Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

COMMENTS OF SPRINT CORPORATION

Marc S. Martin
John Roche
James F. Ianelli
Perkins Coie LLP
700 13th St. N.W., Suite 600
Washington, D.C. 20005-3960
(202) 654-6200

Counsel to Sprint Corporation

Sprint Corporation

Maureen Cooney
Head of Privacy, Office of Privacy
Government Affairs

Matthew Sullivan
Counsel, Office of Privacy
Government Affairs

12502 Sunrise Valley Drive
Reston, VA 20196
703-592-7580; 571-287-8341

May 27, 2015

TABLE OF CONTENTS

SUMMARY

Sprint supported the FCC's reclassification of BIAS under Title II as a common carrier service and the reasonable application of Section 222 to BIAS. Sprint further supports the Commission's desire for privacy rules that reflect the importance of choice, transparency, and data security for BIAS customers. The proposed rules, however, must meet their intended purpose in a manner that (a) is consistent with reasonable BIAS customer expectations, (b) is technically and commercially practicable, and (c) presents a coherent regulatory structure for the broader Internet ecosystem. To satisfy these elements, Sprint offers the following recommendations on the Commission's proposals:

- Adopt a flexible privacy and security regime under Section 222 that closely aligns with the Federal Trade Commission's well-established framework for unfair and deceptive acts or practices. An aligned approach would continue to best protect consumers and would lend the most consistency to consumers' Internet service experience and privacy expectations.

- Limit the scope of privacy and security protections under Section 222 to current accountholders of BIAS services to reflect that Section 222 authority is limited to usage information associated with an actual provider-customer relationship. Further, the BIAS data covered by Section 222 should be limited to CPNI that is, by definition, identifiable to an individual. The Commission should not extend protections to any de-identified information that cannot reasonably be re-identified, regardless of whether such data is aggregate or non-collective.

- Allow BIAS providers to use customer data to engage in first-party marketing of communications-related services *and* non-communications related services, subject to customers' implied consent. The Commission also should adopt a broader view of services within the "communications-related services" category to account for BIAS providers' diverse offerings beyond broadband access, consistent with consumers' expectations and appetite for new and value-added features.

- Permit BIAS providers to tailor privacy notices based on the context of the provider-customer relationship and customer expectations.

- Calibrate the data breach notice proposals to focus on breaches that are reasonably likely to harm consumers, and to more closely align with requirements of the existing state data breach notification regimes, and the CPNI breach notification rules for voice telephony services. BIAS providers also should have flexibility to ensure robust data security using commercially accepted standards, rather than prescriptive risk assessment criteria.

- Uphold customer choice by allowing customers options for BIAS service based on data sharing, and dispute resolution of contracts.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

COMMENTS OF SPRINT CORPORATION

I. INTRODUCTION

Sprint Corporation ("Sprint") respectfully submits these comments in response to the Federal Communications Commission's ("FCC" or the "Commission") Notice of Proposed Rulemaking applying the privacy requirements of Section 222 of the Communications Act of 1934 (the "Act") to broadband internet access service ("BIAS").[1] This proceeding follows from the 2015 Open Internet Order, which reclassified BIAS providers as common carriers, thereby subjecting such providers to Section 222 of the Act.[2]

Sprint supports the primary goal of the Open Internet Order— to protect the vibrancy of the Internet ecosystem from unreasonably discriminatory practices.[3] Sprint believes, however,

---

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, FCC 16-39 (rel. Apr. 1, 2016) ("*Privacy NPRM*").

[2] *See Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015) ("*Open Internet Order*").

[3] *See* Sprint Comments, 2010 Open Internet Proceedings, Docket Nos. 09-191, 07-54, at ii (Jan. 14, 2010) (commenting that "the competitive wireless broadband market has responded and continues to respond to consumer demand for open access to content, applications, and services for their choosing"); *see also*, Letter from Stephen Bye, Chief Technology Officer, Sprint

that any resulting privacy rules should reflect a "*balanced* framework that preserves the ability of [BIAS] providers to offer managed services."[4] To this end, Sprint supports the comments of CTIA and other industry stakeholders that advocate for a flexible privacy and security regime under Section 222 that closely aligns with the Federal Trade Commission's ("FTC") well-established framework for unfair and deceptive acts or practices ("UDAP").[5] This approach would continue to best protect consumers and ensure that common ground rules apply consistently and fairly to all players in the Internet ecosystem.

The continued growth and expansion of the online ecosystem depends upon the symbiotic relationship between BIAS providers and edge providers, which operate in concert to facilitate continued innovation and consumer adoption of broadband services. To maintain this essential equilibrium as the Commission asserts its privacy authority over the BIAS half of the ecosystem, Sprint encourages the Commission to continue to carefully study the broadband marketplace and the close interaction between stakeholders, including consumer expectations for harmonized privacy protections. Such a measured evaluation will help yield workable rules that are consistent with consumers' expectations regarding how their data is collected, used, and shared online and will appropriately address genuine privacy risks.

Sprint's comments include recommendations on Commission proposals relating to key defined terms and the application of Section 222, privacy notices, customer consent, data security and breach notification, arbitration, and service offers based on data sharing. These

---

Corporation, to FCC Chairman Thomas Wheeler (Jan. 15, 2015) (*In the Matter of Protecting and Promoting the Open Internet*, GN Docket No. 14-28).

[4] Sprint Reply Comments, 2010 Open Internet Proceedings, Docket Nos. 09-191, 07-54, at 16 (Apr. 26, 2010) (emphasis added).

[5] *See* CTIA *et al.*, Letter to Chairman Tom Wheeler, Mar. 1, 2016, https://www.ncta.com/sites/prod/files/Letter-PrivacyPrinciples-3-1-16.pdf.

recommendations are intended to help ensure that any final rules placing new or additional duties on BIAS providers are offset by countervailing benefits to consumers.

II. DISCUSSION

A. Defining the Scope of Broadband Customer Data Subject to New Rules

The FCC Chairman recently stated that BIAS providers should "be able to use customer information for . . . purposes that are consistent with customer expectations."[6] Sprint agrees with the Chairman's assessment; we are concerned, however, that certain proposed definitions relating to the scope of data to be protected by the Commission's rules (including "customer" and "customer proprietary information") are overbroad and will restrict data collection and sharing in ways that are inconsistent with consumer experience and expectations.

i. "Customer" as the current accountholder

The Commission initially proposes to define a Customer as: "…1) a current or former, paying or non-paying subscriber to broadband Internet access service; and 2) an applicant for broadband Internet access service."[7] We encourage the Commission to limit the definition of "customer" to a current account holder to ensure that any final rules are appropriately tailored to address the privacy concerns that are the focus of this proceeding.

Indeed, the Commission acknowledges the hardships of defining the term "customer" too broadly and proposes to limit notice and consent requirements to interactions with a single accountholder.[8] Sprint agrees with the Commission that this approach strikes the appropriate balance, and should be adopted.

---

[6] Tom Wheeler, *It's Your Data: Empowering Consumers to Protect Online Privacy*, Huffington Post (Mar. 10, 2016), http://www.huffingtonpost.com/tom-wheeler/its-your-data-protect-online-privacy_b_9428484.html.

[7] *Privacy NPRM* ¶ 31.

[8] *See Privacy NPRM* ¶ 35.

Applicants, for example, should be excluded from the customer definition because such individuals neither use the broadband connections that are the subject of the Commission's rules, nor do they provide data implicated by the application of Section 222.[9] Indeed, an applicant that inquires about BIAS service provides a limited amount of personal information that is merely used to qualify the individual for service and does not include any traditional CPNI usage data. Moreover, the NPRM does not indicate why subjecting broadband applicant information to CPNI or similar requirements will advance privacy protections for these individuals. The Commission's proposal speculates that potential customers may be reluctant to apply for broadband service or switch providers absent the protections provided by the proposed rules, yet this suggestion runs counter to the Commission's own data regarding the continued rapid rise in broadband adoption by consumers.[10]

Similar to applicants, former customers should be excluded from the proposed customer definition. Any data associated with the former customer that is eligible for protection under the CPNI rules would have originated during the time of the provider-customer relationship and, therefore, would already be protected based on the provider's ongoing duty. When a customer changes BIAS providers, the original provider (1) still must abide by the privacy representations that it made at the time the data at issue was collected; and (2) is no longer in a position to collect new information about the individual in the context of a provider-customer relationship.

Lastly, the customer definition should be limited to the named account holder, and not expanded to all members of a household or users of the broadband network as suggested in the

[9] *Privacy NPRM* ¶ 13 ("In the 2015 Open Internet Order, we concluded that Section 222 should be applied to the broadband connections consumers use to reach the Internet. . . .").

[10] *See* 2016 Broadband Progress Report at 46 (finding that broadband adoption rates had increased by nearly 40 percent for unserved Americans in only one year).

NPRM.[11] Stretching the definition of customer to include household members or all conceivable users of the network would lead to unworkable obligations for providers. BIAS providers lack insight into household members who may use the network but do not have a direct relationship with the provider, and providers have no reliable means to verify the identity of any such persons or their relationship with the accountholder.

ii. Customer data under Section 222 is limited to CPNI

The proposed rules would define the information to be protected under Section 222 as "Customer Proprietary Information."[12] This broad category of data would encompass both CPNI, as established and defined under Section 222, as well as personally identifiable information ("PII"), a category of data that is not identified in Section 222. The Commission proposes to adopt rules that would protect Customer Proprietary Information, while also conceding that all of the Commission's previous rulemakings addressing Section 222 have been limited to CPNI.[13] Such an expansion is inconsistent with the plain language and structure of Section 222 and, respectfully, the Commission's statutory authority to regulate data privacy and security. Sprint asks the Commission to revisit its proposal.

A plain reading of Section 222 makes clear that the only customer-related "proprietary" information to which Section 222 applies is CPNI. Indeed, the statute is coherent only if it is read to limit customers' "proprietary information" to CPNI. Section 222(a), titled "*In General*," articulates a general requirement that carriers protect the confidentiality of "proprietary information" of customers, as well as of carriers and equipment manufacturers. Section 222(c) then explains how the general requirement under Section 222(a) is actionable with respect to

[11] *See Privacy NPRM* ¶ 34.
[12] *See Privacy NPRM* ¶ 14.
[13] *See Privacy NPRM* ¶ 56.

customers, and it expressly limits the scope of protected customer information to CPNI, as such term is defined in Section 222(h).[14] Section 222's subsequent provisions would not make sense if Section 222(a) imposed a standalone requirement on providers to protect some additional undefined category of customer information beyond CPNI.

For example, if Section 222(a) were read to impose an independent duty on BIAS providers to protect PII and potentially other data, in addition to CPNI, the exceptions enumerated under Section 222(d)[15] would result in an illogical gap regarding when PII use would be permissible. Specifically, Section 222(d) provides exceptions to the general prohibition on the disclosure of CPNI, allowing use of CPNI for billing, to combat fraud, and to assist in emergency response. There is no similar set of exceptions enumerated for the use of PII because the Commission and Congress did not contemplate the statute or rule to cover PII. Both the statute and the rule are limited to CPNI, which includes the protection of personally identifiable usage information related to a user's telecommunications services, including account information.

iii. Treatment of de-identified non-aggregate data

The NPRM suggests that "de-identified, but *non-collective data*" (i.e., non-aggregate data) from customers should be considered "individually identifiable," and therefore subject to greater privacy requirements, even when such non-aggregate data cannot reasonably be re-identified.[16] Sprint encourages the Commission to revisit this suggestion and base any final rules on whether

[14] 47 U.S.C. §222(h)(1).

[15] 47 U.S.C. §222(d)(2) ("Exceptions – Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents—(2) to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services . . . .").

[16] *Privacy NPRM* ¶ 165.

there is a reasonable risk of re-identification such that it impacts a customer's privacy. This should be the test, rather than whether de-identified data is aggregated or not.

This approach is also appropriate because Section 222 does not support a conclusion that all CPNI should be considered individually identifiable unless it is "aggregate." Such an approach would sweep in every non-aggregate data point that every BIAS provider may collect. In addition to not advancing privacy protection of consumers, Sprint believes this would introduce significant operational costs for BIAS providers and result in non-competitive positioning vis-à-vis edge providers.

The Commission's rules and orders consistently identify three categories of information addressed by Section 222: (1) individually identifiable CPNI,[17] (2) aggregate customer information, and (3) subscriber list information.[18] In order for the phrase "individually *identifiable*" to have meaning under Section 222 and the Commission's rules and orders, it cannot simply be a synonym for "non-aggregate."

For example, the Commission includes "traffic statistics" and "service tier" data among illustrative examples of broadband CPNI.[19] The Commission solicits input on how such data should be treated under Section 222 when it is de-identified, but non-collective.[20] Sprint suggests that such data, and all other categories of customer data within the scope of the proposed rules – either standing alone or when combined with anonymized identifiers, should be treated the same as aggregate data when it does not, and cannot, reasonably identify the individuals from whom the data originates.

---

[17] *See, e.g.*, 47 U.S.C. 222(c)(1).

[18] *See, e.g.*, Report & Order & Further Notice of Proposed Rulemaking, 22 FCC Rcd. 6927, n.7 (Apr. 2, 2007) (collecting authorities).

[19] *Privacy NPRM* ¶ 40.

[20] *Privacy NPRM* ¶ 165.

Sprint's suggestion is consistent with the Commission's current and long-standing application of Section 222 rules for data collection and use with respect to voice telephony services. It is also consistent with the FTC's 2012 Privacy Report, which, following extensive stakeholder roundtables and study by the FTC, summarized the FTC's conclusion that the privacy risk from de-identified data is limited to certain circumstances when such data can reasonably be re-identified and linked to an individual.[21] Further, a consistent approach among agencies would help to alleviate potential customer confusion on this issue and would support a balanced framework for businesses that offer services based on data that does not identify individuals and does not impact consumer privacy.

B. Consent Based on Customers' Reasonable Expectations

i. Implied consent for first-party marketing of communications-related and non-communications-related services

The Commission proposes to distinguish between opt-out and opt-in rules based upon the marketing of "communications-related services" versus "non-communications-related services."[22] Under the proposals, BIAS providers would need to obtain *opt-in* consent from customers before using customer data to market "non-communications-related services," and provide *opt-out* consent when using customer data to market "communications-related services."[23] This regime would apply even in the context of first-party marketing where a commercial entity has an ongoing, established business relationship with a customer. As described below, the proposal is counter to recognition by the Obama Administration and other privacy regulators that, in the context of first-party marketing, implied customer choice is appropriate.

---

[21] *2012 FTC Privacy Report* at 21-22.

[22] *See Privacy NPRM* ¶ 18.

[23] *See Privacy NPRM* ¶ 18.

To ensure consistency across the online ecosystem regarding the use of customer information for first-party marketing, the Commission should allow BIAS providers to use customer data to engage in first-party marketing of communications-related services *and* non-communications related services, subject to implied consent by their customers.

ii. A broader view of "communications-related services"

BIAS providers today offer diverse services and features that extend beyond merely broadband access in order to meet consumers' expectations and appetite for new and value-added features.[24] For example, a BIAS provider may offer edge services, including digital content, entertainment, or music services, under its own branding and where no CPNI is shared with any third parties. The NPRM does not indicate why this scenario should require more than implied consent simply because it may involve a non-communications-related service.

Consumers today fully expect, and increasingly *demand*,[25] that the companies with which they share their personal information will use that data to market new and relevant services to them. When CPNI is not shared outside the first-party marketing context, BIAS providers should be allowed to leverage their proprietary assets to offer the diverse services of interest to their customers, and to compete with edge providers that collect and use the same data for first-party marketing purposes without additional customer consent. The White House privacy

[24] *See, e.g.*, Marc Ferranti, Beyond the hype: Internet of Things shows up strong at Mobile World Congress, PCWorld (Feb. 27, 2014), http://www.pcworld.com/article/2102761/the-internet-of-things-beyond-the-hype-at-mobile-world-congress.html (reporting that as the market for connected services grows, "[l]arge carriers will have to work with younger, nimbler companies to bring new services to subscribers"). Further, edge providers are also likely to expand into mobile, so the FCC should adopt rules that do not prejudice broadband providers that offer edge services, while favoring edge services that are building mobile platforms.

[25] Peter Dahlstrom & David Edelman, *The coming era of 'on-demand' marketing*, McKinsey Quarterly (Apr. 2013), http://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/the-coming-era-of-on-demand-marketing (forecasting increase in customer "expect[ations] [that] all data stored about them [will] be targeted precisely to their needs or used to personalize what they experience.").

framework recognizes that first-party marketing is consistent with consumers' reasonable expectations.[26] The White House Privacy Blueprint framework stated the following:

> *"[C]ompanies may infer consent to use personal data to conduct marketing in the context of most first-party relationships, given the familiarity of this activity in digital and in-person commerce, the visibility of this kind of marketing, the presence of an easily identifiable party to contact to provide feedback, and consumers' opportunity to end their relationship with a company if they are dissatisfied with it."*[27]

Similarly, the FTC in its 2012 Privacy Report indicated that companies "do not need to provide choice before collecting and using consumers' data for commonly accepted practices," including first-party marketing.[28] This conclusion mirrors the practices of companies across sectors. Based on its research, the FTC determined that first-party collection and use of non-sensitive data "creates fewer privacy concerns than practices that involve sensitive data or sharing with third parties."[29] Under the FTC framework, first-party marketing to a business' existing customers using data it has collected about those customers is not limited to a particular set of products or services. Further, because consent is implied in this context, such first-party marketing is not considered an unfair or deceptive act or practice when such advertising is done without collecting additional consent from an existing customer. Sprint encourages the Commission to adopt rules that provide the same flexibility to BIAS providers.

The Commission has precedent for adopting a broader definition of "communications-related services" for purposes of Section 222, as its rules for voice services define

---

[26] The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy at 17 (2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("*2012 White House Privacy Blueprint*").

[27] *2012 White House Privacy Blueprint* at 17.

[28] *2012 FTC Privacy Report* at 36.

[29] *2012 FTC Privacy Report* at 15-16.

communications-related services to include "*information services typically provided by telecommunications carriers*."[30] While the Commission has indicated its initial preference to view "information services" narrowly,[31] such an approach would conflict with how consumers today perceive the scope of services available from their BIAS providers, as well as services they will expect in the future.

iii. Revisiting the total services approach

Additionally, Sprint recommends that the Commission align the current voice CPNI rules under Section 222 with Sprint's comments above as part of this proceeding. Such an update to the existing rules will allow voice providers to market to consumers in a manner that reflects the evolution of the voice services market and that is consistent with the expectations of consumers of voice services.

Under the existing CPNI rules, the "total service approach" allows carriers "to use a customer's entire record, derived from complete service subscribed to from that carrier, to market improved services within the parameters of the existing customer-carrier relationship" and "permits carriers to use CPNI to market offerings related to the customer's existing service to which the customer presently subscribes."[32] Voice providers' services include more than voice connectivity, similar to the description above of BIAS providers' expanding scope of services. Sprint, therefore, asks the Commission to clarify that expanded offerings, including carrier-specific third-party offerings in which CPNI is not shared with a third-party, are within

---

[30] *See* 47 C.F.R. 64.2003(e) (emphasis added); *Privacy NPRM* ¶ 72.

[31] *Privacy NPRM* ¶ 72.

[32] *In the matter of Implementation of Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115 (rel. Aug. 16, 1998) at ¶ 16 (emphasis added).

the parameters of the existing customer-carrier relationship and do not require additional notice or consent under the total service approach.

C. Meaningful Notice to Customers Regarding Privacy Practices

i. General notices

The Commission proposes prescriptive privacy notice disclosure requirements, some of which would require substantial investment and resources by BIAS providers without producing corresponding benefits for consumers. Sprint urges the Commission to give BIAS providers the flexibility to design and choose the most effective privacy notice approach to educate customers within the user experience.

For example, the Commission proposes that notice of privacy practices be provided at the point-of-sale and prior to the purchase of BIAS.[33] Sprint agrees that customers should understand their providers' data collection and use practices at the outset of the provider-customer relationship. It may be most effective to provide privacy notices as part of the user experience with a new device or when establishing an online account. Within those contexts, a user privacy notice may be most relevant to a consumer.

In the alternative, however, the Commission should confirm that BIAS providers can provide a point-of-sale privacy notice as part of the customer agreement, rather than as a standalone document. Customers receive a significant amount of information at the point-of-sale. There is concern that increased disclosure becomes counterproductive at some point.[34] The FTC has commented on this risk of over-disclosure in the broadband context:

---

[33] *Privacy NPRM* ¶ 87, Appendix A, Subpart GG – Privacy of BIAS Customer Information §64.7001(b)(1).

[34] Jason Ross Penzer, *Grading the Report Card: Lessons from Cognitive Psychology, Marketing & the Law of Information Disclosure for Quality Assessment in Health Care Reform*, 12 Yale J. on Reg. 207, 232 (1995) (an increase in disclosure "becomes too complex for consumers to assimilate within a reasonable search time, too expensive for providers, and too extensive to

> *If consumers either do not read disclosures or do not understand them, the purpose of the disclosures is frustrated. The challenge of disclosures in the broadband access area, therefore, is to make such disclosures in a way that will enable consumers to understand both the services at issue and the ISPs' descriptions of how those services are provided.*[35]

The final rules therefore should give BIAS providers flexibility as to the type of notice to provide customers, so long as the notices are "comprehensible and not misleading," "clearly legible," and "readily apparent."[36] Such an approach strikes the right balance because it would result in notices that are more meaningful in the decision-making process for customers.

ii. Dashboards have low consumer uptake

The Commission also seeks comment on whether to require BIAS providers to make available comprehensive "consumer-facing privacy dashboards."[37] Sprint strongly encourages the Commission to forego any privacy dashboard requirement. As a requirement, such an approach largely would be redundant with information included in the privacy notices proposed by the Commission. The record shows that dashboards are unlikely to be used by more than a small fraction of a provider's customers. Consumers have been conditioned over time to seek out publicly-available privacy policies and notices to obtain relevant privacy information, rather than logging onto dashboards.[38] Indeed, the Commission acknowledges that consumer adoption

---

regulate effectively."); Jean Braucher, *Form and Substance in Consumer Financial Protection,* 7 Brook. J. Corp. Fin. & Com. L. 107, 124 (2012) ("[R]egulation by disclosure often fails to work for an array of reasons. Complexity and variety prevent transparency.").

[35] FTC Broadband Connectivity Report, at 133 (June 27, 2007).

[36] *See Privacy NPRM* ¶ 83.

[37] *See Privacy NPRM* ¶ 95.

[38] Aleecia McDonald & Lorrie Cranor, *The Cost of Reading Privacy Policies*, 4 Information Society 543, 544, 564 (2008) (detailing different privacy policy formats designed to "help Internet users gain the tools they need to protect themselves online").

of privacy dashboards has been limited.[39] Given the likelihood of low consumer adoption, and the significant overlap between information in the privacy notices and the proposed dashboard, BIAS providers should not be required to commit the substantial financial and developmental resources necessary to deploy and maintain dashboards that, in reality, would provide a de minimis consumer benefit.

D. Avoiding Over-Notification on Data Breaches

Similar to the proposed expansion of the privacy notice requirements, as described above, the Commission proposes to impose data breach notification requirements that go far beyond the notice obligations in the current voice CPNI rules, as well as the requirements of nearly all 47 states with breach notification laws. Under the proposals, "breach" would encompass the broad CPNI and PII categories and would not include the limiting element of intent that exists in the current CPNI rules.[40] Coupled with this expanded breach definition, the proposals would require providers to notify both the Commission and customers of all breaches, in addition to providing notice to law enforcement for breaches impacting more than 5,000 customers. Thus, under the proposals, any inadvertent unauthorized disclosure of data, regardless of size or the type of data involved, would be considered a breach subject to reporting requirements.

Sprint recognizes and supports the need to provide timely notice following certain data breach events. Any notice requirements, however, must be fine-tuned to ensure that customers, law enforcement, and other stakeholders, receive appropriate and accurate notice calibrated

[39] *See Privacy NPRM* ¶ 95 n.168. The NPRM suggests that low adoption may be due to lack of visibility; however, the White House Big Data Report cited by the Commission also points to notice fatigue, among other factors, for consumers' reticence in using privacy dashboards. *See*, Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values at 42 (May 2014).

[40] *See Privacy NPRM* ¶¶ 75-77.

based on the scope of the breach, including the reasonable risk of harm and the sensitivity of the data at issue, as well as the notice content and timing.

i. Scope of the breach

The Commission's proposed rules on breach notification generally do not limit instances where notice would be required, except that the Commission would not require notice to law enforcement unless a breach is reasonably believed to have compromised the customer proprietary information of more than 5,000 customers.[41] Sprint supports a qualifier based on the potential number of affected customers, such as the one described above, because it better ensures that law enforcement gives attention to notices of significance that they receive from BIAS providers. Sprint encourages the Commission to consider additional ways to bolster the effectiveness of the proposed rules through qualifiers such as the potential size of the breach, the elements of intent and/or harm, and the sensitivity of the data at issue, or some combination of these qualifiers.

Sprint believes that notifying the Commission of *all* breaches would be counterproductive to the Commission's intent to remain aware of issues in the telecommunications industry.[42] For example, an inadvertent unauthorized disclosure involving one, a small handful, or even dozens of customers is unlikely to cast light on a new area of concern that would require the Commission's input or attention. Yet these are precisely the types of events that constitute the majority of "breaches" involving BIAS providers, and, as a result, would take up the majority of the Commission's resources dedicated to notice activity, in addition to unduly taxing providers' resources. To ensure that the Commission can focus its

[41] *See Privacy NPRM*, Appendix A, Subpart GG – Privacy of BIAS Customer Information §64.7006(c).

[42] *Privacy NPRM* ¶ 248.

resources on the types of breaches that merit its attention, we suggest that the rules for notifying the Commission of a data breach mirror those for notifying law enforcement.

With respect to potential qualifiers that could be applied to determine when notice to customers is appropriate, Sprint believes that customers would be best served by notice when there is a risk of harm (including whether the breach involved the disclosure of sensitive data) or misuse. The NPRM acknowledges that certain states do not require companies to notify consumers if they determine that no harm resulted from the breach.[43] Indeed, *most* of the 47 states with data breach notification laws include some type of notification qualifier based on the reasonable likelihood of harm or misuse of the compromised data. A similar qualifier should apply to the consumer notice requirements under the proposed rules. Such an approach will help alleviate concerns relating to notice fatigue and will increase the likelihood that customers who receive a notice will read it, and take appropriate action.

ii. Notice content and timing

With respect to breach notice content and timing, the Commission proposes to deviate from the existing voice CPNI rules under Section 222 by requiring providers to notify consumers within ten days of discovery of a breach (the existing voice CPNI rules do not specify timing for customer notice), and by mandating specific content to be included in the notice (the existing CPNI rules do not prescribe notice content elements). Sprint encourages the Commission to revisit the proposed notice content and timing requirements, and harmonize the requirements with the existing voice CPNI rules to help ensure that the notice that providers send to customers is accurate and meaningful.

---

[43] *See Privacy NPRM* ¶ 237 (citing Alaska Stat. § 45.48.010(c); Arizona Stat. § 44-7501(G); Conn. Gen. Stat. § 36a-701b(b)(1)), and that other states only require notification if there is a likelihood of misuse of the data or harm to the consumer, see NPRM at ¶ 237 (citing Vt. Stat. Ann. Tit. 09 § 2435(d)(1); Md. Com. Law Code Ann. § 14-3504(c)).

Immediately following a breach event, providers focus on preventing further unauthorized access to information and gathering facts as to the origin and scope of the breach. This fact gathering phase reasonably can extend beyond ten days. Under the current CPNI rules, telecommunications service providers have some level of flexibility to delay notice to customers until the pertinent details of the breach have been verified and can be accurately conveyed to customers. In contrast, under the proposed rules for broadband, the combination of the proposed timing and content requirements would increase the chance that providers include incomplete or inaccurate information that might require a subsequent corrective notice that leads to customer confusion. For this reason, Sprint recommends that the Commission adopt the customer notice provisions under the existing voice CPNI rules as the customer notice requirements for broadband.

Lastly, the Commission should use this rulemaking as an opportunity to update the current voice CPNI rules in certain key respects. Specifically, the current CPNI rules under Section 222 require voice telecommunications providers to notify law enforcement of a breach through the central reporting facility established by the Commission.[44] Anecdotal feedback provided by law enforcement to Sprint suggests that most information that carriers provide to law enforcement has no value because it largely relates to small-scale breaches that pose little to no harm to consumers. To help ensure that the information BIAS providers send to law enforcement is valuable and justifies the expenditure of law enforcement resources to process and review, we recommend that the Commission revisit the law enforcement notice requirements in the current CPNI rules and allow providers to limit data breach notice to law enforcement only

[44] *See* 47 CFR 64.2011(a).

where there is a reasonable risk of consumer harm in connection with substantiated data breaches.

E. Enhanced Flexibility to Ensure Robust Data Security

As part of the Commission's proposed data security requirements, the Commission would require BIAS providers to establish and perform regular risk management assessments.[45] The intent of such assessments would be to ensure that providers continue to satisfy the general proposal that providers protect the security, confidentiality, and integrity of customer data that they receive from customers.[46] Sprint recognizes and agrees with the proposed general requirement to protect customer data, including through certain measures found in the existing voice CPNI rules (*e.g.*, employee training). The proposed risk management assessments, however, impose a new prescriptive obligation beyond the existing CPNI rules that is unnecessary given that providers would already be obligated to continuously protect customer data pursuant to the Commission's general requirement. BIAS providers already have security practices and the Commission has not demonstrated an existing need to substitute or add features that will result in expensive operational costs.

Further, the Commission models its risk management assessment proposal on existing requirements under the Gramm Leach Bliley Act and the Health Insurance Portability and Accountability Act, which govern the collection and sharing of *sensitive* consumer financial and health-related information.[47] Under the Commission's proposals, however, the vast majority of data that would be the subject of the required risk management assessments would be non-

---

[45] *Privacy NPRM*, Appendix A, Subpart GG – Privacy of BIAS Customer Information §64.7005(a)(1).

[46] *Privacy NPRM* ¶ 170.

[47] See Pub. L. No. 104-191, 110 Stat. 1936 (1996) (Health Insurance Portability and Accountability Act of 1996 or "HIPAA"); 15 U.S.C. § 6801-6809 (Gramm-Leach-Bliley Act or "GLBA").

sensitive customer data. The record does not support imposing burdensome risk management obligations on BIAS providers that currently do not exist under Section 222, and that are traditionally targeted solely at the collection and use of sensitive personal information.

As an alternative approach, Sprint suggests that the Commission remove the risk management assessment requirement from the proposed rules. Removing this requirement will afford providers greater flexibility to determine the most effective approach to comply with the overarching requirement to protect the security, confidentiality, and integrity of customer data based on the nature and scope of the BIAS providers activities, the sensitivity of the underlying data, and technical feasibility.[48] Moreover, to the extent that BIAS providers handle sensitive data, such as financial data or protected health information, the providers would remain subject to the data security requirements under the existing relevant statutes.[49] Congress tailored privacy and data security in specialized statutes to the sensitivity and use of data and potential harm to consumers by misuse or disclosure.

F. Upholding Customer Choice

In his recent Senate testimony, Chairman Wheeler described the current proceeding as "narrowly focused on personal information collected by broadband providers as a function of providing [consumers] with broadband connectivity."[50] Sprint agrees with the Chairman as to the necessary aim of this proceeding to the extent that it focuses on CPNI; however, we are concerned that certain proposals in the rulemaking exceed the scope of authority granted under Section 222. For example, the proposals would prohibit BIAS providers from offering

[48] *See Privacy NPRM* ¶ 170.

[49] *See* HIPAA, GLBA, and 15 U.S.C. 6501–6505, Children's Online Privacy Protection Act of 1998 ("COPPA").

[50] Prepared Testimony of Chairman Tom Wheeler, *Examining the Proposed FCC Privacy Rules*, Before the Senate Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law, at 2 (May 11, 2016) ("*Chairman's 2016 Privacy Testimony*").

customers an expanded range of services (including lower price and free service options) based on the customer's informed choice in allowing the provider to collect and use more customer data. The Commission also proposes to bar private parties from compelling arbitration as a forum to resolve disputes, even though such provisions in commercial contracts afford consumers a low cost and efficient means of issue resolution.

We encourage the Commission to resist the temptation to use this proceeding as a means to accomplish broader policy objectives and decline to give these proposals further consideration as part of this proceeding.

i. Retaining lower cost / free service plan options based on data sharing

The Commission has made clear that customer choice regarding how data will be used and shared is a core element of the current proceeding.[51] Sprint agrees with the Commission's position that customers should be empowered to make informed decisions regarding how their data will be collected and used. For this reason, the Commission should not enact rules barring BIAS providers from offering customers the ability to choose among tiered-pricing or free services based on a willingness to share data with the provider, so long as the customer receives the information necessary to make an informed decision.

The Commission acknowledges that such tiered-pricing options are commonplace in the online ecosystem, and include instances where BIAS providers offer customers discounted or free services, such as Wi-Fi, in exchange for using data collected by that service "to tailor ads and offers to customers' interests."[52] BIAS providers and customers should not be prohibited

[51] *See Chairman's 2016 Privacy Testimony*, at 2 ("This proposal is built on three core principles--transparency, choice, and security.").

[52] *Privacy NPRM* ¶ 259; *see also* See Maureen Morrison, AT&T Tries Injecting Extra Online Advertising Via Free Wi-Fi Hotspots, AdAge.com (Aug. 27, 2015), http://adage.com/article/digital/att-injects-ads-free-wi-fi-hotspots/300120/ (reporting on the

from agreeing to similar exchanges based on the customer's informed consent. Indeed, evidence increasingly shows that consumers willingly disclose such information in order to obtain a variety of benefits, including personalization,[53] free services, and useful advertisements.[54]

ii. Arbitration as an efficient form of dispute resolution for consumers

The Commission solicits input on whether to prohibit BIAS providers from including mandatory arbitration clauses in their contracts with customers.[55] The suggestion that such a prohibition may be appropriate under this proceeding is rooted in the Commission's view that consumers are disadvantaged by the arbitration process.[56] Sprint recommends that the Commission decline to adopt a prohibition on mandatory arbitration clauses as part of this proceeding in light of the Federal Arbitration Act (FAA) and legal precedent relating to wireless carriers' use of such provisions.

Under the FAA, arbitration provisions included in contracts are "valid, irrevocable, and enforceable, save upon grounds as exist at law or in equity for the revocation of any contract."[57] The FAA's mandate applies unless it is shown that Congress intended to override the FAA in

---

offering of free Wi-Fi by AT&T, Comcast and hotels). See also, Louis Bedigian, Why Is Google Giving Starbucks Customers Free Wi-Fi?, Benzinga.com (Aug. 1, 2013), http://www.benzinga.com/news/13/08/3805982/why-is-google-giving-starbucks-customers-free-wi-fi (noting the branding and data collection rewards of providing free Internet access at Starbucks compensates for the investment in Wi-Fi that is "likely to cost Google or Starbucks a lot of money up front"); Spotify.com/us/premium (last accessed May 14, 2016) (noting that for $9.99 per month, Premium users can listen to Spotify with "[n]o ads, [j]ust uninterrupted music").

[53] Heng Xu, *et al.*, *The Role of Push-Pull Technology in Privacy Calculus*, 26 J. Mgmt. Info. Sys. 135, 142 (2009) (noting "the value of personalization with the emphasis on individualized functionalities that add to the user experiences and smoothness of interactions").

[54] Sy Banerjee & Ruby Roy Dholakia, *Mobile Advertising: Does Location Based Advertising Work?*, 3 Int'l J. of Mobile Marketing 68, 72-73 (2008).

[55] *Privacy NPRM* ¶ 274.

[56] *See* 2015 Open Internet Order, 30 FCC Rcd at 5718, ¶ 267.

[57] 9 U.S.C. § 2.

another federal statute.[58] The applicable federal statute for this proceeding – the Act – does not override the FAA because it does not contain any reference to arbitration provisions in agreements for telecommunications services.[59]

Further, with respect to mobile telecommunications services providers, the Supreme Court held in *AT&T Mobility v. Vincent Concepcion* that wireless carriers can include mandatory arbitration provisions in subscriber agreements, subject to certain consumer protections.[60] Indeed, the Court noted that an arbitration system that includes features that encourage the pursuit of small claims and shifts costs to the defendant when the consumer is successful places consumers in a better position than as members of a class action that "could take months, if not years, and . . . may merely yield an opportunity to submit a claim for recovery of a small percentage of a few dollars."[61]

At bottom, arbitration affords individual consumers legitimate opportunities to assert their rights and pursue their disputes. Further, the question as to the legality of mandatory arbitration provisions within agreements between BIAS providers and their customers is well-settled. We encourage the Commission to avoid adding measures to any final rules that would limit consumers' access to this valuable form of dispute resolution.

---

[58] *See Shearson/Am. Express, Inc. v. McMahon*, 482 U.S. 220, 227 (1987) (Congressional intent to override the FAA in another federal statute must be shown through a "contrary congressional command" that is "discernible from the text, history, or purposes of the statute.").

[59] The Consumer Financial Protection Bureau ("CFPB") recently proposed rules that would limit the use of pre-dispute arbitration agreements by financial service companies. *See Arbitration Agreements*, Proposed Rule With Request for Public Comment, CFPB, Docket No. CFPB 2016 0020 (rel. May 3, 2016). The Dodd-Frank Act expressly authorized the CFPB to study the effects of arbitration and issue regulations restricting or prohibiting the use of arbitration agreements if the CFPB found that such rules would protect consumers. *Id*. at 3. In contrast, the Communications Act does not include a comparable provision giving the Commission authority to restrict or prohibit the use of arbitration agreements.

[60] 563 U.S. 333 (2011).

[61] *Id*. at 352.

III. CONCLUSION

Sprint supports the Commission's effort to fulfill its mandate under the Open Internet Order by proposing privacy rules that focus on choice, transparency, and data protection for BIAS customers. As described above, Sprint believes that the most effective approach to achieving the Commission's objectives is a set of flexible rules for BIAS providers that are consistent with the privacy framework that applies to all other players in the Internet ecosystem. Such an approach would give certainty to consumers by ensuring consistent treatment and protection of data no matter the online entity with whom the consumer interacts. This approach also would account for the symbiotic relationship between BIAS providers and edge providers, website developers, and others, and the positive impact of this relationship on continued growth and adoption of broadband. We encourage the Commission to continue taking a thoughtful approach to this rulemaking so that the final outcome is a series of measured rules that accomplish the Commission's privacy objectives within the Commission's authority under Section 222.

Respectfully submitted,

/s/ Marc S. Martin
Marc S. Martin
John Roche
James F. Ianelli
Perkins Coie, LLP
700 13th St. N.W., Suite 600
Washington, D.C. 20005-3960
(202) 654-620

Counsel to Sprint Corporation

Sprint Corporation

Maureen Cooney
Head of Privacy, Office of Privacy

Government Affairs

Matthew Sullivan
Counsel, Office of Privacy
Government Affairs

12502 Sunrise Valley Drive
Reston, VA 20196
703-592-7580; 571-287-8341

May 27, 2016