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 CENTURYLINK, INC.

Kathryn Marie Krause
Associate General Counsel
CENTURYLINK, INC.
1099 New York Avenue, NW
Suite 250
Washington, D.C. 20001
(303) 992-2503

Linda K. Gardner
Chief Privacy Officer and
Associate General Counsel
CENTURYLINK, INC.
600 New Century Parkway
New Century, KS 66031
(913) 353-7030

Russell P. Hanser
Joshua M. Bercu
WILKINSON BARKER KNAUER, LLP
1800 M Street, NW, Suite 800N
Washington, D.C. 20036
(202) 783-4141

May 27, 2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY

CenturyLink shares the Commission's commitment to protecting broadband consumers' privacy, but respectfully disagrees with the *Notice*'s unsupported claim that the agency must adopt aggressively prescriptive privacy rules in order to do so. The framework proposed in the *Notice* dramatically and unwisely departs from the principles-based FTC approach to Internet privacy that has served consumers extremely well for decades. Rather than impose this unprecedented privacy regime, the Commission should adopt principles based on the framework set forth by a coalition of industry groups earlier this year. Such principles would protect consumer privacy and security while also affording providers flexibility to implement and update their practices.

The Notice's Proposal Relies on a Misunderstanding of the Internet Ecosystem and Consumer Expectations. The proposed rules are based on the erroneous view that BIAS providers enjoy unique access to commercially valuable consumer information. In particular, the supposed distinctions between broadband companies and edge providers do not survive scrutiny. BIAS providers have neither comprehensive nor unique access to consumer information. BIAS

notices available at the point of sale is simply impractical, particularly given the high proportion of CenturyLink customers who purchase service over the phone. Also problematic is the Commission's proposal regarding how to communicate advance notice of material changes. In practice, this proposed mandate would amount to impractical overkill, contrary to the very privacy-enabling goals the Commission espouses.

***The Commission Should Not Adopt the Restrictive Customer-Approval Framework Proposed in the* Notice.** The Commission should reconsider the proposed approval framework in its entirety. In practice, the *Notice*'s proposal would hamper BIAS providers from making uses and disclosures beneficial *to their customers.* Any consent framework should take into account the sensitivity of the consumer information used and whether such information is disclosed outside the BIAS provider's relationship with third parties who might work on behalf of the BIAS provider or in concert with them in creating bundled packages. Any rules should require, at most, that providers offer the ability for consumers to opt out of certain uses and disclosures of information. The proposed framework poses substantial challenges to BIAS providers' ability to serve their customers, and should be amended to better meet the needs of customers and BIAS providers alike.

The Commission Should Not Restrict Consumer Choice. The Commission should not deny consumers the ability to make certain choices. For example, it should not bar customers from accepting financial inducements, such as lower monthly rates, in exchange for their consent to use and share certain information. There is nothing in the Communications Act that can be read to address such practices, and such prohibitions would be bad policy.

The Proposal's Data Security Requirements Afford Providers Insufficient Flexibility. CenturyLink agrees with the *Notice*'s premise that strong data security is important. However, the *Notice*

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 CENTURYLINK, INC.

CenturyLink, Inc. ("CenturyLink") here responds to the Notice of Proposed Rulemaking ("*Notice*") in the above-referenced proceeding.[1] As described herein, CenturyLink understands the importance of protecting consumers' privacy. Nevertheless, CenturyLink has significant concerns regarding numerous aspects of the *Notice*, which depart dramatically from the general and long-standing U.S. regulatory approach to Internet privacy and ultimately would disserve the consumers whose interests it purports to promote. CenturyLink urges the Commission to reconsider its proposed approach.

I. INTRODUCTION.

CenturyLink understands and affirms the critical importance of protecting the privacy and security of broadband Internet access service ("BIAS") customers. Customers need and deserve to trust their Internet service provider ("ISP"),[2] and ISPs work hard to develop and

---

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

maintain that trust. Moreover, in the competitive BIAS marketplace, CenturyLink faces challenges from cable companies, wireless providers, satellite operators, and new rivals such as Google. We must work diligently to satisfy user demands, including those regarding privacy protections, to have any hope of maintaining (much less growing) our customer base. To this end, CenturyLink respectfully disagrees with the *Notice*'s unsupported claim that "[a]bsent legally-binding principles, [broadband] networks have the commercial motivation to use and share extensive and personal information about their customers."[3] Quite the contrary. The primary incentive faced by CenturyLink and other BIAS providers is to attract and retain customers. We cannot do so if we exploit our customers or otherwise fail to meet customer expectations. Thus, CenturyLink and other BIAS providers have long incorporated into their business operations well-established privacy principles, such as those espoused by the Federal Trade Commission ("FTC"). This approach has protected consumers, while providing CenturyLink and others the flexibility to conduct their businesses and compete in the Internet ecosystem.

The framework proposed in the *Notice*, unfortunately, represents a dramatic and unwise departure from the long-standing principles-based FTC approach to Internet privacy, which has served consumers well. The *Notice* claims that this departure is supported by consumer expectations and the Commission's notion that BIAS providers enjoy unique access to valuable customer information that distinguishes them from other players within the Internet ecosystem, such as Google, Facebook, and other content providers. But both of these premises are false. First, the *Notice* is bereft of any support for the proposition that BIAS providers generally are

[3] *Notice* ¶ 3.

"us[ing] and shar[ing] extensive and personal information about their customers"[4] in ways inconsistent with customer expectations.[5] The absence of such evidence is particularly striking given that most BIAS providers have long operated under the FTC framework that the *Notice* deems inadequate.

Second, BIAS providers do not, in fact, en

BIAS providers differ from other Internet ecosystem enterprises in significant ways – is meritless and should be abandoned.

In any event, the *Notice*'s proposed approach would fail consumers. It would inhibit providers' ability to offer services in the way their customers demand, and to find new ways to generate revenue, which in turn would reduce investment incentives.[7] It would most certainly perplex consumers, who could mistakenly think that the Commission's privacy rules apply broadly to *all* Internet companies. It would then compound this confusion by inundating customers with notifications that are not relevant to their needs and might prevent them from using the services they enjoy. Finally, the proposal would distort the marketplace by imposing burdensome and restrictive rules on one set of market participants but not their competitors – an outcome that Section 222 does not mandate, even if one assumes that that provision applies to BIAS in some form. The proposed approach would create these consumer and marketplace problems without any corresponding benefits to consumer privacy. There is no evidence either that broadband providers are systemically mishandling user information or that the overly prescriptive regime the *Notice* contemplates would remedy any real-life harm.

Thus, while CenturyLink shares the Commission's view that protecting the privacy of sensitive customer information is important, it believes that the proposed framework is poorly suited for achieving that goal. In fact, adoption of the framework would be inimical to the interests of consumers, competition, investment, and continued innovation. Rather than impose this unprecedented privacy regime, the Commission should adopt a regime based on the

[7] *See Moody's Says FCC Internet Privacy Could Harm Broad Internet Providers*, Reuters (Mar 15, 2016), http://www.reuters.com/article/us-usa-fcc-internet-moody-s-idUSKCN0WH1TC

framework recently set forth by a coalition of industry associations ("Industry Framework").[8] The Industry Framework appropriately calls for a flexible approach to privacy and data security for CPNI that is harmonized with the FTC's framework and backed by enforcement against unfair or deceptive acts or practices that materially harm consumers. It specifically sets forth the principles of (1) transparency, focused on notice about a provider's CPNI use and disclosure practices; (2) respect for context and consumer choice, including by considering the sensitivity of the data and the context in which it was collected when determining an appropriate choice mechanism; (3) data security based on reasonable security safeguards; and (4) data breach notification in which providers have the flexibility to determine how and when to provide consumers notice of breaches.[9] Such a framework would protect consumer privacy and security while also providing flexibility for providers to implement and update their practices as consumer expectations and technologies evolve.

II. THE *NOTICE*'S PROPOSAL RELIES ON A MISUNDERSTANDING OF THE INTERNET ECOSYSTEM AND CONSUMER EXPECTATIONS.

The Commission's proposed framework and rules are based largely on the notion that BIAS providers can comprehensively monitor their customers' Internet traffic and enjoy unique access to commercially valuable consumer information. This view is incorrect, and has resulted in a deeply flawed proposal.

According to the *Notice*, BIAS providers "have the ability to capture a breadth of data that an individual streaming video provider, search engine or even e-ecommerce site simply does

[8] *See* Letter from Matthew M. Polka, Steven K. Berry, Meredith Attwell Baker, Michael Powell, and Walter M. McCormick, Jr. to Tom Wheeler, Chairman, FCC (Mar. 1, 2016), https://www.ustelecom.org/sites/default/files/documents/Wheeler%20Letter%20Re%20Privacy%20Principles%203%201%2016%20%283%29.pdf.

[9] *Id.*

not."[10] The *Notice* suggests that edge providers only have direct access to the information that customers choose to share with them by virtue of

with whom BIAS providers compete in a variety of contexts – have access to as much commercially valuable consumer information as BIAS providers do, if not more.[13]

Further, as technology evolves, the information-collection capabilities of these non-ISPs are increasing, not decreasing. Developments such as the use of encryption and secure online services (*e.g.*, VPNs) have substantially limited BIAS providers' ability to view their consumers' online activities. Most significant is the rapid shift away from the basic HTTP protocol to the HTTPS protocol, which prevents BIAS providers from being able to see customer content and detailed URLs.[14] The Commission acknowledges the significance of encryption, noting that "*absent use of encryption*, the broadband network has the technical capacity to monitor traffic transmitted between the consumer and each destination, including its content."[15] The "absent use of encryption" predicate is critical, however, because the class of instances in which users are not encrypting data is shrinking rapidly. Today, all of the top 10 web sites, and the vast majority of the top 50, are encrypted by default or upon user log-in; by the end of 2016, more than two-thirds of online traffic will be encrypted.[16] In fact, Google states that 77% of the data associated with its services already is encrypted.[17]

---

[13] *Id.* at 8.

[14] *Id.* at 9

[15] *Notice* ¶ 4 (emphasis added).

[16] Swire Paper at 7, 28-29.

[17] *See* Michael Grothaus, *Google Reveals How Many Requests To Its Sites Are Now Encrypted*, Fast Company (Mar. 16, 2016), http://www.fastcompany.com/3057915/fast-feed/google-reveals-how-many-requests-to-its-sites-are-now-encrypted?partner=rss. The *Notice* suggests that encryption is of limited use because BIAS providers are aware of the top-level domains that their subscribers visit and additional information, including how long a user visited a website, even when traffic is encrypted. *See Notice* ¶ 4; *see also* Swire Paper, Diagram 1-A. As Professor Swire has explained, however, "these sources of data are less useful for tracking and online

In addition to a greater use of encryption, BIAS providers' access to sensitive user data is curtailed by the growing trend towards the use of proxy services such as VPNs. Use of such services blocks from the ISP's view not only the content and detailed URLs associated with a given communication, but also the name of the domain the user visits. While current statistics show modest adoption in the U.S.,[18] leading Internet companies are offering proxy services, suggesting that the use of such privacy-enhancing offerings "will climb sharply in the coming years."[19] For example, Google has introduced the "Data Saver" proxy service, the scale of which "is likely to become substantial because it is integrated with Google's operating system and web browser."[20] More recently, Opera announced a free VPN feature for its desktop web browser and iOS mobile web browser, indicating that "[w]ith Opera VPN you can block ads, change your virtual location and stop sites from tracking you around the web."[21] While not yet pervasive, the availability of easy-to-use proxy services, including but not limited to VPNs, is clearly on the rise, and use is set to grow dramatically. Growth in these offerings, combined with the trend toward encryption of nearly all Internet traffic, should put to rest any notion that BIAS providers enjoy ubiquitous access to users' Internet activities.

---

advertising than content or detailed URLs" (which encryption blocks). "Today, content and deep links are blocked for roughly half of traffic, and [Swire et al.] expect that fraction to rise." Addendum to Swire Paper at 2 (Mar. 6, 2016), http://www.iisp.gatech.edu/sites/default/files/documen

Edge providers, in contrast, are enjoying greater and growing access to online consumer information. The expansion and increased use of the Internet has boosted the number of non-BIAS providers that have access to significant online user activity, often across multiple networks. Platforms such as social networks, search engines, operating systems, webmail, browsers, mobile apps, and e-commerce sites are proliferating and can easily obtain consumer data.[22] The pervasive access enjoyed by these edge providers – no matter how many different ISPs customers might use to access them over the course of a day – provides them with a comprehensive view of individual online activities.

In addition to the data available to providers of each type of such services, an important trend is the emergence of integrated companies that collect data from consumers across various different services or "contexts." While a BIAS provider has access to information about customers only when the customer is using its network, companies capable of "cross-context" and "cross-device" tracking are able to combine information from numerous services/platforms about an individual using multiple devices over *multiple* networks.[23] As a result, the top 10 ad-selling companies earn 75 percent of online advertising dollars.[24] None of these entities achieved its position as a result of providing BIAS. Indeed, these entities and other edge providers enjoy first-mover advantages stemming from their relatively long-term use of customer

[22] *See, e.g.*, Swire Paper at 4.

[23] As Swire describes, non-ISPs "dominate" in both cross-context tracking ("combining information from multiple services/platforms," *e.g.*, social networks and webmail, to capture "the real insights") and cross-device tracking (tracking targeting the user across multiple devices, such as smartphones, tablets, and laptops). *Id.* at 8.

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

data for advertising and other commercial purposes. As the Swire Paper notes, "ISPs are not market leaders in any of these major areas; rather, they are just starting to compete in some of them."[25]

In response to evidence that edge providers enjoy access to at least as much customer information as do BIAS providers, the Commission appears to assume that, if BIAS is a telecommunications service, Section 222 demands the application of sector-specific privacy requirements that need not track those applicable to other actors in the Internet ecosystem.[26] Even assuming *arguendo* that the classification of BIAS withstands judicial scrutiny,[27] nothing in the Communications Act or in the record co

a Commission order from 2002.[28] Nearly 15 years old, that decision predates Gmail by two years, the first iPhone by five years, and other common features of today's Internet (e.g., mobile applications) by even longer. And the Commission's order is just that – an order, not research demonstrating consumer expectations.[29] Regulating one segment of the complex Internet ecosystem differently from the rest will harm competition, inhibit innovation, and cause other unintended consequences. Rather than protect consumers, application of unduly prescriptive privacy and data security rules only applicable to a subset of Internet companies will give consumers a false impression about how online data is collected and shared. This is a recipe for consumer confusion, as well as industry and marketplace stagnation.[30]

Forcing BIAS providers to comply with rigid rules while other providers – those with equal or greater access to consumer information – are permitted to continue offering services under the FTC's more flexible regime will also make it more difficult for BIAS providers to compete in the online marketplace. A strict opt-in regime for all but a few routine uses of data would result in increased costs for consumers and a reduction of competitive online service offerings. A recent essay by former FTC Chairman John Leibowitz and former FTC General Counsel Jonathan Nuechterlein summarizes the situation well:

---

[28] Notice ¶ 129 (citing Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, 14883 ¶ 51 (2002) (discussing record, and not research, regarding third-party disclosure of CPNI, then understood to apply only to telephony)).

[29] See id. In several areas, the Notice also cites research from the Pew Research Center to try to demonstrate consumers' expectations. See, e.g., id. However, such research focuses on consumer expectations on the Internet generally, not the practices of broadband providers. It therefore cannot form the basis for a regime that sharply differentiates between BIAS providers and edge providers.

[30] See infra Section IV.

> The rules would further subject all ISPs—and ISPs alone—to unprecedented compliance costs and keep them from efficiently monetizing online data in the same way that Google and Facebook have long done, with astounding consumer benefits. Such restrictions would exert upward pressure on broadband prices and undercut the FCC's central mission of promoting broadband investment and adoption.[31]

Given the well-documented economic and consumer benefits produced by the Internet ecosystem to date, and the indisputable benefits of competition in promoting consumer welfare, government public policy should encourage a level playing field for Internet industry rivals. Unfortunately, the proposals in the *Notice* would do just the opposite.

III. THE COMMISSION LACKS THE LEGAL AUTHORITY TO ADOPT THE SWEEPING PRIVACY REGIME IT PROPOSES.

Even assuming *arguendo* that the Commission may lawfully impose Title II common carrier obligations, including Section 222, on BIAS providers, the Commission lacks the legal authority to impose the specific privacy rules proposed by the *Notice*. The proposed rules govern a BIAS provider's use, disclosure, and protection of a wide swath of information – essentially any customer information that a BIAS provider may have obtained or generated regarding a customer – and extend well beyond the scope of the jurisdiction afforded the Commission by Congress.

At the outset, the Commission must exercise restraint in its interpretation of Section 222. It must, in the first instance, respect the framework adopted by Congress. Moreover, regulations implementing Section 222 trigger First Amendment concerns and must be narrowly tailored to advance the objectives identified by Congress. That constitutional problem would apply not only to a BIAS provider's commercial communications with current or potential customers for the

[31] Jon Leibowitz and Jonathan Nuechterlein, *The New Privacy Cop Patrolling the Internet*, Fortune (May 10, 2016, 1:00 AM), http://fortune.com/2016/05/10/fcc-internet-privacy/.

purpose of proposing a commercial transaction, but also to communications and information shared among that provider's own affiliates or business partners. Given these threshold limitations on the Commission's jurisdiction and discretion, the *Notice*'s proposed rules, if adopted, would not stand.

Section 222 limits the Commission's privacy and data security authority to CPN8(N4-0.0003 Tw[(adop2ed,

Section 201(b)[35] or any other provision of the Communications Act to expand the limited privacy authority that Congress provided the agency through Section 222. Doing so would effectively give the agency unlimited authority over subjects Congress chose *not* to address. This is both unsustainable and contrary to principled statutory interpretation.[36]

Just as the Commission cannot expand CPNI beyond those elements included by Congress in its definition, it cannot use the general language of Section 222(a)[37] – stating that a carrier "has a duty to protect the confidentiality of proprietary information of, and relating to, . . . customers" – to expand the scope of protected customer information beyond CPNI to some undefined and unbounded range of customer proprietary information ("CPI"). This is clear from Section 222's structure. Section 222(a) sets forth the general objective of the provision – to protect proprietary information of "other telecommunication carriers . . . and customers" – without providing any specifics. The specifics are then supplied by the following subsections: Section 222(b) details the protection of proprietary information obtained from other carriers, and Section 222(c) details the protection of customers' individually identifiably proprietary information, limited to CPNI as that term is defined in Section 222(h)(1).

Given the legal doctrine that "a specific statute controls a general one,"[38] and the express labeling of Section 222(a) as "general," Section 222(a) cannot be construed to provide the

---

[35] *Notice* ¶ 295.

[36] *See, e.g., Whitman v. Am. Trucking Ass'ns, 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.").

[37] 47 U.S.C. § 222(a).

[38] *RadLAX Gateway Hotel v. Amalgamated Bank*, 132 S. Ct. 2065, 2070-71 (2012); *Bulova Watch Co. v. United States*, 365 U.S. 753, 758 (1961) (citing *Fourco Glass Co. v. Transmirra Corp.*, 353 U. S. 222, 228-229 (1957)); *Clifford F. MacEvoy Co. v. United States*, 322 U.S. 102,

Commission with unbounded authority to regulate a service provider's protection of customer information beyond the specific protections and categories set out in Section 222(c) and Section 222(h)(1). Congress identified specific privacy concerns regarding CPNI and adopted specific measures to address those concerns; it gave no indication that it was granting a much broader customer privacy mandate with respect to concerns it had not identified about a broader class of customer information that it had not discussed at all (and, what's more, for a class of services that did not even exist at the time the provision was adopted).[39] Simply put, the statute cannot reasonably be read to grant the Commission authority to regulate BIAS providers' confidentiality obligations respecting customer information other than individually identifiable CPNI.

The *Notice*'s effort to expand the class of customer information covered by Section 222 is especially problematic in the context of information that is readily available to any entity within

customer is indisputably wrong. Rather, often it is easily obtained by multiple parties, and cannot be deemed CPNI.

Further, applying any proposed requirements to all CPI without adequately taking into account the sensitivity of any given category of information is bad policy and inconsistent with consumer expectations. Consumers expect that their sensitive information will be treated differently then information that is not sensitive, such as information that is readily and publicly available and thus poses no risk of identity theft or consumer harm. Applying one set of prescriptive requirements to all personally identifiable information ("PII"), CPI (however defined), and CPNI could, for example, force BIAS providers to expend unnecessary resources protecting non-sensitive information rather than prioritizing resources for sensitive information. Rather than adopt broad definitions of PII, CPI, and CPNI,[41] the Commission should limit its focus to defining and addressing any categories of sensitive information BIAS providers may obtain by virtue of providing BIAS service that consumers would expect the provider to properly protect and secure.

The Commission also should exclude from the CPNI category information, such as traffic statistics, that is best viewed as proprietary to the *provider*, and not the customer.[42] Such information is not "made *available* to the carrier *solely* by virtue of the carrier-customer relationship,"[43] but rather is created by the BIAS provider, and not subject to Section 222's

[41] CenturyLink urges the Commission to rethink this sweeping approach in general; below, these comments highlight specific problems of applying the proposed rules to essentially all consumer information, irrespective of the sensitivity of such information. At the very least, the Commission must either reconsider each of its proposals to take into account data sensitivity or define the categories of information covered by its proposal in a more limited manner.

[42] *See, e.g.*, *Notice* ¶¶ 41, 47.

[43] 47 U.S.C. § 222(h)(1) (emphasis added).

mandates. In this respect, the *Notice*'s suggestion that *all* customer-related information is presumptively proprietary to the customer – or, put differently, that customers have an exclusive property interest in this information[44] – ignores longstanding business practices and commercial realities. Indeed, customers in all sectors routinely provide information to their service providers, be they credit card companies, grocery stores, banks, or others, which invest in collecting, maintaining, and aggregating that information as part of their routine business operations. Thus, courts have long observed that customers do not possess a sole or overriding proprietary interest in assets of service providers,[45] which would include information assets. Rules premised on the view that customers are the sole owners of the underlying information generated by a provider's rendering of service, to the exclusion of a provider's rights to make use of information for reasonable business purposes, would pose the risk of an unconstitutional taking. Such risks should not be ignored or minimized.

Finally, information that is anonymized and/or reasonably de-identified cannot and should not be covered by the rules, regardless of whether it is in aggregate form. Section 222(c) clearly limits the restrictions it sets forth to "individually identifiable" CPNI.[46] Consistent with

---

[44] *See, e.g.*, *Notice* ¶ 10 (referring to "customers' own data"); *id.* ¶ 36 (referring to customers' "protection of their own private information"); *id.*, App. A, 47 C.F.R. § 64.7001(a)(2) (discussing customers' rights "with respect to their own proprietary information").

[45] *See, e.g.*, *Board of Pub. Util. Comm'rs v. New York Tel Co.*, 271 U.S. 23, 32 (1926) ("Customers pay for service, not for the property used to render it. … By paying bills for service, they do not acquire any interest, legal or equitable, in the property used for their convenience or in the funds of the company."); *see also Pacific Gas & Electric Co. v. Public Utilities Comm'n*, 475 U.S. 1, 22 n.l (1986) (Marshall, J., concurring in the judgment).

[46] *See* 47 U.S.C. § 222(c)(1).

the statute, the Commission cannot address any information that is properly de-identified, and for which there is little to no privacy risk to consumers.[47]

IV. THE PROPOSED TRANSPARENCY OBLIGATIONS WILL CONFUSE CONSUMERS.

CenturyLink, like other BIAS providers, already delivers clear and readily accessible notice about our privacy practices to consumers. We believe it critical that consumers understand how we use, store, and disclose the information we hold about our customers. In an era when dissatisfied customers can – and do – switch to other BIAS providers, this is not only good practice, but good business. The *Notice* blithely presumes a "lack of competition between BIAS providers and … high switching costs."[48] But CenturyLink knows that in the real world, broadband providers do face competition – customers who experience practices that do not meet their demands do not remain customers for long. To ensure that customers understand how CenturyLink treats the customer information in our possession, we have carefully constructed our privacy policy and related disclosures to make them clear and comprehensible.

In fact, CenturyLink's website provides several different tools to enable current and prospective customers to review and understand our practices. These include a series of short videos in which key company officials – such as our Chief Privacy Officer, Linda Gardner –

---

[47] This would be consistent with the FTC's approach, which exempts data from that agency's privacy framework if three conditions are met: (1) "the company must take reasonable measures to ensure that the data is de-identified" by means of "a variety of technical approaches"; (2) the company "must publicly commit to maintain and use the data in a de-identified fashion"; and (3) if the company "makes such de-identified data available to other companies . . . it should contractually prohibit such entities from attempting to re-identify the data." *FTC Privacy Report* at 20-22.

[48] *Notice* ¶ 128.

describe our privacy and data security practices in transparent and understandable terms.[49] They also include both a brief overview[50] and a more fully detailed explanation[51] of our policy, as well as answers to frequently asked questions.[52] The *Notice*'s proposal would in effect supplant these customer-friendly, market-driven disclosures with an expansive one-size-fits-all mandate, the effect of which would be to decrease, not enhance, consumer welfare.

A. The *Notice*'s Approach to Transparency Is Overly Prescriptive.

CenturyLink agrees that transparency is a critical ingredient in any privacy framework, but believes that the proposal, which would legislate the content of specific disclosures, would be unproductive and overly prescriptive. Regulations dictating the location, timing, and content of information-practice disclosures, rather than allowing providers flexibility to determine how best to communicate such information to their customers, would disserve consumers.[53] As the FTC noted in its comprehensive *FTC Privacy Report*, consumer interests are best promoted by endowing providers with the flexibility to tailor their disclosures to specific evolving needs over

[49] Linda Gardner et al., *Privacy Policy Video Series – Privacy Overview, Information Security, Information Collection, Information Sharing, and Children's Privacy*, CenturyLink,

time.[54] This pragmatic approach considers whether customers received adequate notice of relevant and material information, rather than compelling comprehensive but largely irrelevant disclosures that must utilize a prescribed font or template.[55]

Moreover, the laundry list of information the Commission proposes to require in privacy policies is at odds with the agency's goal that companies provide "understandable information about their privacy practices"[56] and general trends to make privacy policies simpler for consumers to understand. The Commission's proposal – which would effectively require significant expansion and likely additional complication of privacy policies – would only exacerbate the trend to shortening privacy policies and making them more reader-friendly, undoing the steps companies like CenturyLink have taken to enable more tailored consumer access and render practices comprehensible by consumers.[57]

Another significant problem is presented by the proposal that providers make their about theirrt

customers' bills, *and* (3) a link on the provider's homepage, mobile application, and any functional equivalent.[61]

In practice, this mandate would amount to impractical overkill, contrary to the very privacy-enabling goals the Commission espouses. CenturyLink today provides advance notice of material changes through our website and privacy policy. By mandating other forms of notice, however, the proposal ma

customers can exercise their choice in the matter."[64] But in practice, the *Notice*'s proposal would hamper BIAS providers from making such "beneficial uses and disclosures of customer PI" – uses and disclosures beneficial *to their customers* – without offering any offsetting benefit to customer privacy. It thus would inhibit providers from offering the services their customers want and demand. The Commission should reconsider the proposed approval framework in its entirety. Any rules should require, at most, that providers offer the ability for consumers to opt out of certain uses and disclosures of their information.

A. Any Consent Framework Should Take Into Account the Sensitivity of the Consumer Information Used and Whether Such Information Is Disclosed.

The *Notice* suggests that "[c]ustomers' privacy is affected differently depending upon the entity using or accessing their private information and the purposes for which that information is being used."[65] But, as described above, the entity using the data is not the most critical issue.

personal data."[67] Indeed, as the White House has observed, "[u]nauthorized *disclosure* of *sensitive* information can violate individual rights."[68] The White House's focus on sensitive information is telling – the collection, use, and sharing of consumers' non-sensitive information, including information that is publicly available, generally will not have a significant impact on consumer privacy.

Similarly, the FTC has observed that "first-party collection and use of non-sensitive data (*e.g.*, data that is not a Social Security number or financial, health, children's, or geolocation information) creates fewer privacy concerns than practices that involve sensitive data or sharing with third parties."[69] Therefore, according to the FTC, first-party marketing generally need not require choice, except in certain circumstances – such as where companies seek to use *sensitive* data for first-party marketing.[70] Again, the FTC indicated specific concerns with respect to the use of *sensitive* data and the *sharing* of consumer data, but did not raise the same concerns with regard to internal use of non-sensitive information.

The *Notice* now, however, proposes to depart from the more restrained approach of the White House and FTC, and instead adopt a framework under which most *uses*, let alone *disclosures*, of collected information would require opt-in consent, regardless of the sensitivity of such information. This departure is unnecessary and ultimately will disserve consumers, for the reasons discussed below.

---

[67] The White House, *Consumer Data Privacy in a Networked World*, at 11 (Feb. 2012) (emphasis added), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[68] *Id.* at 6 (emphases added).

[69] *FTC Privacy Report* at 15-16.

[70] *Id.* at 40, 47.

B. The Proposed Framework Poses Substantial Challenges to BIAS Providers' Ability to Serve Their Customers.

Not only is the proposed regime inconsistent with the framework established by the FTC (which generally applies to providers of all other Internet services that collect, use, and disclose consumer information), but it also would unnecessarily restrict BIAS providers' ability to serve their customers. To provide just one example: as drafted, the proposal explicitly would require opt-in consent for the sharing of customer information with joint venture partners and independent contractors.[71] The *Notice* claims that this aspect of its proposal is consistent with the Commission's existing CPNI rule.[72] It is not. Regardless of whether such rule is justified to begin with, 47 C.F.R. § 64.6007 requires opt-in consent from a customer before disclosing that customer's *CPNI* to a carrier's joint venture or independent contractor for the purpose of *marketing* services to that customer.[73] The proposal here, however, would broadly apply to disclosure of *any* customer information for *any* purpose, other than those narrow purposes which meet the Commission's proposed criteria for "implied" or "inferred" approval.[74] Thus, the

[71] *See Notice* ¶ 127 n.221.

[72] *See id.*

[73] *See* 47 C.F.R. §§ 64.7002(e), (f).

[74] The proposed "inferred" approval categories are also indeed exceedingly narrow. *See* Proposed 47 C.F.R. § 64.7002(a) (deeming approval inferred for the provision of BIAS; billing purposes; protecting the provider or users; inbound marketing, referral, or administrative services only if initiated by the customer; certain public safety and emergency purposes; and as required by law). Notably, for inbound marketing, referral, or administrative services, "[a] customer is considered to have provided approval" if the "interaction was initiated by the customer and the customer *approves* of the use of such information to provide such service." *See id.* § 64.7002(a)(4) (emphasis added). Thus, for inbound marketing, referral, or administrative services, the customer actually would need to *explicitly* approve the use or disclosure of his or her information; it is by definition not inferred.

proposal is substantially more re

These barriers to the use and sharing of customer information could very well stop joint ventures from forming at very early stages, even if they would have provided beneficial new services to consumers and injected new competition to the marketplace. Such limits on providers' ability to innovate and compete undercut consumers' interests.

Nor can these challenges be overcome simply by obtaining consent, as the Commission seems to assume.[78] Companies would be left with impossible choices under the proposed framework. In many cases, affirmative requests for consent might annoy or confuse customers – especially given that the proposal will massively increase the number of such requests that providers must issue. Thus, in each particular case, a provider would need to decide whether to make the request or to forego the new beneficial practice altogether to conserve customer goodwill. If companies do not limit activities requiring customer consent, the result under a strict opt-in approach would be to subject consumers to repeated pop-ups or emails seeking their consent to a wide variety of practices, many of which would not concern all but the most privacy-focused consumers.[79]

In sum, the proposed restrictions pose substantial challenges to servicing customers, and even could undermine the development and deployment of services that consumers may demand. They are certainly not critical or necessary to protect consumer privacy.

---

[78] *See id.*, Statement of Chairman Tom Wheeler at 2 ("And this proposal does not prohibit ISPs from using and sharing customer data – it simply proposes that the ISP *first* obtain customers' express permission before doing so.").

[79] As FTC Commissioner Maureen Ohlhausen has explained, setting privacy baselines "[t]oo high … 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." Maureen K. Ohlhausen, Commissioner, FTC, *The FTC, the FCC, and BIAS*, Remarks at the George Mason University School of Law, Public Policy Briefing on Privacy Regulation after Net Neutrality (Mar. 30, 2016), https://www.ftc.gov/system/files/documents/public_statements/942823/160331gmuspeech1.pdf.

C. Any Consent Framework Should Rely on Notice and Choice Through the Customer's Ability to Opt Out.

CenturyLink's belief that the Commission's proposed approval framework is severely misguided should not be read as a repudiation of our customers' privacy interests. To the contrary. As described above, CenturyLink and other BIAS providers' primary incentive is to attract and retain customers. We could not do so if we exploited our customers or otherwise failed to meet customer expectations, such as by using and disclosing customer information in ways contrary to our customers' expectations and desires.

Accordingly, any approval framework the Commission ultimately adopts should reject a default opt-in. Instead, it should require opt-in consent only (if at all) for the use and disclosure of particularly sensitive information; all other uses should be subject to implied consent or an opt-out regime. An opt-out regime is flexible enough to allow companies to innovate and provide services that consumers demand. And it has been deemed sufficient by the White House and FTC to protect consumers. In other words, opt-out ensures consumer privacy protection and responds to providers' need for flexibility, without risking the privacy-imperiling effects of consent fatigue. There is no reason to doubt an opt-out regime's efficacy in protecting consumers' privacy interests.[80] CenturyLink thus supports the application of an opt-out framework in which the party collecting information makes the means of opting out very clear to consumers (and in a manner the provider believes best designed to inform consumers), and reduces or eliminates relevant barriers to such opt-out, ensuring that customers who wish to do so can easily make that election.

[80] *See, e.g., U.S. West v. FCC*, 182 F.3d at 1239 ("Even assuming that telecommunications customers value the privacy of CPNI, the FCC record does not adequately show that an opt-out strategy would not sufficiently protect customer privacy.").

VI. THE COMMISSION SHOULD NOT RESTRICT CONSUMER CHOICE.

As described above, CenturyLink believes that the restrictive consent regime proposed in the *Notice* would inhibit providers from effectively serving their customers without an actual corresponding benefit to meeting consumers' privacy preferences. But the *Notice* does not stop there. Instead, it asks whether it should categorically remove consumers' ability to make certain choices about those preferences.[81] It appears that the Commission believes it needs to save consumers from themselves. But informed consumers can and should be the ones making choices about their privacy, such as whether to opt out of certain uses or disclosures of their information and under what circumstance. The Commission should not paternalistically and unilaterally remove such choice.

The Commission asks, for example, "whether business practices that offer customers financial inducements, such as lower monthly rates, for their consent to use and share their confidential information, are permitted under the Communications Act."[82] As an initial matter, there is nothing in the Communications Act that can be read to address such practices. An insurmountable ban on such financial inducements would be not only unlawful but also bad policy. As the *Notice* admits, "it is not unusual for consumers to receive perks in exchange for use of their personal information. In the brick-and-mortar world, loyalty programs that track purchasing habits and provide rewards in exchange for that information are common."[83] While

[81] *See Notice* ¶¶ 256-270.

[82] *Id.* ¶ 259.

[83] *Id.* ¶ 260. The *Notice* then observes that "[i]n the broadband ecosystem, 'free' services in exchange for information are common." *Id.* Notably, however, there are many services within the broadband ecosystem which are not free, but still rely on the exchange of information to improve the service, to control costs of the service, or for other purposes.

the Notice theorizes that consumers may not understand that they are exchanging their information as part of these bargains,[84] consumers actually reveal their true preferences by selecting such programs – they clearly prefer the lower costs of the goods and services made available in exchange for the information they offer up.[85] Thus, any outright prohibition adopted by the Commission would disserve consumers, who might miss out on services they want and value propositions they appreciate.[86] Any broadband privacy rules should permit properly informed customers voluntarily to enter contracts for lower monthly rates or to accept other financial inducements in exchange for their consent to the use and/or sharing of their information.

VII. THE PROPOSAL'S DATA SECURITY REQUIREMENTS AFFORD PROVIDERS INSUFFICIENT FLEXIBILITY.

CenturyLink agrees with the Notice's premise that strong data security is an important component of protecting our customers' privacy online.[87] Indeed, CenturyLink has been an industry leader in connection with data security and cybersecurity for many years, working collaboratively with the Commission and other stakeholders on various initiatives. These include membership in the Commission's Communications Security, Reliability, and

---

[84] Id. ¶ 261.

[85] The Commission seems to assume that companies that offer rewards programs or other financial inducements could simply offer the lower prices without the program. That is incorrect – companies offer such programs because they get value from the exchange that offsets the reduced revenue. Banning such programs necessarily means higher prices from the companies that offer them, a result that is not in consumers' interests.

[86] Moreover, there is no justification for treating BIAS providers differently from other companies in both the online and offline worlds that could continue to offer such programs.

[87] See, e.g., Notice ¶ 167.

Interoperability Council ("CSRIC"), where CenturyLink representatives have participated at all levels from working groups to Chair.[88]

CenturyLink is committed to keeping customers' information secure and already invests substantial resources in doing so – *all without any regulatory compulsion*. CenturyLink uses reasonable technical, administrative, and operational safeguards to protect customer information and maintains a hierarchy of information-security related policies and standards, using ISO 27001 and NIST Special Publications as underlying guidance. These practices include extensive controls in the areas of personnel, systems, and facility security. CenturyLink's information security teams develop and maintain processes designed to identify new risks and to monitor and respond to known security risks. For example, the teams utilize intrusion detection and prevention systems, ongoing assessment of systems, software, and network environments, and partnering with audit teams to ensure CenturyLink systems and processes are in compliance with information security policies and standards. CenturyLink monitors suspicious events across all networks and systems; limits access to critical systems; ensures network availability and redundancy; and partners internally and externally with private industry associations and federal agencies on information sharing and mitigation efforts. In addition, CenturyLink has a fully documented, comprehensive disaster preparedness program ensuring all CenturyLink business units have business continuity, disaster recovery and emergency response plans for all critical

[88] *See, e.g.*, *FCC Announces the Recharter, Chair, Membership, and First Meeting of the Communications Security, Reliability, and Interoperability Council*, Public Notice, 30 FCC Rcd 6262 (PSHSB 2015) (announcing membership of CSRIC V); *FCC Announces Membership of the Communications Security, Reliability, and Interoperability Council*, Public Notice, 26 FCC Rcd 10973 (PSHSB 2011) (announcing appointment of CenturyLink's CEO as Chair of CSRIC for a two-year term).

functions and processes. They are reviewed, updated, and tested annually at a minimum to ensure their effectiveness.

CenturyLink also offers an array of retail security services solutions – ranging from penetration testing to Information System Security ("INFOSEC") Risk Assessment to data forensics – intended to empower businesses of all sizes to protect their own customers' information through flexible and scalable security solutions.[89] Consistent with our own practices and activities, CenturyLink believes that all providers should adopt reasonable data security safeguards based, in the *Notice*'s words, on "the nature and scope of the BIAS provider's activities, the sensitivity of the underlying data, and technical feasibility."[90]

The *Notice*, however, ultimately goes far beyond such a reasonable approach and would impose substantial costs without corresponding benefits. Notably, although the *Notice* purports to espouse a general data security standard based on reasonableness that would largely be consistent with the FTC's current approach,[91] the language of the proposed rule appears to contemplate a strict liability framework that obliges BIAS providers to ensure data security under any and all circumstances. In particular, it states unequivocally that "[a] BIAS provider *must ensure* the security, confidentiality, and integrity of *all* customer PI the BIAS provider

---

[89] *See, e.g.*, CenturyLink Business, *Professional Security Services*, http://www.centurylink.com/business/security/professional-security-services.html (last visited May 27, 2016).

[90] *Notice* ¶ 170.

[91] *See, e.g.*, *id.* ¶ 172 (stating that the proposal is "consistent" with FTC enforcement for companies' failure to take "reasonable and appropriate" steps to protect consumer data); *id.* ¶ 217 ("Our proposed approach also mirrors our existing CPNI rules for voice providers, which permit telecommunications carriers to individually determine the specific 'reasonable measures' that will enable them to comply with the general duty to discover and protect against unauthorized access to proprietary information.").

receives, maintains, uses, discloses, or permits access to from *any* unauthorized uses or disclosures, or uses exceeding authorization."[92] That articulation of the rule eschews all of the nuance implied by the *Notice*'s earlier endorsement of security practices "calibrated" to a provider's specific circumstances.[93]

The interpretation of this proposal as promulgating a strict liability approach is not alarmist or unfounded – indeed, that language is consistent with (if not foreshadowed by) the inflexible enforcement posture the Commission has taken in connection with cases involving data security to date. These enforcement decisions have recited a standard under which BIAS providers would be expected to take "*every* reasonable precaution" to protect customer data, effectively negating the "reasonableness" criterion altogether.[94] For instance, in the case against AT&T,[95] the Commission imposed an historic penalty after rogue call center employees with authorization to access customer information to fulfill their duties apparently sold customer information to criminals.[96] Similarly, in *TerraCom/YourTel*,[97] the companies were found apparently liable after customer information maintained by a vendor was accessed by a journalist

[92] *Id.*, App. A, 47 C.F.R. § 64.7005(a) (emphasis added).

[93] *Id.* ¶ 169.

[94] Despite their use of the term "reasonable," these decisions suggest that a provider must take every precaution that may on its own be considered reasonable, rather than undertaking precautions that are *collectively* reasonable.

[95] *AT&T Servs., Inc.*, Order and Consent Decree, 30 FCC Rcd 2808 (Enf. Bur. 2015).

[96] News Release, FCC, *AT&T to Pay $25 Million to Settle Consumer Privacy Investigation; FCC's Largest Data Security Enforcement Action*, 2015 FCC LEXIS 1042 (Apr. 8, 2015).

[97] *TerraCom, Inc. and YourTel America Inc.*, Order and Consent Decree, 30 FCC Rcd 7075 (Enf. Bur. 2015).

who "used" it only in the sense of threatening to publish a story about his ability to access the information.[98]

While CenturyLink does not condone any clearly improper conduct that may have occurred in those instances (many of the pertinent facts are not publicly available, and CenturyLink has taken no public position on the underlying issues), this precedent signals that the Commission is poised to look beyond providers' data security *practices* to scrutinize their data security *results* – with anything less than perfection exposing providers to significant enforcement liability. Such an absolutist approach to data security does not make sense in the complex and challenging environment in which data incidents occur.[99] As is widely recognized in the context of cybersecurity, different industry sectors and the companies within those sectors face unique and evolving threats that cannot always be anticipated and for which no defense may be feasible.[100] As a result, data incidents occur despite providers' best efforts – a regrettable reality, to be sure, but reality nonetheless.

---

[98] *TerraCom, Inc. and YourTel America Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13327 ¶ 6 (Enf. Bur. 2015).

[99] In contrast, the FTC's approach to data security focuses on reasonableness (which is sensible), not absolute security (which is unrealistic). *See, e.g.*, Edith Ramirez, Chairwoman, FTC, Prepared Statement before the U.S. Senate Committee on Homeland Security and Governmental Affairs at 4 (Apr. 2, 2014) ("[T]he [FTC] has made clear that reasonable and appropriate security is a continuous process of assessing and addressing risks …. [T]he [FTC] does not require perfect security.… [T]he mere fact that a breach occurred does not mean that a company has violated the law.").

[100] *See, e.g.*, National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, at 2 (Feb. 12, 2014) ("NIST Cybersecurity Framework") (observing that "[o]rganizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances" and referring to the "dynamic and challenging environment of new threats, risks, and solutions").

The infeasibility (and basic unreasonableness) of the *Notice*'s approach is further demonstrated by the unintended consequences that would arise as providers made decisions regarding how to manage their operations and treat data in an effort to guard against liability. For example, if providers will be strictly liable for illegal actions by their employees or a vendor's – even where they put in place reasonable administrative and technical safeguards to evaluate, train, and monitor such employees and to restrict their access to the customer information they truly need – they may be forced to reduce their customer-care staffs to reduce the risk that any of the customer representatives are bad actors. As a result, customers would experience longer wait times and delays in reaching customer service. In the alternative, providers may need to restrict the information that customer-care representatives may access, impairing their ability to resolve even routine customer concerns and increasing the need to place customers on long holds as disempowered representatives speak with supervisors with access to the necessary information. In addition, to avoid or at least mitigate potential liability, providers may ultimately determine not to retain certain data that could otherwise be used to offer customers conveniences and services.

A strict liability approach is particularly problematic given the *Notice*'s sweeping approach to defining customer PI for purposes of these rules. As discussed above, the proposal would apply Section 222's mandates to "any information that is linked or linkable to an individual" without regard to its sensitivity.[101] This broad scope may cause BIAS providers to employ data security practices designed solely to facilitate technical compliance with the rules, even if they involve an inefficient use of resources that otherwise could be allocated to protect sensitive consumer data. By way of example, to mitigate liability risk, providers might utilize

[101] *Notice*, App. A, § 64.7000(j).

resources to encrypt non-sensitive or otherwise publicly available data, such as a customer's name, thereby complicating the customer service experience and customers' access to their own data. The cost of such measures ultimately will be borne by consumers, who will reap no corresponding benefit.

In short, a general "reasonableness" standard is an appropriate baseline with respect to data security, and the relevant rules must remain tethered to reasonableness. To that end, the Commission should not impose prescriptive data security practices to meet this overarching standard.[102] Instead, it should afford providers full flexibility to protect customer information through means that are reasonable in light of their particular circumstances. Although the *Notice* does at times acknowledge the utility of such an approach,[103]

challenges associated with managing vendors and other external actors), and then goes further by proposing specific terms for those contracts.[105]

The imposition of such mandates – whether the five higher-level requirements that the *Notice* affirmatively proposes or the various details that the *Notice* proceeds to suggest – would contravene the government-wide consensus explicitly favoring flexibility over prescriptive, one-size-fits-all security mandates. Most notably, Executive Order 13636 directed that the nationwide Cybersecurity Framework must be "flexible, repeatable, performance-based, and cost-effective," and "incorporate voluntary consensus standards and industry best practices to the fullest extent possible."[106] The NIST Cybersecurity Framework that resulted "is not a one-size-fits-all approach to managing cybersecurity risk" but instead "is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes."[107] The Commission itself has embraced this paradigm – CSRIC IV and Commission officials have uniformly recognized that an approach based on voluntary mechanisms "can address fast-changing technology-based issues better than prescriptive regulation."[108] NTIA has embraced the same approach in its parallel multistakeholder process

---

[105] *Id.* ¶ 212.

[106] Exec. Order No. 13636, *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 11739, 11741 (Feb. 19, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[107] NIST Cybersecurity Framework at 2, 6.

[108] Admiral David Simpson, Remarks at the WTA – Advocates for Rural Broadband Spring Meeting, Cybersecurity Panel, at 3 (May 5, 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf; Communications Security, Reliability and Interoperability Council IV, *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report*, at 113 (Mar. 2015), http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf ("The NIST Framework is effective because it identifies functional categories of processes that industry members can self tailor according to their particular needs and capabilities. Rigid,

exploring cyber vulnerabilities.[109] All of these initiatives and positions are well known, yet the *Notice* does not even mention them. Their absence is especially conspicuous given the *Notice*'s professed interest in drawing guidance from external sources – for instance, the *Notice* cites every other NTIA multistakeholder process in recent years *except* for the one addressing cybersecurity.[110] Nor does the *Notice* even mention the pending Internet Policy Statement, which is expected to embrace CSRIC IV's non-prescriptive voluntary approach.[111]

To the extent the Commission, notwithstanding the well-understood and widely accepted virtues of a more flexible approach, remains inclined to mandate specific data security practices like those that comprise the second part of the *Notice*'s proposed two-step security framework, it should not prescribe the specific ways in which providers would implement these high-level

practices. Rather, it should allow providers the flexibility to adjust their practices as customer expectations, customer demands, and technologies evolve.

Without substantial changes, many of these further requirements would impose tremendous costs with limited benefit. For example, the *Notice* asks about requiring providers to provide their customers with access to all customer PI in their possession, including all CPNI, and a right to correct that data.[112] BIAS providers' networks and systems are not configured for the type of access the *Notice* contemplates. The technical updates required to allow a customer to access and correct all manner of information would be very costly, and those costs (like *all* costs) would ultimately be borne by consumers. There would, however, be very little corresponding consumer benefit, especially with respect to a great deal of information that has little or no consequence. Thus, any access requirement should be limited to information that a customer may actually have a reasonable interest in accessing and correcting, such as the customer's name, address, and payment information.

VIII. THE PROPOSED DATA BREACH NOTIFICATION WOULD RESULT IN OVER-NOTIFICATION AND NOTICE FATIGUE.

A. Current Regulation of Breach Notification Is Sufficient, Given Providers'

authorization, has gained access to, use, or disclosed customer proprietary information."[115] The *Notice* also seeks comment on a trigger to address over-notification.[116]

These proposals would result in a constant barrage of notifications to consumers, even in circumstances where said individuals are not at risk. As currently drafted, a "breach" notice obligation may be triggered by an event as innocuous as the disclosure of already-public data. This would desensitize customers to notices and give them a false impression about the security of their information on the Internet. Over-notification would also impose substantial disruptions on the consumer-BIAS provider relationship. Because the *Notice* singles out BIAS providers for its unduly prescriptive breach framework, such providers would be forced to inundate customers with notifications of "breaches" that are not comparably reported by other online entities under state laws. This asymmetry risks causing a significant artificial disparity in notification volume, which would confuse consumer evaluations of different entities' success in protecting data. The harm to public perception and brand value of the BIAS provider that would result is both unnecessary and unfair – and could even, in some cases, lead consumers to opt out of broadband use entirely.

C. Even if the Commission Moves Forward With Breach Notification Requirements, It Should Draw on State Law for Guidance.

To the extent that the Commission pursues its own separate breach notification obligation, it must address several concerns, and it should look to state laws for guidance.

Harm Element. The Commission should not require notice for "breaches" of information whose disclosure poses no risk of harm to consumers, including information that

[115] *Notice* ¶ 75.

[116] *See id.* ¶ 237

already is publicly available. Similarly, a good-faith exposure of customer information to employees should not be covered by any Commission breach notification rule.[117] It similarly makes no sense to require notification of a breach that only involves encrypted data. In these cases, the hassle and potential confusion occasioned by notification itself will impose greater harm than the purported "breach." Likewise, a provider's obligation to notify customers of a breach should not be triggered if, after an appropriate investigation, the provider determines that there is not a reasonable likelihood that material harm to the consumers has resulted or will result from the breach.[118] A harm element is particularly important given the exhaustive scope of information to which the proposed rules, if adopted, would apply.[119]

Reasonable Reporting Window. Providers need a reasonable amount of time to investigate and remediate any given breach before they are obligated to report. The *Notice* proposes to require BIAS providers and other telecommunications carriers to notify customers of CPI breaches no later than 10 days after discovery of the breach, absent a request by federal law enforcement to delay customer notification.[120] But to protect providers and consumers alike, the Commission must provide more time for post-determination reporting to both customers and the agency.[121] This approach would be in keeping with the aforementioned state-law regimes under which the Internet ecosystem has flourished to date.[122]

---

[118] *See id.* ¶ 237.

[119] *See generally* NCSL Security Breach Laws. Unlike the proposal here, state breach laws define PII in specific and concrete ways.

[120] *Notice* ¶ 236.

[121] That is, reports would be required no earlier than 30 days after the BIAS provider has determined the extent of the breach, what information is involved, and what customer's information was involved. Additionally, if a particular reporting deadline is prescribed,

Breach investigations are complex undertakings, and as a result take time. As a preliminary matter, investigations only begin with discovery of the breach itself; that is, responsible persons must somehow be made aware if the situation. Post-discovery, investigation itself takes time, as internal and external experts rigorously evaluate the situation. Sometimes, appropriate breach-related responses are readily apparent; often, however, they are not. When the latter is the case, additional time is necessary to conclusively determine what did or did not occur. Additionally, companies require time to address and remediate vulnerabilities before publicly disclosing a breach. If companies provide public notification of a breach prior to this point, they could be announcing the presence of a possible vulnerability to malicious actors that might still seek to exploit the vulnerability. Given these facts, premature notification can result in the provision of inaccurate and incomplete information regarding the scope of the breach and any potential harm to consumers.[123] As with Aesop's "Boy Who Cried Wolf," such notifications would corrode trust in the online ecosystem even when there has been no actual breach.

Ultimately, any notification timeline should be tied initially to the determination that a breach has occurred. Then, even after a BIAS provider has determined that a breach has occurred and its scope, it will need time to undertake several preparatory steps to assess how best to meet customer needs. Such steps might include, depending on the context, training customer service representatives to answer affected customers' questions in a meaningful and accurate

---

providers should be permitted to submit "initial reports," followed by "final reports" upon the termination of a full investigation.

[122] This window would, as discussed above, be comparable to period set out in the most stringent of all state reporting requirements. *See, e.g.*, NCSL Security Breach Laws.

[123] *See Lewert v. P.F. Chang's China Bistro, Inc.*, 2016 U.S. App. LEXIS 6766 (7th Cir. Apr. 14, 2016) (addressing potential legal consequences associated with an initially over-broad breach announcement and notification).

fashion, establishing specific 1-800 numbers for affected customers, making available credit monitoring services, and taking other necessary pre-notification steps. Mandating notice to customers before the requisite infrastructure is in place would make it more difficult for customers to get information they need and answers to questions they have, compounding rather than ameliorating any customer harm.

IX. CONCLUSION

For the reasons stated herein, the Commission should reconsider many of the proposals set forth in the Notice. The privacy interests of BIAS customers are undoubtedly important. The best way to protect those interests, while also promoting the continued development of a vibrant Internet ecosystem that has conferred great value on consumers for several decades, is to conform any broadband privacy regime to the approach long pursued by the FTC – an approach that has served consumers well. That approach should be grounded in flexibility and targeted at circumstances in which consumers face the prospect of actual harm. It should recognize the significant costs imposed by prescriptive micromanagement and the ways in which customers will be disserved by voluminous notifications and incessant requests for consent. And it should recognize that, even absent a detailed top-down legal regime, BIAS providers have and retain strong incentives to ensure the privacy and security of their users' data.

Respectfully submitted,

CENTURYLINK

/s/ *Russell P. Hanser*
Russell P. Hanser
Joshua M. Bercu
WILKINSON BARKER KNAUER, LLP
1800 M Street, NW, Suite 800N
Washington, D.C. 20036

Kathryn Marie Krause
Associate General Counsel
CENTURYLINK, INC.
1099 New York Avenue, NW
Suite 250