. Linkability to devices thus raises privacy concerns only if there is some genuine basis for linking the devices to particular people. *See* O'Rielly Dissent 214.

Finally, the Commission should extend the "business customer" exemption to broadband Internet access services purchased by enterprise customers, such as E-Rate and Rural Health Care participants. As we have explained, the relevant question 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 that often uses formal bidding processes or negotiated contracts. *See* PFR 21. None of the oppositions appears to address the merits of that issue.

[17] *See* PFR 20 (discussing *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016)).

CONCLUSION

For the reasons discussed above, the Commission should reconsider the *Order* and the petition for reconsideration should be granted.

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

March 16, 2017