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

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

COMMENTS OF NTCA–THE RURAL BROADBAND ASSOCIATION

NTCA-The Rural Broadband Association
4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203
703/351-2000

May 27, 2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY i

I. INTRODUCTION 1

II. DISCUSSION 11

A. DEFINITIONS OF KEY TERMS 11

1. Broadband Provider 11

2. Affiliate 12

3. Definition of Customer and Other Users 13

(a) Applicants and Former Customers 13

(b) Protections for Multiple Users 17

(c) Consistency in the Rules 19

4. Defining CPNI in the Broadband Context 19

(a) Elements of Service 19

(b) MAC and IP Addresses and Applications 21

(c) Customer Premises Equipment 23

5. Proposals to Create New Categories of Purportedly Protected Information 26

6. Content of Customer Communications 30

B. APPROVALS FOR USE OF INFORMATION 30

1. Communications-Related Services and Related Terms 30

2. Breaches 32

3. Proposals to Establish Broader Obligations 35

C. PRIVACY POLICIES 35

1. Privacy Notice Requirements 35

2. Timing and Placement of Privacy Notice Requirements 40

3. Burdens on Providers 41

4. Providing Notice of Material Changes in Privacy Policies 42

D. CUSTOMER APPROVAL PROCEDURES 43

1. Harmonizing Notices for Voice, Video, and Broadband Services . . 43

2. Customer Approval Requirements for the Use and Disclosure of Customer Proprietary Information 44

3. Permissible Uses and Disclosures of Customer Proprietary Information for Which Customer Approval Is Implied or Unnecessary 45

4. Emergency Services 46

5. Marketing Communications-Related Services 47

6. Other Purposes 48

7. Soliciting Customer Approval 52

8. Documenting Compliance 55

9. Use and Disclosure of Aggregate Customer Proprietary Information 56

E. SECURING CUSTOMER PROPRIETARY INFORMATION 58

1. Industry-Developed Practices, Rather than Prescriptive Mandates, are Best Suited to Securing Networks and Information 58

2. Customer Access to Customer Proprietary Information 64

3. Accountability for Third Parties 65

4. Destruction of Customer Proprietary Information 66

F. DATA BREACH NOTIFICATION REQUIREMENTS 67

1. Customer Notification 67

2. Notification to Federal Law Enforcement and the Commission . . . 69

3. Third-Party Data Breach Notification 70

G. PRIVACY REQUIREMENTS AND CUSTOMER RELATIONSHIPS . . . 71

III. CONCLUSION 72

EXECUTIVE SUMMARY

NTCA–The Rural Broadband Association responds herein to the Commission's *Notice of Proposed Rulemaking* examining the promulgation of rules to address the privacy of broadband Internet access service customers' information. As small rural network operators committed to the communities in which they live and serve, NTCA members are committed to protecting their customers' data. This includes maintaining secure networks and protocols that protect user information consistent with fair and reasonable market expectations and practices. NTCA, however, observes that many content owners and other 'edge providers' have as much or even greater access, ability, and incentive to maintain and utilize consumer data. Consumer information that warrants protection should be subject to a standard of care that is consistent across all fields of those who might control it, and no one class of industry should be subject to greater obligations when the same data is considered.

In these comments, NTCA urges the Commission to hew to the statute and address any new Section 222-sourced rules to those data sets that arise uniquely out of broadband Internet access service. Other data sets should be managed in a manner consistent with the standards to which other actors in the broadband field, as well as other providers of goods and services, generally, are bound. The language of the statute contemplates narrow, specific sets of data that are considered customer proprietary network information (CPNI). Ultimately the task of identifying, promulgating, and implementing rules would be more effective if only information that is specific to broadband Internet access service were to be applied within the CPNI

framework. This "uniquely telecom" approach would also create a uniform set of expectations and industry practices for the balance of information that is implicated by broadband activity.

Accordingly, the Commission should reject proposals to create new sets of so-called "customer proprietary information" that are not contemplated by the relevant statute. Follow-on proposals that are premised upon such innovations should similarly be rejected.

In addressing provider interactions with customers, the Commission's attention is directed to Federal Trade Commission policies that govern edge and application providers, and is urged to ensure a consistent standard of care across the broadband marketplace. Toward that end, consumers and providers will benefit from a uniform approach to privacy matters. Proposals to create regulations that apply to only one segment of the industry should be rejected.

Regarding network security practices, the industry has undertaken collaborative efforts to identify and create best practices. These incorporate a cooperative recognition of technological and market conditions and contemplate a dynamic and evolutionary response to changing needs. Burdensome and prescriptive requirements will not enhance customer protection, and at worst could impose inefficient measures that would consume resources and attention which would better directed toward effective industry practices.

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

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

COMMENTS OF NTCA–THE RURAL BROADBAND ASSOCIATION

I. INTRODUCTION

NTCA–The Rural Broadband Association (NTCA)[1] hereby submits these comments in response to the *Notice of Proposed Rulemaking*[2] issued in the above-captioned proceeding. As small, community-based providers that live among and work alongside their subscribers, NTCA members are committed to protecting the private information of their customers in a manner consistent with industry practices. As a general matter, however, NTCA members do not broker their customers' information, and even prior to reclassification of broadband Internet access service (BIAS) as a telecommunications service[3] generally accorded their BIAS customers the same treatment as their voice customers whose accounts are governed by

[1] NTCA is an industry association composed of nearly 900 rural local exchange carriers ("RLECs"). While these entities were traditional rate-of-return-regulated telecommunications companies and "rural telephone companies" as defined in the Communications Act of 1934, as amended, all of NTCA's members today provide a mix of advanced telecommunications and broadband services, and many also provide video or wireless services to the rural communities they serve.

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

[3] *See, generally, Protecting and Promoting the Open Internet: Report and Order on Remand, Declaratory Ruling, and Order*, Docket No. 14-28, FCC 15-24 (2015).

customer proprietary network information (CPNI) rules.[4] Indeed, to the extent that the same standards and processes could be used to govern customer relationships for CPNI arising out of both services, this would (and has) represented an efficient and effective way for small carriers to operate. Indeed, this could have been the model to which the Commission might have logically looked in deciding how to incorporate BIAS services into CPNI protections in a simple and straightforward way. Unfortunately, the NPRM evidences a different conclusion. Rather than looking to determine how best to include BIAS-related data that comport squarely with the statutory definitions of CPNI into existing processes that are already working to protect other telecommunications data, the Commission has instead launched a sweeping and far-reaching inquiry regarding how to remake the CPNI rules and processes as a whole, threatening new burdens and creating legal question marks of all kinds where none were needed.

Following the reclassification of BIAS as a telecommunications service, the Commission engaged conversation with the industry to determine the form of rules based upon Section 222 of the Communications Act, as amended,[5] rules to BIAS. NTCA identified the hallmarks of "notice, choice and security" in these regards.[6] These touchstones should serve as guiding principles in the development of strong, technology-flexible, self-regulating standards that will be best suited to keep pace with the dynamic field. Several guidelines, however, must attend the Commission's work in this regard. As an overarching concern, the instant proceeding should not be conducted

[4] 47 C.F.R. § 64.2001, *et seq.*

[5] 47 U.S.C. § 222.

[6] Statement of Joshua Seidemann, NTCA Vice President of Policy, FCC Public Workshop on Broadband Consumer Policy (Apr. 28, 2015) (*see,* "FCC Staff Announce Agenda for Public Workshop on Broadband Consumer Policy," FCC News (Apr. 22, 2015) (https://apps.fcc.gov/edocs_public/attachmatch/DOC-333155A1.pdf) (last viewed May 10, 2016, 13:44)).

as an exercise to overhaul the existing CPNI process or regime. Therefore, and as explained further in these comments, the Commission should refrain from increasing the scope of current CPNI rules, even where such action might be advocated in the spirit of conforming telephone rules to BIAS standards. Revisions to CPNI rules should reflect *only* those "customer proprietary network information" data that are unique to BIAS. In this vein, the Commission should also reject proposals to adopt unprecedented, wholesale introduction or expansions of categories of protected information, particularly where the same data are in the possession of and available from a variety of other sources not subject to such requirements. As described below, proposals to exert Commission jurisdiction over data protected by current Federal Trade Commission (FTC) or other existing Federal or local guidelines should be rejected.

And, yet, in the instant NPRM, the Commission has taken staggering and unprecedented steps toward a regime that expands regulations beyond the scope of the statute to potentially create unsettling disparities in the way various actors, all with access to the same data, might be regulated differently. These proposals risk creating new burdens that offer little, if any, incremental protection for consumers. Regulatory disparity that arises incidentally is regrettable; disparity by design is to be eschewed. As Chairman Wheeler stated before the House Subcommittee on Communications and Technology, consumers deserve "a uniform expectation of privacy."[7] Certain of the Commission's proposals, however, presage the potential to inject both confusion and unnecessary burdens upon the marketplace, particularly where the proposed

[7] Hearing before the U.S. House of Representatives Subcommittee on Communications and Technology, "Oversight of the Federal Communications Commission," Preliminary Transcript at 141 (Nov. 17, 2015). Chairman Wheeler explained the Commission "will not be regulating the edge providers differently" from Internet service providers (ISPs).

rules stray from well-established processes to protect customer data and from existing standards that reflect market expectations and consumer demand.

To the extent the Commission endeavors to extend Section 222 obligations to BIAS, current Commission guidelines, as articulated in the CPNI rules, provide a rational basis for formulating a statutory-grounded approach to protecting CPNI-type data that arises specifically out of BIAS. The Commission recognized this implicitly when it declined to forbear from enforcing those requirements after the reclassification of BIAS as a telecommunications service.[8] Many actors beyond network operators, however, play a role upon the broadband stage, and consistent with goals of maintaining clarity for consumers and parity in the marketplace, Section 222 should be viewed a resource to address data that is narrowly analogous to CPNI, rather than all information that might pass between parties in a BIAS provider/customer relationship. Types of data that are common to edge, application, and BIAS providers should remain subject to a uniform structure girded with standards established by Section 5 of the Federal Trade Commission Act.[9] The Commission should avoid actions that precipitate regulatory disparity among multiple parties who all have access to the same customer information. At best, an expansion of Section 222 regulations would roughly duplicate FTC guidelines that address unfair or deceptive trade practices; at worst, disparate treatment will impose an unwarranted thumb upon the market's scales, codifying confusing and conflicting consumer-facing standards. The NPRM ostensibly seeks to barricade the BIAS front door with reporting requirements,[10]

[8] *See, Protecting and Promoting the Open Internet: Report and Order on Remand, Declaratory Ruling, and Order,* Docket No. 14-28, FCC 15-24, para. 461, *et seq* (2015).

[9] 15 U.S.C. § 45.

[10] *See, e.g.,* NPRM at para. 233, *et seq.*

contractual mandates,[11] an expansive realm of protected information,[12] and harbingers of strict liability[13] whilst the back door for edge and app providers is secured sufficiently with a deadbolt backed by the FTC. And, setting aside the uneven impact on providers, will consumers understand and be better able to manage their own data needs given these critical differences in levels of protection?

FTC guidelines of fair trade practices provide a substantial, relevant analytical construct. As the NPRM bears out, privacy law in the United States could be discerned as a patchwork of different regulations that address different industries. For example, HIPPA covers health care data,[14] while other regulations address children's online privacy protection.[15] Generally, however, consumer data is governed by comprehensive principles that address the *type* of information rather than the *holder* of the information. On-line retailers process substantially the same information as their brick and mortar counterparts, which may be include information that is identical to that obtained by app providers or social media sites. Consistent protections formed on the basis of the data should apply to all who hold characteristically similar information. Websites such as Facebook, Amazon, and others gather information about user habits and preferences, but there is no formal body of "Internet law" whose specific regulations address those practices. Rather, an evolving body of case law applies proven principles to the industry as

[11] *See, e.g.,* NPRM at paras. 154, 160-162, 211.

[12] *See, i.e.,* NPRM at paras. 57-66.

[13] *See,* NPRM at para. 75.

[14] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936, *codified at* 42 U.S.C. § 300(gg), 29 U.S.C. § 1181 *et seq. and* 42 U.S.C. 1320(d) *et seq.*

[15] Children's Online Privacy Protection Act of 1998, Pub. L. 105-277, 112 Stat. 2681, *codified at* 15 U.S.C. § 6501, *et seq.*

it evolves to meet changing consumer perceptions, technology and market demands. This approach is sensible and creates a level playing field for all actors on the broadband stage. NTCA does not advocate any level of disregard for privacy; instead, NTCA advocates a *consistent regard* for privacy that addresses all players in the market regardless of whether they fall beneath the jurisdiction of the Commission.

The FTC is empowered to initiate actions for a company's breach of promise of how it will protect a customer's information, regardless of industry or vertical sector. And, the FTC can act against deceptive or unfair acts or practices. The primary source for FTC authority is Section 5 of the FTC Act, which prohibits "unfair or deceptive or practices in or affecting commerce." "Unfair or deceptive" is a material representation, omission, or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment. "Practice" is an action that (a) causes or is likely to cause substantial injury to the consumer which is not (b) reasonably avoided by the consumer or (c) outweighed by countervailing benefits to the consumer or competition.[16] These may be violated by: retroactive policy changes; deceitful data collection; improper use of data; unfair design; and, unfair information security practices. In the vein of "notice, choice and security," the FTC umbrella can cover obligations of providers to maintain confidentiality; to collect data only in a manner consistent with stated policies; and, to

[16] *See*, 15 U.S.C. §45(n). This standard is also incorporated in the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111-203, 124 Stat. 1376, *codified at* 12 U.S.C. § 5511 (2011). This three-prong approach was first articulated in the FTC's "Policy Statement on Unfairness," and later incorporated into the FTC Act. *See*, https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (last viewed May 26, 2016, 12:27).

protect that data.[17] These standards provide sufficient standards against which edge, app and BIAS providers can be held.

Within the principles of Section 5, industry has favored consumer choice and best practices, a form of self-regulation based upon "notice and choice." The Clinton Administration created the Information Infrastructure Task Force, which in 1995 and 1997 recommended self-regulation. Under self-regulation, firms determine the standards and self-articulated rules for data collection, use and disclosure. By way of example, in the late-1900s TRUSTe symbolized voluntary standards, issuing a seal to websites that agreed to abide by certain practices. And, even as the FTC remains a potent backstop to discourage companies from engaging in "unfair or deceptive" practice, the industry pursues practices that are consistent with consumer demands. As noted by Google as it elucidated a backdrop of Federal and state backstops in support of their sufficiency in a similar context, "Privacy policies are now commonly posted on websites, and businesses compete to provider better privacy protections than their peers."[18]

The Commission has recognized the FTC's significant role. Referring to "a consumer protection Memorandum of Understanding (MOU)," the Commission explained that it and the FTC each "recognizes the others' expertise" and each agreed to "coordinate and consult on areas of mutual interest."[19] Likewise, the Commission's apparent disposition to address consumer

[17] *See, FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015) (failure to use readily available technology such as firewalls; storage of information in plain text; failure to implement adequate policies; failure to remedy known vulnerabilities; failure to use adequate protocols and passwords; failure to restrict access to network; and failure to follow incident response procedures, taken together, constitute unreasonable behavior).

[18] *Expanding Consumers' Video Navigation Choices; Commercial Availability of Navigation Devices: Comments of Google, Inc.*, Docket Nos. 16-42, 97-80, at 7 (internal citation omitted).

[19] NPRM at para. 8.

privacy issues in the telecommunications space is not disputed. NTCA submits, however, that with a broad roster of broadband players, a uniform set of standards creates a level playing field and rational set of consumer expectations. In contrast, certain of the Commission's proposals would account some in the online marketplace to Commission-established standards while others who are not within the regulatory purview of the Commission (and yet have access to the same information) would be subject to FTC oversight, instead. This result does not establish "parallel and equivalent" regulatory regimes (however inefficient that may be), but rather would propose to implement explicit, prescriptive regulation on one sector while another is enabled to use the same data to respond quickly to industry needs and best practices that meet current consumer demands. It is also important to consider that from the consumer's perspective, a consistent form of regulation for data, regardless of which party has access to it, will enable consumers to act with careful consistency in their management of information.

The Commission quotes the FTC recognition that ISPs are "in a position to develop highly detailed and comprehensive profiles of their customers – and to do so in a manner that may be completely invisible."[20] And, yet, that same affirmation may be made in regard to others in the arena. By way of example, unless disabled, mobile Google maps can track a user's physical location and store that information over a period of years.[21] And, even disabling the function will not erase past history; one periodical declared, "Google's Location History

[20] NPRM at para. 4.

[21] "Where to Find the Map that Shows Google is Tracking Your Location," Matt Elliott, c|net (Nov. 5, 2015) (http://www.cnet.com/how-to/how-to-delete-and-disable-your-google-location-history) (last viewed May 19, 2016, 17:49).

Browser is a Minute-By-Minute Map of Your Life"[22] (IoS users must initiate a five-step process to disable the function). Indeed, recent announcements confirm the extent to which firms that are not beneath the Commission's jurisdiction are utilizing consumer data. Google has introduced new artificial intelligence (AI) software that will analyze the *content* of text messages and photos in order to recommend responses to received messages; the software will also "learn" user preferences in order to provide tailored responses to inquiries. Amazon, Facebook, WhatsApp, and Apple offer competing technologies. The Washington Post uses cookies, web beacons and "other technologies" for online tracking and advertising.[23] To be sure, NTCA does not decry these technologies, which promise consumer benefits beyond restaurant recommendations: the ability of Google to review "big data" enables its software to now recognize eye disease in scanned images. [24] Rather, NTCA proposes that the security and use of data sets should be addressed based upon the data, and not upon the holder. As the Commission moves forward with this proceeding, NTCA urges the Commission to balance all market needs. As noted above, NTCA members generally do not, as a practice, dabble in the business of brokering customer data. But, neither should any BIAS provider be prevented from nor held liable for actions that if undertaken by another party would be permitted, or at least governed by a standard of law that

[22] "Google's Location History Browser is a Minute-By-Minute Map of Your Life," Greg Kumparak, TechCrunch (Dec. 18, 2013) (http://techcrunch.com/2013/12/18/google-location-history) (last viewed May 19, 2016, 18:05).

[23] Privacy Policy, Washington Post (https://www.washingtonpost.com/privacy-policy/2011/11/18/gIQASIiaiN_story.html) (last viewed May 25, 2016, 10:50). The Post explains further that in addition to itself, "third-parties may collect or receive certain information about your use of Services, including through the use of cookies, beacons, and similar technologies, and this information may be combined in information collected across different websites and online services."

[24] "Google Touts New AI-Powered Tools," Jack Nikas, Wall Street Journal, p.B1 (May 19, 2016).

provides comprehensive and uniform protections to customers. NTCA therefore supports a logical, limited, and narrow application of CPNI rules that are specific to the "telecommunications services" aspect of BIAS, and which do not depart fundamentally from the processes by which CPNI is protected today. Paired with the guidance of self-determined industry best-practices and FTC oversight with respect to protection of consumer data, this approach will provide consistent and comprehensive consumer protection while promoting parity among market players.

By way of a specific and important example, NTCA opposes the exercise of Commission jurisdiction over "personally identifiable information" (PII) (which is already addressed by the FTC)[25] and the follow-on new category of "customer proprietary information," the latter of which the Commission intends to include both CPNI and PII.[26] Accordingly, NTCA opposes any recommendation that is grounded in the creation of a "customer proprietary information" category. Therefore, in the comments set forth below, NTCA positions regarding such matters as "personally identifiable information" and the collective "customer proprietary information" are offered as "pleadings in the alternative," with the implicit qualification of "to the extent the Commission adopts or exerts jurisdiction over such categories. . . ." It is from this perspective that NTCA accordingly addresses the Commission's recommendations, below.

[25] *See,* NPRM at para. 60.

[26] NPRM at para. 57.

II. DISCUSSION

A. DEFINITIONS OF KEY TERMS

1. Broadband Provider

The Commission proposes to apply the definition of "Broadband Internet Access Services" or "BIAS" that was used in the *2015 Open Internet Order*.[27] Specifically, the Commission proposes to define broadband as a

> mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this part.

Consistent definitions are useful for network operators and their advisors, and in this regard, NTCA supports incorporation of the definition provided above. Notably, however, this definition, which focuses on the *holder* of the information, rather than the information itself, underscores the potential outcome of the Commission proposals, specifically that one sector of the broadband industry would be subject to regulations while others with access to identical information, such as edge providers, are not regulated similarly. In addition to regulatory disparity, as noted above, this approach can lead to grave customer confusion. Most users will be unaware that regulatory oversight could depend less upon the *nature* of the data and more upon the *holder* of the data. A generally applicable standard of care derived from and beneath the jurisdiction of FTC principles that apply to all players would be a sounder approach.

[27] NPRM at para. 29.

2. Affiliate

The Commission seeks comment on the definition of "affiliate" for purposes of Section 222-sourced rules for BIAS providers. The Communications Act defines "affiliate" to mean "a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person," where the term "own" is defined to mean "to own an equity interest (or the equivalent thereof) of more than 10 percent."[28] Consistent with its general support for consistency among defined terms, NTCA supports this proposal. In the first instance, aligning the definition with the statute will preempt confusion among companies complying with the rules. The definition also accommodates a field of entities that would be able to compete effectively with firms that are not affiliated with regulated entities. This could be particularly beneficial to small BIAS providers serving small markets. Those markets which are at the outset uneconomic to serve for BIAS providers may be similarly unattractive to other technology-focused firms. In such instances, the local, community-based BIAS provider would be naturally well-suited to provide invoke its expertise and provide technology and communications-focused services to the community. A small BIAS provider may, for various reasons, establish different corporate structures from which to provide these services, yet its ultimate goal will be to provide critical technology services its small community. A consistent definition of affiliate that would then define groups of entities with which information can be shared (to the extent the Commission imposes restrictions on sharing certain data with unaffiliated parties) would assist the provision of technology services in rural areas.

[28] 47 U.S.C. § 153(1).

3. Definition of Customer and Other Users

(a) Applicants and Former Customers

The Commission proposes to define "customer" to mean (a) a current or former, paying or non-paying subscriber to BIAS; and (b) an applicant for BIAS. The Commission also seeks comment on whether the existing Section 222 definition of customer should be "harmonized" with this proposed broadband definition.

The Commission explains that under current Section 222 rules, "[a] customer of a telecommunications carrier is a person or entity to which the telecommunications carrier is currently providing service." The Commission proposes that the existing rule's limitation to current subscribers is insufficiently narrow, particularly as applied to the broadband context due to advances in retaining, using and selling personal information.[29] The Commission speculates that "[b]ecause BIAS providers have the ability to retain and reuse applicant and former customer proprietary information long after the application process is over, or the former customer has discontinued its subscription," a customer for BIAS purposes should include "both applicants for BIAS and former BIAS customers."[30] As explained below, the rationale to extend Section 222 protection to applicants conflicts with the statute and is moreover insufficient and should be rejected. Applicants (and former customers) can obtain sufficient protection within the same arena as edge and app providers that are governed by FTC standards.

The Commission's rationale is conceivably applicable to *any* business whose application process may collect various information. These may include both communications and non-

[29] NPRM at para. 32.

[30] *Id.*

communications firms, including department stores and gasoline stations whose business practices are governed adequately by existing proscriptions on unfair or deceptive practices. For example, an on-line application for a JC Penny credit card requires name, address, Social Security number, mother's maiden name, annual income, date of birth and home telephone number,[31] information that is mostly identical to the Commission's proposed category of regulated "PII."[32] Quite notably, Synchrony Bank, which administers the service, informs applicants that they **cannot** limit that firm's sharing of personal information for their marketing purposes, for joint marketing with other financial companies, and for their affiliates' everyday business purposes that include information about the customer's "transactions and experiences."[33] There is no sufficient basis to conjecture that BIAS or other communications providers, by contrast, are especially motivated to play "fast and loose" with information of prospective customers; this is especially true of applicants who have not generated any usage data. A consistent application of FTC standards is sufficient.

NTCA therefore supports the current definition of "customer" as defined by 47 CFR § 64.2003(f),[34] and opposes extending the rigorous protocols that govern *actual* customer information to information provided by *prospective* "customers." To be sure, NTCA does not

[31] https://www.onlinecreditcenter6.com/eapplygen2/load.do?cHash=1342177401&subActionId=1000 (last viewed May 20, 2016, 9:14).

[32] *See*, NPRM at para. 62.

[33] *See*, https://nj04.rfecom.com/consumereApply/Internet/jcpenney/en/js/TermsConditions.htm#Privacy (last viewed May 20, 2016, 9:18).

[34] The section states, "A customer of a telecommunications carrier is a person or entity to which the telecommunications carrier is currently providing service." This is wholly consistent with 47 U.S.C. 222(h)(1)(A) which specifies ". . . subscribed to by any customer . . . ."

propose that sensitive information disclosed in applications should be scattered to the four winds. Rather, NTCA proposes that current FTC and applicable local standards are sufficient to ensure the proper treatment of prospective customer information, particularly given that the information gathered from such applicants does not include the type of information upon which the statute actually confers protection as CPNI (*i.e.*, "information that relates to the quantity, technical configuration, type, destination, and amount of use of a *telecommunications service* subscribed to by any customer of a telecommunications carrier").[35] This discussion highlights a concern that permeates the NPRM: as noble as the Commission's goals may be, its powers are granted pursuant to and limited by statute. Nothing in the statute enables the Commission to ignore the "subscribed to" language in finding suddenly that a *prospective* customer who has *not* subscribed is the beneficiary of CPNI protections. The Commission needs at every turn to turn to the *actual language of the statute* in considering potential expansions of the existing program.[36]

As noted above, the Commission offers only conjecture that this ability to retain data, or to process it, or to possess so-called incentives exists with broadband more than any other

[35] 47 U.S.C. § 222(h(1)(A) (emphasis added).

[36] It is worthwhile at this point to amplify a characteristic of NTCA providers, who are locally-operated and community-based, that was noted above. In the small communities served by NTCA members, the local communications provider is often the largest employer in the community. NTCA members are also frequently involved with many community efforts, including local Chambers of Commerce and assisting with community initiatives or events. On a more personal level, in a small community, staff of the local provider are often known personally to the customers; managers and directors are similarly known. To wit, at a recent NTCA member meeting, a director of a locally-operated provider asked his industry peers in an open forum how they manage customer service requests from friends or neighbors who contact board directors, rather than the customer service office, for assistance. In addition to the legal obligations to which NTCA members are already bound, deep social and community imperatives govern their respect and protection of customer information. To the extent that regulatory imprint is necessary when the market cannot regulate itself effectively, that concern does not attach as readily with regard to small, community-based providers

service. Applicants for broadband service do not generate more information than applicants for any other service, and in that respect there is no reason why the Commission should endeavor to place upon providers of BIAS obligations to which providers of other services are not bound. Moreover, from a management perspective, incorporating the applications of persons seeking but not subscribing to service into the universe of protected records and data would increase administrative burdens for small providers. Standard business practices already impose sufficient incentives for protecting sensitive information, such as record destruction policies, and need not be duplicated by rules that themselves are intertwined with reporting requirements. Doing so will simply increase burdens on providers, especially those who by definition of their size have limited staff.

The Commission asks whether "without the privacy protections of Section 222, consumers may be hesitant to apply for BIAS or current BIAS users may be apprehensive about switching service providers out of concern that their current provider may stop protecting their privacy after they switch providers."[37] These questions presuppose without basis that BIAS providers (and only BIAS providers) would masquerade or harbor ill intentions in this presumed parade of horribles. NTCA returns to the proposition that existing practices and obligations to which providers (and other firms) currently abide are sufficient, and that in these regards consumers should have no different concerns than other providers of goods or services with which a customer might terminate a contract. Consumers will understand correctly that sufficient protections under existing Federal and local regulations will be applied for as long as the entity retains their information. Similar concerns could conceivably be conjured about a person's

[37] NPRM at para. 33.

accountant, but there is no indication or basis for the implied assumption in the Commission's proposal that consumers would have greater concerns that once they sever their relationship with a provider, their information may be cast to the four winds. Or, these same arguments could apply with equal force to any content or edge provider with which a consumer interacts – knowing that Google, for example, can use whatever input a customer provides to render "relevant" advertisements on other websites months later. Therefore, while consumer protections are advised, the basis for implementing them should not be misplaced considerations that post-customer relationship protections are necessary to advance competition.

Federal and local guidelines that govern effectively the relationships of firms and their prospective or past customers exist. There is no reason to impose additional standards upon only one segment of the broadband industry while others remain subject to existing and effective standards.

(b) Protections for Multiple Users

The Commission notes that "a single BIAS subscription is often used by multiple people. Residential fixed broadband services typically have a single subscriber, but are used by all members of a household, and often by their visitors." The Commission asks whether the definition of customer should reflect the possibility of multiple broadband users.[38]

"There is nothing new under the sun."[39] In the realm of plain of telephone service (POTS), numerous people may share a single line. Family plans for mobile phones, even so-called "flip phones" that lack a broadband capability, similarly offer users the ability to attach

[38] NPRM at para. 34.

[39] Ecclesiastes 1:9.

multiple devices to a single account. Current CPNI requirements address the account holder, and the same construct should apply in the BIAS environment. A provider cannot know who is using the service at any particular time. Setting a stage on which the provider would be required to identify and establish some form of privity with each user (even a registered user in a family plan) creates an administrative nightmare: Would a provider be required send multiple notices to a single household? If members of the "family plan" live away from home (at school, for example) would the provider be required to develop a database of separate family addresses and send notices to multiple locations? With whom would responsibilities to identify, locate and notify each user at any location reside?

NTCA supports the Commission's proper proposal to "limit[] the proposed notice and consent requirements to interactions with a single account holder, as opposed to every individual who connects to a broadband service over that connection."[40] Consistent with current CPNI procedures, the notice should be provided to the account holder. Imposing any other sort of requirement on carriers would increase complexity for both the carriers and consumers. It would implicate requirements involving consent and contracts with minors if family plan members are beneath the age of majority. For small providers, especially, the notion that all potential users would be warrant notification would place an undue burden on those firms whose limited resources would be required to consistently monitor and update the contact information of multiple users, as well as undertakes steps necessary to accommodate the special circumstances of minors.

[40] NPRM at para. 35.

(c) Consistency in the Rules

The Commission asks whether definition of "customer" in the existing CPNI rules should be consistent with its proposed definition of "customer" in the BIAS context. Inasmuch as NTCA opposes the Commission's expanded definition of "customer" in the BIAS context, NTCA opposes such "harmonization." If the Commission disregards reasoned bases for maintaining the existing standard and adopts an expanded definition for BIAS, then the existing CPNI rule as applicable to voice providers should remain, and obligations and liabilities for existing relationships and regulatory structures should not increase.

4. Defining CPNI in the Broadband Context

(a) Elements of Service

Section 222(h)(1) defines CPNI to mean "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship" and "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer or a carrier" (except that subscriber list information can be provided upon request to any person publishing directories).[41] The Commission asks whether there is any need to include the second part of that definition, specifically, the portion referring to "telephone exchange or telephone toll service, in its rules regarding BIAS services.[42] NTCA submits that portion can be excised. More generally, NTCA reiterates that new regulations

[41] 47 U.S.C. § 222(e).

[42] NPRM at para. 38.

intended to create analogous CPNI treatment in the broadband context should hew to the statutory construct of addressing information that arises specifically and uniquely from use of the communications service, rather than information of a type that is collected and potentially used by both by firms that offer and those do not offer communications services.

The Commission proposes that the various information be included in CPNI as it may relate to BIAS, including, but not limited to: (1) service plan information, including type of service, service tier, pricing, and capacity; (2) geo-location; (3) media access control (MAC) addresses and other device identifiers; and (4) source and destination Internet Protocol (IP) addresses.[43]

NTCA submits that information related to a customer's broadband service plan can be viewed as analogous to voice telephony service plans, and can therefore support the Commission's proposal to consider it as CPNI. NTCA notes, however, that this is limited to information that would address the type of service, the service tier, pricing and capacity as outlined above. NTCA similarly notes the statute states clearly that CPNI includes the "location . . . of the *service.*"[44] Therefore, information relating to "the physical or geographical location of a customer or the customer's *device*"[45] may be CPNI *only* to the extent that it may reveal location of the device at the time service was being used. Accordingly, the current standard of "location . . . of the service" is sufficient, and there is no need to incorporate the device into the definition.

[43] NPRM at para. 41.

[44] 47 U.S.C. § 222(h)(1) (emphasis added).

[45] *See*, NPRM at para. 43 (emphasis added).

(b) MAC and IP Addresses and Applications

The Commission proposes to consider a media access control (MAC) address associated with a customer's device to be CPNI in the broadband context.[46] MAC addresses are assigned to network adapters. A MAC address is transmitted only from device to device; at each "stop" along the way, the MAC address is replaced serially by the next device in line. At most, a MAC address is associated to a device, but not to a location. And, since MAC addresses can be changed, the ability to associate a particular address with a specific device is not guaranteed. MAC addresses are used for networking. They do not identify either a user or an account. Therefore, they should not be included within the definition of CPNI.

The Commission proposes to consider source and destination IP addresses as CPNI in the broadband context.[47] NTCA submits that the Commission's comparison of IP addresses to telephone numbers in the voice telephony context is of limited application. The Commission explains that it has previously held telephone numbers dialed to be CPNI.[48] Even if *destination* IP addresses are considered as CPNI, source IP addresses should not be considered CPNI. Source IP addresses are available in many ways, including with every email sent. It is, therefore, inconceivable that a BIAS provider would be required to protect information that is provided freely by users in many of their current online interactions. To the extent that source IP address information would utilized in a manner that conflicts with fair trade practices, then actionable

[46] NPRM at para. 44.

[47] NPRM at para. 45.

[48] *Id.*

offenses could be addressed under applicable laws. The source IP address information *per se*, however, should not be protected information.

The Commission seeks comment on whether it should consider port information to be "technical configuration," "type," "destination" information and/or any other category of CPNI under Section 222(h)(1)(A).[49] The Commission explains that a port is a logical endpoint of communication with the sender or receiver's application, and that the destination port number determines which application receives the communication. The Commission states its position that port numbers "identify or at least provider a strong indication of the type of application used, and thus the purpose of the communication, such as email or web browsing." By the Commission's acknowledgement, port information describes the application used, but not the content thereof. It can be used to discern whether a person was using email or browsing the Internet, but there is no compelling reasons to capture this information within the strict standard of CPNI. To the extent a provider uses it unfairly, applicable FTC or other guidelines may be applied.

The Commission seeks comment whether and under what circumstances data the broadband provider collects about the use of applications would meet the statutory definition of CPNI.[50] NTCA submits that including this information would be a significant and unnecessary expansion of the CPNI requirement. The CPNI rules adopt the statutory definition of CPNI.[51] The statute addresses "quantity, technical configuration, type, destination, location, and amount

[49] NPRM at para. 49.

[50] NPRM at para. 50.

[51] 47 C.F.R. § 64.2003(g).

of use of a *telecommunications service."*[52] The bounds of reasonableness are stretched by a proposal to extend that statutory definition to the add-on applications a user might engage. To reiterate, NTCA does not propose that these types of data can be used *volens nolens,* without regard to consumer expectations or demands. Rather, NTCA submits that the standards addressing such usage should be equivalent across the range of firms that engage with this data, and that to the extent non-BIAS providers fall beneath the jurisdiction of the FTC, BIAS providers should be under no greater obligation to protect this information than edge or application providers who have access to the identical information and who are not bound by Commission requirements. Unlike HIPPA, which addresses the *type* of information at issue, this requirement would impose disparate regulatory structures upon different parties that have access to the *same* information. Therefore, treatment of this information should fall beneath the standard of "unfair and deceptive trade practices," rather than prescriptive prohibitions as proposed by the Commission.

(c) Customer Premises Equipment

The Commission seeks comment on whether information regarding customer premises equipment (CPE) should be considered CPNI.[53] The Commission suggests that this may include, "a customer's smartphone, tablet, computer, modem, router, videophone or IP caption phone."[54] This proposal should be rejected outright, and for several reasons. First, there is no statutory basis in Section 222 to contemplate CPE as an included element. CPNI is defined as the

[52] 47 U.S.C. § 222(h)(1) (emphasis added).

[53] NPRM at para. 52.

[54] *Id.*

"quantity, technical configuration, type, destination, location, and amount of use of a *telecommunications service,"*[55] and does not address the device incorporated by the customer in using the service. The Commission's reference in the NPRM to the definition of CPE correctly cites 47 U.S.C. § 153(16) to define CPE, but nowhere in Section 222 is CPE mentioned. In fact, the only point in Section 222 at which "equipment" (the salient element of CPE) is mentioned refers to *equipment manufacturers.*[56]

The Commission proposes that under its proposal, customer proprietary information could include "a customer's smartphone, tablet, computer, modem, router, videophone, or IP caption phone,"[57] a suggestion that illustrates fully the astonishing outcomes the NPRM could allow. In the first instance, CPE is not in any way, shape or form envisioned by the statue as being bound up in the fortifications of CPNI. *Arguendo* Section 222 could be read to afford the Commission discretion to include CPE, it would implicate an illogical if not irrational outcome in which BIAS providers would be subject to requirements and liabilities to which vendors such as BestBuy, Amazon and Walmart or manufactures from Apple to Zyxel would not be subject. Further, *arguendo* Section 222 could be read to include CPE, the absurdity of the Commission's proposal is illuminated as each type of equipment the Commission conceives to address is examined. For example, broadband interaction is but a single purpose of a desktop or laptop computer, which may be used for word processing, accounting, mathematical and scientific applications, and other functions wholly unrelated to and not reliant on BIAS. Information about

[55] 47 U.S.C. § 222(h)(1) (emphasis added).

[56] 47 U.S.C. § 222(a).

[57] NPRM at para. 52.

mobile devices, such as smartphones and tablets, by virtue of their intended mobile use may be independently derived by public observation.

Third, and critically, the instant proposal must be rejected because it is an unwarranted departure from the Commission's explicit prior ruling that CPE does not "constitute 'telecommunications services as defined by the Act.'"[58] In fact, the Commission noted expressly that "information derived from the provision of any *non-telecommunications service, such as CPE . . . is not covered* . . . ."[59]

The Commission seeks comment on the potential impact on small providers.[60] NTCA reiterates its opposition to the proposal. NTCA further submits that the ability of any provider to document CPE would be frustrated by the ability of consumers to obtain devices from many varied retailers. To the extent, however, that the Commission entertains any notion of including CPE in the bucket of protected information, enumerated lists, such as those that would provide defined categories of CPNI, could be useful inasmuch as they would provide the "rules of the field" plainly at the outset. And, such lists should be limited strictly to devices provided by the provider; under no circumstances should a provider obligated to protect information relating to devices obtained from other parties. Finally, it must be noted that these sort of lists will become rapidly outdated as technology expands the various devices that will be available.

---

[58] *See, Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information: Order,* Docket No. 96-115, DA 98-971, at para. 4 (1998).

[59] *Id.,* at para. 3 (emphasis added; internal citation omitted).

[60] NPRM at para. 55.

5. Proposals to Create New Categories of Purportedly Protected Information

The Commission proposes to create a new category of protected information, specifically, "personally identifiable information" (PII) and to define PII to mean any information that is linked or linkable to an individual.[61] The Commission also seeks comment on whether it should "harmonize" existing CPNI rules with those it proposes for BIAS.[62] Before addressing the issue of "harmonization" among rules, NTCA will address the imperative that the promulgation of rules can be effected only insofar as they are harmonious with the statute.

Perhaps no phrase is better suited to approach the matter of PII than Commissioner O'Reilly's assessment of "make-believe authority."[63] The Communications Act gives the Commission the job of telecommunications regulation; it is nothing more, and no matter how noble the cause or intent, the Commission's authority to take any particular action is necessarily defined and limited by the four corners of the statute. Here, the statute addresses "quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service" and "information contained in bills."[64] It does not address the laundry list of information the Commission proposes to now extend its protection. The statute does not address Social Security numbers, nor date and place of birth, nor mother's maiden name, nor unique government identification numbers. It neither addresses email addresses nor education or

[61] NPRM at para. 57.

[62] NPRM at para. 59.

[63] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services: Dissenting Statement of Commissioner Michael O'Reilly,* Docket No. 16-106, FCC 16-39 (rel. Apr. 1, 2016).

[64] 47 U.S.C. § 222(h)(1) (emphasis added).

employment information. It further does not address biometric or shopping information. In fact, to the extent the Commission conjectures that a customer's name, address and phone number should be protected, NTCA directs attention to the Commission's prior declaration that "[a] customer's name, address, and telephone number are not CPNI."[65]

Neither "PII" nor the collective "customer proprietary information" category proposed by the Commission[66] appear in the statute, and neither does the statute confer upon the Commission authority to create such categories. The Commission proposes that the Section 222(a) description of "proprietary information of . . . customers" is a category apart from "customer proprietary network information" as described by Section 222(c).[67] This expansion is not supported by the plain language of the statute. Section 222(a) discusses the confidentiality of proprietary information, and then establishes which parties enjoy protection under the statute; these include telecommunications carriers, equipment manufacturers, and customers. In fact, Section 222(a) does not describe, define, or otherwise indicate any *type* of information that would fall within that general category of "proprietary," but rather merely lists the entities to which the section applies. In contrast, Section 222(c) draws upon the incorporation of customers in the section, and then elucidates the type of information (specifically, CPNI) that is protected. If, as the Commission reasons, Section 222(a) would create a separate category of information, then the section would certainly have included a description of information *other than* that which is defined by Section 222(c). The absence of any other specifications reveals that CPNI is precisely

[65] *Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information: Order,* Docket No. 96-115, DA 98-971, at para. 1 (1998).

[66] NPRM at para. 57.

[67] NPRM at para. 56.

and solely the customer information that is protected by Section 222(c). These statutory considerations aside, NTCA now turns to the substance of the Commission's proposal.

Even if the Commission possessed the authority to expand the statute to create a new set of protected information, the Commission's proposal must be rejected on several grounds. To be sure, the proposition that Social Security numbers, date and place of birth, mother's maiden name, and unique government identification numbers, such as driver's license or passport numbers, are guarded by customers is likely consistent with current consumer expectations. The proposition that the Commission should regulate treatment of this information, however, is not consistent with current practices. As has been noted throughout these comments, numerous firms, both within and without of the broadband communications industry, have access to this information, and are governed by Section 5 of the FTC Act. There is no justifiable reason to single out BIAS providers for special regulations that do not apply to other actors on the broadband stage, such as edge or app providers who have access to the same information, and under the same circumstances.

But the Commission does not stop with simple regulatory disparity in the regions of information whose private nature may be acknowledged. Instead, the Commission attempts to cast a net over data that is so pervasively public that the Commission's proposal to render it protected "PII" sends the temperature on an already chilling shroud of regulatory disparity plummeting. In no logical world does information that is part of the public record, including physical or postal addresses, fall beneath the umbrella of protection. Similarly, telephone numbers, which can be found in telephone books (and which, in fact, must be provided under

Section 222 statute to third parties),[68] and eponymous email addresses, which by definition disclose the name of the holder, similarly fail to exhibit any indicia of the owner's desire for secrecy. Education and employment information are readily available through sources such as alumni organizations or professional associations. And, shopping information, which is similarly tracked by retail stores through various promotions, is also readily available and used by retail and other firms.

NTCA does not propose license to use these data deceptively or unfairly. Rather, NTCA proposes that existing Federal and local regulations and practices govern a universe of firms that have access to and utilize this information, and the Commission's proposal to select a sliver of the market and impose upon it discrete responsibilities and liabilities is inconsistent with the statute and parity. The Commission's approach should be formed by consumer and market expectations of privacy, grounded in FTC principles of determining what might be an "unfair and deceptive" action, rather than a laundry list that includes information that is obtainable from easily accessible resources, including public records. Treatment of that information, and of entities that use that information, should be addressed within the parameters formed by Section 5 of the FTC Act. The Commission's proposal to "consider a BIAS customer's name, postal address, and telephone number" as protected "PII" stretches the bounds of credulity. The Commission's distinction that the "statutory definition of CPNI 'does not include subscriber list information,'"[69] is notable; the volume of junk mail and "junk calls" from parties as varied as political action groups, charities and window sellers demonstrates (a) that this sort of information

[68] *See*, 47 U.S.C. § 222(e). The statute provides that the subscriber list information exemption is for directories "in any format," which would include on-line.

[69] NPRM at para. 63.

is readily available and (b) subjecting BIAS providers to protection requirements whilst the local lawn improvement firm is bound by no such obligations represents an unsustainable disparity.

6. Content of Customer Communications

The Commission seeks comment on how it should define and treat the content of customer communications.[70] The Commission explains that existing Federal and state laws, including the Electronic Communications Privacy Act (ECPA), the Communications Assistance for Law Enforcement Act (CALEA), and Section 705 of the Communications Act, address the content of BIAS and PSTN communications.[71] NTCA submits that these existing statutes and regulations obviate the need for the Commission to layer on additional regulation. If anything, the existence of statutes already governing such information should speak volumes as to the lack of any need or reason to shoehorn such information into yet another statutory provision that heretofore was never contemplated to cover such information; when Congress intended to speak on such matters, it clearly knew how to do so. To the extent the content contains information previously enumerated as CPNI, then violations for disclosure may attach, and the Commission's goal of implementing disincentives to inappropriate behavior will be fulfilled.

B. APPROVALS FOR USE OF INFORMATION

1. Communications-Related Services and Related Terms

The Commission proposes to define the term "opt-out approval" as a method for obtaining customer consent to use, disclose, or permit access to the customer's proprietary information.[72] NTCA submits that the objective here should be to retain existing practices and

[70] NPRM at para. 68.

[71] *Id.*

[72] NPRM at para. 67.

processes governing use of CPNI, with only the narrow scope of analogous information arising in the BIAS market to be brought into the purview of those processes. The Commission should reject recommendations to expand both the carrier obligations and the information to which they might apply. Toward this end, NTCA again states its opposition to the creation of any category of "PII" or a follow-on, collective "customer proprietary information." BIAS provider use of that information may be exercised in the same manner as undertaken by broadband industry firms that are not under the authority of the Commission.

The Commission seeks comment on how best to define "communications-related services" for purposes of its proposal to allow BIAS providers to use customer information to market communications-related services to their subscribers, and to disclose customer information to their communications-related affiliates for the purpose of marketing communications-related services subject to opt-out approval.[73] NTCA suggests that the Commission should not limit "communications-related services" to services that are regulated by the Commission. Rather, "communications-related services" should include those services offered by the BIAS provider or its affiliates that rely upon the core communications services offered by the provider. As the Commission notes, the current Section 222 rules define communications-related services to mean "telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision or maintenance of customer premises equipment."[74] These are distinguished by the rules to exclude retail customer services that are accessed by the Internet.[75] NTCA submits that the current

[73] NPRM at para. 68.

[74] NPRM at para. 72.

[75] 47 C.F.R. § 64.2003(i).

definition should include a broad scope of services, including those related to the providing BIAS. These may include the marketing, installation and technical support for modems or accessories; Internet-based security monitoring of both premises and networks; and "smart home" applications, including devices intended to enable personal or utility applications. NTCA emphasizes that this is not intended to convey a position that information collected or used in these regards may be used freely and without restrictions; rather, NTCA submits that BIAS providers utilizing such information would comport their behavior to standards as formed beneath FTC guidelines.

The Commission proposes to define aggregate customer proprietary information as collective data "from which individual customer identities and characteristics have been removed."[76] NTCA supports this approach, which is consistent with Section 222(h)(2). By definition, aggregate information is rinsed of personal identifiable information and therefore does not implicate privacy concerns.

2. Breaches

The Commission proposes to define "breach" as any instance in which "a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information."[77] Critically, however, the Commission proposes that this new proposal would not (a) not include an intent element, as do the current rules, and (b) would cover all "customer's proprietary information," rather than only CPNI. NTCA opposes this measure, which risks imposing upon BIAS providers a standard that approaches, if not meets, strict

[76] NPRM at para. 74.

[77] NPRM at para. 75.

liability. Under this rubric, and to the extent the Commission adopts a "customer's proprietary information" standard (which would include "PII"), it is conceivable that a postal carrier's delivery of a bill that contains "PII" to an incorrect address would meet the standard enabling "access, use[], or disclos[ure]" of information and subject the BIAS provider to an enforcement action. Moreover, under the Commission's proposed notification rules, the provider would be required to notify the Commission and undertake numerous administrative steps in regard to the error, regardless of whether any harm occurred. NTCA submits that the Commission should maintain the element of intent in the standard, and that any harm arises from unintentional disclosures can be addressed within the context of traditional constructs of law.

The Commission justifies its proposal by reasoning that "not including a requirement that the unauthorized access be intentional in the definition of 'breach' will ensure data breach notification in the case of inadvertent breaches that have potentially negative consequences for customers."[78] Two qualities, however, mitigate against the Commission's concern. In the first instance, providers seeking to maintain their reputation and relationship with consumers will have sufficient incentive to not be viewed as accomplices to damage, and will therefore be expected to notify customers should harm be reasonably predicted to occur; this is especially true for small providers such as the members of NTCA.[79] Second, existing legal standards are eminently capable of addressing issues such as negligence and due care, and the Commission should forbear from regulatory imprints that exceed the standard level of care adhered to by the industry outside of CPNI rules, particularly when other entities that have access to the same

[78] NPRM at para. 76.

[79] *See,* fn. 36, *supra.*

information are not similarly regulated. At the very least, the Commission should ensure that good-faith acquisition of covered data by an employee or agent of the company, where such information is not used improperly or further disclosed, be excluded from any definition of a violation. The lack of an element of intent risks casting a large net of liability over unintentional and largely harmless disclosures, such as those that might arise within the four walls of the company or its affiliates. Accordingly, intent should continue to be a required element in the Section 222 regime, while unintentional breaches should follow standard business protocols as governed by general statutes and the FTC.

To the extent the Commission implements a new category of "PII," including that information within the definition of breach[80] would only exacerbate disparities because it includes information to which many other firms have access. If the Commission were to include physical address or telephone number information, then the impacts would be even more dissonant with user, business and market expectations. The proposal to require notifications for unintentional disclosure of so-called "PII" beyond those that would be covered by existing state laws or Federal legal standards independent of Section 222 sets forth a scenario in which the regulated providers will be held to, and accountable for, standards to which other firms with the same information are not subject. As described above, this proposal could have a profound effect on small businesses. The risk of strict liability for actions that do not cause harm could well discourage small companies from entering or expanding their markets. This could prove troublesome to not only the providers but to prospective customers, as well, who would be affected adversely by a lack of service. NTCA submits that the Commission must take a

[80] *See,* NPRM at para. 75.

reasoned and balanced view of the market and address whether consumer expectations and marketplace realities (the latter of which contemplates numerous non-communications companies with access to the same data but without the same liabilities) support a regime that favors regulatory disparity.

3. Proposals to Establish Broader Obligations

The Commission proposes to revise current CPNI rules to clarify that they apply only to telecommunications services other than BIAS.[81] The Commission requests comment on the benefits or burdens of updating these definitions, particularly for small providers. NTCA submits that its members currently treat broadband subscriber information with the same attention as they ascribe to voice service customer information. Although a uniform set of regulations would increase administrative efficiency and would effectively "codify" the practices of NTCA members, uniformity should be pursued *only* to the extent that such reconfiguration does not increase obligations with regard to voice services. Firms with limited staff and resources should not be burdened with the imposition of multiple strains of regulatory processes. At most, the Commission might prescribe safe harbor conduct standards, and allow that providers operating otherwise will be subject to general FTC standards.

C. PRIVACY POLICIES

1. Privacy Notice Requirements

The Commission proposes to require BIAS providers to provide customers with "clear and conspicuous notice of their privacy practices at the point of sale and on an on-going basis

[81] NPRM at para. 80.

through a link on the provider's homepage, mobile application, and any functional equivalent."[82] NTCA submits that the required provision of notice should be limited to the point of sale and the provider homepage. NTCA also submits that "notice" should be understood should include notification of the policy, rather than an open-ended obligation for the company to recite the policy word-for-word. Consumers with specific questions will be motivated to seek counsel from provider staff if they have specific questions; provider staff will be motivated by corporate commitments to avoid unfair or deceptive practices to provide forthright and useful information upon request. To the extent that "mobile application" refers only to the firm's website interface with consumers via a mobile device, that requirement may be acceptable. However, the conjunctive form of the proposal ("*and* any functional equivalent") should be rejected in favor of flexibility that requires the firm to provide notice at the point of sale and on the homepage, but which permits the firm to identify mobile or other venues that would best serve consumer needs. Further, it is not clear how the Commission would define "application" for purposes of this section. Many BIAS providers have multiple mobile apps, including those that track usage and data consumption; those that enable bill payment; and those that enable assistance with devices. A requirement pertaining to point of sale and the provider's home page is sufficient.[83]

The Commission proposes a comprehensive list of requirements that would attend the provision of privacy notices to consumers.[84] NTCA submits that it does not *per se* oppose notice requirements that describe the types of customer information that the BIAS provider collects by

[82] NPRM at para. 82.

[83] The proliferation of mobile-friendly website design as a standard is further diminishing the role of certain apps.

[84] NPRM at para. 83.

virtue of its provision of broadband service; how the BIAS provider uses, and under what circumstances it discloses, each type of customer information that it collects; and the categories of entities that will receive the customer information from the BIAS provider and the purposes for which information may be used. However, certain of the Commission's specific proposals in these regards draw concerns. How broadly would terms such as "categories of entities" drawn? Would "marketing" be defined to include all marketing efforts, or just marketing of defined services? The application of these rules must reflect consumer habits and preferences, accommodate flexibility and an ability to respond to market demands, and adhere to principles of regulatory parity such that BIAS providers comport to general industry standards as adhered to by edge, app, and other providers that conform to FTC guidelines and industry practices.

NTCA concurs with the principle that notices must advise customers of their rights and provide access to a simple, easy-to-access method for customers to provide or withdraw consent to use, disclose, or provide access to customer information *to the extent* such "opt-outs" are required by the law. NTCA proposes that the homepage links discussed above satisfy the Commission's desire that such methods be available persistently at no additional cost to the customer.

NTCA does not object to a requirement to provide an explanation that a denial of approval to use, disclose, or permit access to use certain information for purposes other than providing BIAS will not affect the provision of any services to which the customer subscribes. NTCA supports the Commission proposal that carriers be permitted to "provide a brief description, in clear and neutral language, describing any consequences directly resulting from

the lack of access to the customer proprietary information."[85] NTCA submits, however, that the Commission not limit the ability to carriers to exercise commercial speech in selling or marketing and accordingly either eliminate or modify the qualification "brief" from any final expression of the rule. Providers should be permitted to explain as they see necessary the purposes for which the sharing of information may be beneficial to the customer; by way of example, providers could be required to provide *"at least* a brief" description.[86] NTCA supports practices that ensure that such notices are comprehensible and not misleading and, when in print, be legible and use sufficiently large type. NTCA notes that ability of consumers to read notices on a small-screen mobile device may rely upon customer-established settings, but proposes that the ability of many touch screen devices to "expand" an image would preempt any problems. As noted above, NTCA supports the recommendation that customers be made aware of these terms at the terms of sale and thereafter have access to the information through the homepage.[87]

As stated above, NTCA members generally utilize the same rigorous CPNI procedures as have been promulgated for voice services for their broadband customers. This practice has been the case even before reclassification of broadband as a Title II service. However, NTCA registers its concern with certain of the Commission's proposed expansions of requirements. By way of example, the Commission asks whether in order to ensure that information is accessible to customers with a disability, a link to a video of the notice conveyed in American Sign Language

[85] NPRM at para. 83.

[86] To the extent there are concerns that a provider might attempt to bury critical information in a long, drawn out notice statement, such practices would conceivably be actionable as an "unfair and deceptive practice."

[87] NPRM at para. 83.

(ASL).[88] NTCA proposes that as well-intended as certain of these types of proposals might be, a series of "one size fits all" obligations will not serve the intended goal. To invoke the Commission's example, it can be presumed that a hearing impaired customer who might benefit from viewing ASL would be equally served by similarly viewing words on a webpage or a printed page. It is the provision of a *visible* disclosure that transcends the customer's hearing impairment.

The Commission asks whether providers should be required to provide customers with information concerning their data security practices, or the firm's policies relating to the retention and deletion of customer information, or notice of the specific entities with which the provider seeks to share the information.[89] NTCA submits those are unnecessary. In the first instance, that level of detail would be of little, if any, interest or use to most consumers. Additionally, such specificity could provide a roadmap to those seeking to inflict nefarious designs upon the company's processes. Similarly, if a "category of entities" rule were to be adopted, the proposal that providers be required to share notice of the specific entities, rather than categories of entities, with whom information might be shared should be rejected. In the first instance, this would create an administrative nightmare and hamstring a provider's ability to create arrangements in "real market time" with third parties; this could leave these providers severely disadvantaged against other firms that are not subject to Commission requirements. Moreover, this requirement could be triggered if a third party undergoes an internal corporate

[88] NPRM at para. 84.

[89] NPRM at para. 85.

restructuring, and then foists upon the provider a liability whose cause of action rests solely within the domain of the restructured third-party.

2. Timing and Placement of Privacy Notice Requirements

The Commission asks whether it should require carriers to provide notices in addition to those offered at point of sale and through the firm's web portals.[90] NTCA suggests that carriers will best identify the routes through which their customers access information. Accordingly, providers may find that most customers notice privacy disclosures through the firm's homepage; others may find that consumers might be alerted by a notice printed on a mailed bill. However, to the extent that many consumers may either opt for electronic billing, or for automatic billing, it is not necessarily the case that a notice requirement hinged on printed bills would be effective. Indeed, the Commission as much recognizes this phenomenon, noting, "Because we require BIAS providers to have easy-to-access links to their privacy notices that are persistently available . . . we do not think it is a good use of resources to require BIAS providers to periodically provide their privacy notices to their customers."[91] Accordingly, it is sufficient to require providers to provide notice at the point of sale and on the provider's homepage, and to institute a print requirement only to the extent that the provider issues printed bills to the customer. And, in those instances, the notice requirement should not exceed an obligation to

[90] NPRM at para. 87.

[91] NPRM at para 87. NTCA notes, however, that the Commission's full statement here imparts an assumption that proposed rule that will be adopted. The NPRM reads, "Because we **require** BIAS providers to have easy-to-access links to their privacy notices that are persistently available **on their homepage, through their mobile applications, and through any functional equivalent,** we do not think it is a good use of resources to require BIAS providers to periodically provide their privacy notices to their customers" (NPRM at para. 88, emphasis added). However, no BIAS rules are currently in place. The NPRM should rather reflect "to the extent BIAS providers may be required . . . ."

provide notice of the policy with direction to the website or other source, rather than a full printed version of the policy with each billing statement; that route would increase printing and postage costs significantly.

3. Burdens on Providers

The burden on small providers to comply with multiple layers of periodic notice requirements must be considered. Broadband service effectively pre-supposes the availability of textual communications to customers that can be accessed at all times. Requirements for printed or other forms of notice, and mandated periodic notices to consumer once past the sale, are unnecessary in an environment in which constant electronic notice can be accessed through various devices.

Replying to the Commission's inquiry regarding the usefulness of standard forms of notice,[92] NTCA submits that providers should be permitted to determine the format that best meets their market needs. However, NTCA would support a standard form that could be used as a safe harbor.[93] A safe harbor could provide an accessible, low-cost format for small providers. The Commission should rely upon the effectiveness of current CPNI requirements and refrain from imposing additional regulations, such as requiring providers to create notices that are "palatable" to consumers.[94] In these proposals, the Commission appears to questionably require providers to discern the tastes of their consumers and to then formulate their commercial speech accordingly. NTCA submits that this aspect of the proposal should be rejected without further

[92] NPRM at para. 90.

[93] *See,* NPRM at para. 91.

[94] NPRM at para. 95.

consideration. Likewise, the proposal that providers be required to create a "consumer-facing privacy dashboard"[95] would similarly impose upon providers a mandate addressing not simply *what* they communicate to their customers but extensive directions regarding *how* they communicate to their customers. For small providers, particularly, the creation of such a comprehensive, interactive, individually-tailored interface would require significant resources aimed at customizing such a "dashboard" to reflect each consumer's status. This would require both initial design, coding, and on-going updates to user's on-line profiles. This would an extraordinarily complex exercise to capture all individual variables and to convey them meaningfully to every consumer. No single form should be imposed. Each company should determine the method and approach that best meets its and the customers' needs.

4. Providing Notice of Material Changes in Privacy Policies

The Commission proposes to require BIAS providers to (1) notify their existing customers prior to the effectiveness of any material changes in the BIAS provider's privacy policies, and (2) include specific types of information within these notices of material changes.[96] NTCA submits that notice of the change provided by electronic means to the consumer, *i.e.,* via email and in a billing statement, is sufficient, and that the notices then available at the firm's website can be relied upon to provide sufficient information to the customer. The Commission seeks comment on the burden that its proposed material change notice requirements will place on BIAS providers, particularly small providers.[97] Small providers are not seeking any accommodation than should apply rationally to all carriers, except that to the extent pervasive

[95] *Id.*

[96] NPRM at para. 96.

[97] NPRM at para. 101.

notice requirements are adopted, small providers should have the choice to designate and then utilize a primary form of contact with customers – a prominently placed "headline" in a bill announcing a change and then directing users to an electronic platform should be sufficient. Modifying every home page, app, and "functional equivalent" is unnecessary for all providers, but especially burdensome to the smallest.

D. CUSTOMER APPROVAL PROCEDURES

1. Harmonizing Notices for Voice, Video, and Broadband Services

The Commission seeks comment on whether it should "harmonize" privacy notice requirements for voice, video, and broadband services.[98] The Commission notes that many providers offer bundles of voice, broadband, and video services.[99] NTCA supports the ability of providers to utilize a single notice protocol per bundled account. So-called "harmonized requirements" for separate services may be relied upon, but as NTCA noted above, such "harmonization" should not work to *increase* requirements for lines of service that are currently operating effectively. NTCA therefore supports a single form of notice approach. However, at the core of any standard that seeks to reconcile forms of notice must remain a recognition that information that is within the control of the provider is often of the same substance and sensitivity that is available to non-regulated entities, such as edge providers or app sellers. No standard should subject one industry participant to a higher or more burdensome standard than others.

[98] NPRM at para. 103.

[99] NPRM at para. 104.

2. Customer Approval Requirements for the Use and Disclosure of Customer Proprietary Information"

The Commission proposes to require BIAS providers to give a customer the opportunity to opt out of the use or sharing of "customer proprietary information" prior to the BIAS provider (1) using the "customer proprietary information" to market other communications-related services to the customer; or (2) sharing the "customer proprietary information" with affiliates that provide communications-related services, in order to market those communications-related services to the customer. The Commission also proposes to require BIAS providers to solicit and receive opt-in approval from a customer before using "customer proprietary information" for other purposes and before disclosing "customer proprietary information" to (1) affiliates that do not provide communications-related services and (2) all non-affiliate third parties.[100] NTCA qualifies its responses here with its general opposition to the creation of the additional category of "PII," and therefore stipulates that use of the collective term "customer proprietary information" is intended to mean CPNI, except to the extent that the Commission incorporates CPNI and "PII" in a collective category of "customer proprietary information." NTCA submits that BIAS providers should not be restricted to any extent greater than edge or app providers, or other broadband ecosystem participants, or other providers of goods and services that enjoy access to the same types of information. At the least, NTCA submits that providers should be permitted to use information within the corporate family, subject to the standards of "unfair and deceptive" principles.

[100] NPRM at para. 107.

3. Permissible Uses and Disclosures of Customer Proprietary Information for Which Customer Approval Is Implied or Unnecessary

The Commission explains that Section 222(c)(1) permits a BIAS provider to "use, disclose, or permit access to individually identifiable [CPNI] in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service."[101] The Commission seeks comment on how it should interpret the scope of activities that are "in the provision" of BIAS. NTCA proposes that activities that are "in the provision" of BIAS include hardware, software, and solutions, including, but limited to, modems, technical support, trouble shooting, consultation with technical or management consultants, network management, and assistance with connecting user devices and a premises network. Alternatively, all of these would certainly fit beneath "services necessary to, or used in, the provision" of broadband service in the BIAS context. NTCA submits, as well, that "services . . . used in the provision" include such offerings whose sole ability to operate rests upon the BIAS service. These may include "over the top" offerings or other services that are wholly dependent upon and intertwined with the BIAS offering. NTCA supports the Commission proposal to "allow BIAS providers to use any customer proprietary information [to the extent any such obligation is adopted] and not only CPNI, for the purpose of providing BIAS or services necessary to, or used in, the provision of BIAS." No confidentiality concerns are implicated if a seller of BIAS alerts a customer to hardware, software or applications that could make the BIAS service more useful to the customer. To the contrary, service providers who do not offer such counsel could be perceived as

[101] NPRM at para 112.

less interested in customer service than receipt of invoice payments each month. Whether an activity is "necessary" is a malleable term. The focus should be directed, instead, toward determining whether the uses is consistent with ordinary customer expectations. Customers largely expect firms that have access to their data to use their data; consumers expect providers to identify the services and uses that best meet their needs. This all consistent with the dynamic nature of the market, and attended to sufficiently by the FTC standards that look toward unfair or deceptive practices as the triggers for enforcement actions.

NTCA supports the Commission proposal to permit BIAS providers to use "customer proprietary information" (to the extent such an expansion is adopted) for the purpose of marketing additional BIAS offerings in the same category of service.[102] This is fully consistent with consumer expectations. Marketing is not harmful disclosure. NTCA clarifies, however, that "same category of service" should include categories that offer functionally equivalent services, such as video which may be offered over multiple platforms.

4. Emergency Services

NTCA supports the ability of BIAS to use "customer proprietary information" for the delivery of emergency services, to protect users or others from cyber security threats or vulnerabilities, and to address such issues as "spoofing" and unlawful "robobcalls."[103] The linchpin to this discussion is "consumer protection," which is the self-same goal from whence Section 222 arises. This is neither functionally nor philosophically different than the statutory

[102] NPRM at para. 114.

[103] NPRM at paras. 115-118.

exemption granted by Section 222(c)(1). Use of this information for consumer protection and public safety should be permitted and no liability under Section 222 should attach.

NTCA supports the proposal of the Commission to permit broadband providers to use CPNI without customer approval in the provision of inside wiring installation, maintenance, and repair services.[104]

5. Marketing Communications-Related Services

NTCA recognizes that the Commission's position that BIAS providers provide a customer with notice and the opportunity to opt out before using the "customer proprietary information" to market communications-related services to that customer, or before sharing that information with the affiliate, is consistent with current rules.[105] NTCA submits that in light of the prevalence of bundled services, customers generally expect that their broadband providers may use or share the customers' proprietary information with affiliates to market voice, video, or any types of communications-related services tailored to their needs and preferences. NTCA also notes that competition between BIAS providers and over-the-top service providers that offer services will be skewed if some market participants are subject to regulatory constrictions to which others are not. These concerns noted, an opt-out regime for the sharing of CPNI with affiliates that offer communications-related services for purposes of marketing such services would adequately protect consumers' privacy. In contemplating the FTC's recommendation that affiliates generally be treated as "third parties . . . unless the affiliate relationship is clear to

[104] NPRM at para. 121.

[105] NPRM at para. 123.

consumers,"[106] NTCA submits that simple references, rather than actual co-branding, should suffice.

6. Other Purposes

The Commission proposes to require BIAS providers to obtain customer opt-in approval before (1) using customer proprietary information for purposes other than marketing communications-related service; (2) sharing customer "customer proprietary information" with affiliates providing communications-related services for purposes other than marketing those communications-related services; and (3) sharing customer "customer proprietary information" with all other affiliates and third parties.[107]

The Commission seeks comment on whether BIAS providers need or benefit from using "customer proprietary information" "for purposes other than marketing communications-related services.[108] NTCA submits that although its members generally do not use this information for these purposes, the question of "whether BIAS providers need or benefit" approaches only the present tense, when in fact the potential impact on future market needs and practices should be considered. As a first step in addressing this, "communications-related services" must be considered as expansively as are the applications to which broadband may apply. Given the prevalent incorporation of broadband into education, health care, public utilities and economic development, the universe of "communications-related services" is expanding. Therefore, there may well be benefit in the near future of BIAS providers utilizing this information. Certainly, the growing number of app and edge providers that have access to this information underscores how

[106] NPRM at para. 126.

[107] *Id*.

[108] NPRM at para. 127.

deeply disruptive inconsistent regulations for BIAS and other providers with identical access and similar market strategies would be. The Commission should resist what could be characterized as a temptation to expand the CPNI rules, and rather rely upon uniform frameworks of regulation as afforded by a consistent FTC construct. The Commission should limit the inquiry to determine what aspects of BIAS are CPNI, and leave the rest to the able processes of the FTC and applicable local processes.

The Commission seeks comment on the burdens that the proposed opt-in framework for disclosure to third parties would impose on broadband providers, including small providers.[109] NTCA notes again the disparity that would seep into the marketplace as some broadband market participants would be barred from utilizing such information while others might not. Therefore, NTCA suggests that any Section 222-based requirement be grounded in principles of what might equate to an unfair or deceptive practice, and that opt-out opportunities be provided as a safe harbor.

The Commission seeks comment on what effect, if any, its proposed opt-in approval framework would have on marketing in the broadband ecosystem.[110] The Commission articulates concerns noted by NTCA, specifically, that "edge providers, who may have access to some similar customer information, are not subject to the same regulatory framework, and that this regulatory disparity could have competitive ripple effects." Although the Commission explains how these concerns might be mitigated, NTCA submits that the very reasons cited by the Commission actually support the argument that specific Section 222-sourced regulation is

[109] NPRM at para. 131.

[110] NPRM at para. 132.

duplicative and market-skewing in these regards. Starting from the proposition that regulatory parity is an imperative, NTCA frames the Commission's observations in the form of questions.

> *First*, to the extent the FTC "actively enforces the prohibitions in its organic statute against unfair and deceptive practices against companies in the broadband ecosystem that are within its jurisdiction and that are engaged in practices that violate customers' privacy expectations," how are Section 222-sourced regulations aimed at only a segment of that "ecosystem" justified, particularly when the Commission affirms that it has "no doubt that the FTC will continue its robust privacy enforcement practice?"
>
> *Second*, to the extent the industry has "developed guidelines recommending obtaining express consent before sharing some sensitive information, particularly geo-location information, with third parties, and large edge providers are increasingly adopting opt-in regimes for sharing of some types of sensitive information," what justifies specific Section 222-based regulations that place BIAS providers outside of the community of those firms that develop and then implement best practices that best meet the combined demands of consumer interests and legal obligations?
>
> *Third*, *arguendo* edge providers have direct access to only some information, and *arguendo* broadband providers have direct access to potentially *all* customer information, why should different standards be established for access to the same types of information? The Commission's reasoning in this regard implies that only Section 222 can apply a suitably rigorous regime when confronting firms with access to large swathes of data, and would seem to imply a trigger at which an edge provider that acquires a certain amount of information would be subject to Section 222 requirements.

At the least, the situation of small, community-based providers should be considered. The improbable benefits of Commission-specific regulations in a space in which multiple actors dealing with same information are treated differently is illuminated above. And, as noted previously, NTCA members are inextricably linked to the communities they serve and therefore have already have positive incentives to motivate good corporate relationships with their consumers. Accordingly, and in light of the market-tilting outcomes that could be precipitated by treating some actors differently than others, NTCA submits that at most, small providers should

be governed by an the opt-out approval process to the extent that any disparate treatment is bestowed upon various actors in the industry.

NTCA appreciates the Commission's queries regarding different types and contexts of information, and whether there is a risk that customers could be overwhelmed by choice as they navigate various options for different types of information.[111] NTCA submits that standards drawn broadly to apply to communications-related or communications-reliant services be implemented.

The Commission asks whether a broadband provider should obtain some form of consumer consent before combining data acquired from third-parties with information it obtained by virtue of providing the broadband service.[112] NTCA submits that such a requirement would be neither necessary nor useful. A single authorization covering all applicable use should be implemented in order to (a) enable customer ease; (b) facilitate administrative efficiencies; and (c) preempt customer confusion as provider staff presents multiple forms of authorization. Specialized authorization for particular uses could be permitted to the extent a provider wishes to engage in that sort of layered process. But, the threshold requirement should enable any carrier to obtain authorization to use the information, with a general description of what that usage might entail, including combining it with other information to which the broadband provider may have access in order to pursue lawful aims under the rules.

[111] NPRM at para. 135.

[112] NPRM at para. 138.

7. Soliciting Customer Approval

The Commission proposes to require BIAS providers to solicit customer approval the first time that a BIAS provider intends to use or disclose the "customer proprietary information" (to the extent such a category is implemented) in a manner that requires customer approval under its proposed rules.[113] NTCA submits that this recommendation would impose a costly and burdensome requirement among providers who may be required to initiate thousands of individual customers' contacts for authorization that more easily would have been obtained at the point of sale. A one-time, point of sale authorization would not conflict with the Commission's interest in giving customers a "convenient and persistent ability" to express their approval or disapproval of the use or disclosure of their information. And, a standing link on the company's homepage, or a contact number provided in billing statements, could provide an on-going point of contact for customers. Likewise, NTCA does not oppose the Commission's proposal that a customer's choice must persist until it is altered by the customer,[114] but does suggest that the standard "promptly" as proposed by the Commission incorporate consideration of logistical processes necessary to effect the change in the company record and notification to company personnel. Accordingly, NTCA suggests that the standard be revised to "with reasonable promptness consistent with standard industry practices relevant to the incorporation of such information in consumer records and account." NTCA supports the application of voice notice requirements specific to one-time usage of CPNI to BIAS providers' one-time usage of customer

[113] NPRM at para. 139.

[114] *Id.*

information. These enable complete conversations among customers and customer service representatives.

NTCA opposes any requirements that would require a BIAS provider to share information about the entities with which the information might be shared. To the extent providers would be required to notify customers about the *types* of entities with which information might be shared, any requirement that obligates the provider to notify customers of the *specific* entities should be rejected. As business needs and planning evolve, providers may identify an evolving set of entities within any particular class with whom information sharing might be beneficial. Customers may benefit from knowing their data is being shared with communications equipment vendors, but it would be of little benefit to require providers to unleash a list of local and national retail outlets. Moreover, such a requirement would create an ongoing burden were providers required to notify every customer each time a new potential vendor or partner was identified. Sufficient transparency and consumer protection is provided by notifying consumers of the type of information and potential use of it.

NTCA does not oppose providing a link or other direction to the provider's privacy notice at the time approval is sought.[115]

NTCA suggests that the notice provided at a "at a time and in a context that is relevant to consumers"[116] be defined to include the point of sale. Although the Commission questions whether customers might be overwhelmed with other information at that point, NTCA submits that it is precisely at the point of sale at which the customer is digesting all of the material that is

[115] *See, id.*

[116] NPRM at para. 141.

relevant to the plan. In all likelihood, consumers will be less likely to pay attention to subsequently provided material. At the point of sale, consumers are most likely to be focused particularly on requesting information from the carrier about the plan, payment, rates, terms and conditions – including those parameters relating to privacy. And, customers working with a provider representative at that time would be in a natural context in which questions regarding all facets of the service would be posed. Subsequent notices, whether one month, three months or six months down the road are less likely to be given as much attention. NTCA submits the Commission has recognized this in the NPRM question, "Could notices upon use or disclosure contribute to 'notice fatigue' over time, instead of lessening its impact at point of sale,"[117] and proposes that point of sale notice is sufficient. Moreover, such "notice fatigue" would be aggravated were the Commission to require BIAS providers to notify customers of their privacy choices and solicit customer approval at other "prominent points in time."[118] Therefore, NTCA opposes proposals that would require broadband providers to solicit customers' "just-in-time" approval whenever the relevant customer information is collected or each time the broadband provider intends to use or disclose the relevant customer information. Such a requirement would not be only unduly burdensome, but would contribute to "notice fatigue."

NTCA supports proposals that each BIAS provider be permitted to determine the best method for soliciting customer approval.[119] NTCA could support, generally, Commission-recommended methods that could be invoked as a safe harbor.

---

[117] *Id.*

[118] NPRM at para. 142.

[119] NPRM at para. 144.

NTCA supports the proposition that providers may offer customers access to privacy policies and an ability to effectuate related choices through a variety of means, including via telephone or on-line interactions. Providers should have latitude to determine the most effective course of providing notice to their customers through those methods.

8. Documenting Compliance

NTCA supports permitting small providers who have already obtained customer approval to use their customers' proprietary information to grandfather in those approvals,[120] and to allow that authorization to apply to all uses contemplated in the original authorization. NTCA members generally do not share information with third parties, but NTCA nevertheless recommends that if the original authorization extended to include third parties, then the grandfathering provisions apply to those actions, as well, for smaller providers. The Commission proposes to define "smaller providers" as those with 5,000 accounts or fewer.[121] NTCA submits that the Commission has previously relied upon 100,000 (one hundred thousand) or fewer broadband subscribers as reported on Form 477, aggregated over all of the provider's affiliates, when defining "small provider."[122] And, when approaching the same issue, the U.S. House of Representatives identified 250,000 as the proper threshold.[123]

[120] NPRM at para. 151.

[121] *Id.*

[122] Protecting and Promoting the Open Internet: Report and Order on Remand, Declaratory Ruling, and Order, Docket No. 14-28, FCC 15-24, at para. 173 (2015).

[123] *See*, Small Business Broadband Deployment Act, H.R. 4596, 114th Congress (H. Rept. 114-444) (2016).

The Commission asks whether "harmonizing" its existing and proposed rules benefit providers who offer both services.[124] NTCA submits that striving toward consistency among rules is a valuable pursuit, but should not be obtained at the expense of increasing regulatory obligations or decreasing regulatory parity.

9. Use and Disclosure of Aggregate Customer Proprietary Information

NTCA supports generally the Commission proposal to permit BIAS providers to use, disclose, and permit access to aggregated customer proprietary information.[125] NTCA supports the proposition that aggregated information should not be reasonably linkable to a specific individual, but proposes that certain aggregated information relating to the types of devices in the marketplace may be useful while not implicating privacy concerns, and therefore suggests that aggregated information that reveals the *type* of device while not revealing the *user* of that device would not implicate concerns.[126]

NTCA submits that the Commission's proposal that BIAS providers retain documentation regarding their analyses of information that it has treated as aggregate is burdensome and unnecessary.[127] The Commission has already intimated that that the burden of proof will be on provider. Therefore, providers will take steps necessary to ensure that they will be able to defend their practices, as may be necessary. Prescriptive regulations effectively addressing how providers might form that defense are not necessary. NTCA would support a record keeping requirement to the extent it serves as a safe harbor. Similarly, the proposal that

[124] NPRM at paras. 152, 153.

[125] NPRM at para. 154.

[126] *See*, NPRM at para. 157.

[127] *See*, NPRM at para. 159.

BIAS providers be required to publicly commit to maintain and use aggregate customer information in a non-individually identifiable fashion and to not attempt to re-identify the data is of dubious value. BIAS providers are subject to many obligations that are not linked to an affirmative requirement to declare compliance. Providers that are committed to protecting their customers' interests and which discern positive benefits of self-extolling will likely make such comments, anyway.

To the extent the Commission expands current practices and addresses contractual requirements among BIAS providers and third parties, NTCA would not oppose requiring BIAS providers to contractually prohibit any entity to which the BIAS provider discloses or permits access to the aggregate customer data from attempting to re-identify the data.[128] However, such a provision should serve to indemnify the BIAS provider should the third party violate that contract, and in no circumstances should the BIAS provider be required to engage in any form of post-provision monitoring. The point of the contract provision is to recognize the obligations of the third party. NTCA does not oppose the development of a list of identifiers that must be removed from data in order to determine that "individual customer identities and characteristics have been removed,"[129] but cautions that the rapid evolution of technology and the aspects of communications or consumer data from which identifiers can be gleaned may diminish the value of such a list in the future. NTCA therefore suggests that a list would be useful, and certainly so as a safe-harbor, but that providers have flexibility to "de-identify" data in other manners if the provider can demonstrate equivalent effectiveness.

[128] NPRM at para. 161.

[129] NPRM at para. 163.

E. SECURING CUSTOMER PROPRIETARY INFORMATION

1. Industry-Developed Practices, Rather than Prescriptive Mandates, are Best Suited to Securing Networks and Information

The Commission proposes to adopt a general standard and identify specific activities the provider must engage in when securing customer propriety information.[130] The Commission invokes HIPAA, GLBA, Commission and FTC actions, and state laws in this approach.[131] NTCA submits that general FTC principles, rather than industry-specific approaches contained within HIPAA and GLBA, should serve as overriding principles.

NTCA submits that information provided to third parties with the consent of the customer and in conformance with contractual obligations that specify the permitted uses of the information should not remain a snare to the provider. BIAS providers who protect information and who undertake all reasonable measures when releasing the information legally and with specific instruction to the third party should not be held liable for misconduct by the third party. Regarding the Commission's inquiry as to whether "security," "confidentiality," "integrity" indicate three separate duties or are elements of a single overarching duty,[132] NTCA submits they are elements of a single duty. These articulations serve to illustrate the various considerations that must be engaged when the management of confidential information is considered. To the extent, however, that they are elements of a single duty, a provider's shortcoming in one element should not be evaluated to be a shortcoming in all elements.

[130] NPRM at para. 167.

[131] NPRM at para. 168.

[132] NPRM at para. 173.

NTCA supports the proposition that providers must protect their customers' information. NTCA notes, however, that the evolving, dynamic field of communications technology, coupled with the many varied approaches to security and management, argue for flexibility in designing individual provider responses to security.

As NTCA has noted in other venues, the U.S. government, including the Commission, has endorsed the Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 ("the Framework")[133] as the overarching blueprint for current and future cybersecurity efforts by critical infrastructure operators and owners.[134] In turn, the Framework is built on a risk management approach to cybersecurity that enables critical infrastructure operators to identify, assess, and adequately respond to cybersecurity risk. Precise security measures and practices can and should vary, as a given critical infrastructure operator prioritizes the greatest risks to its

[133] *See* "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0, NIST, rel. February 12, 2014, available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[134] Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience," advances a "national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure." Released in tandem with the Presidential Policy Directive, Executive Order 13636 called for the development of a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks – and it asked regulatory agencies to leverage the Framework as appropriate to mitigate cyber risk. *See* White House, Statements and Releases, "Executive Order on Improving Critical Infrastructure Cybersecurity," released February 12, 2013: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0. In addition, in the wake of the release of Framework, the FCC convened its Communications Security, Reliability and Interoperability Council IV Working Group 4 ("CSRIC IV WG4") to adapt the Framework to the communications sector and provide voluntary cybersecurity best practices for industry use. More than 100 industry representatives participated in CSRIC IV WG4, among them NTCA. The CSRIC IV WG4 "Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report" is available at https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

operational needs and functions, and then subsequently determines where and how best to apply resources to minimize, monitor, and mitigate the probability and/or impact of potential cybersecurity events. Critical infrastructure operators of all sizes must be able to retain this flexibility in order to respond to changing marketplace demands and evolving technological capabilities, as well as cyber-based threats. In juxtaposition, a prescriptive approach to cybersecurity would eliminate the innate agility and subsequent security advantages inherent through the use of risk management.

Toward these ends, NTCA agrees with the Commission's proposal to "not . . . specify technical measures for implementing the data security requirements."[135] In similar vein, and consistent with principles articulated previously in these comments, NTCA submits that the proposal to require BIAS providers to establish and perform regular risk management assessments and promptly remedy any security vulnerabilities identified by such assessments[136] is not necessary and is further cost prohibitive and impractical. In the first instance, providers will be sufficiently encouraged to perform regular monitoring and updating in order to conform to their obligations. Further, given the industry's commitment to the development of the Framework, the creation of the accompanying CSRIC IV WG4 guidance, and subsequent outreach and education efforts,[137] BIAS providers of all sizes are already adopting a risk

[135] NPRM at para. 176.

[136] NPRM at para. 179.

[137] As noted in other venues, NTCA remains dedicated to assisting its members in this arena, having embarked upon a comprehensive educational campaign to alert its members to the evolving nature of cybersecurity threats; the need for every communications carrier to adopt a cybersecurity risk management program; and the availability of Federal resources such as the Framework and WG4 guidance. *See, CSRIC IV Cybersecurity Risk Management and Assurance Recommendations: Reply Comments of NTCA*, Docket No. 15-58 (Mar. 19, 2015).

management approach to protecting their critical assets and infrastructure. In addition, regardless of a provider's size, it is unrealistic to assume that the operator can mitigate *all* security risks; in the case of a small, resource-constrained provider, the operator needs the flexibility to prioritize its cybersecurity threats and subsequently implement associated mitigation techniques. Finally, mandating "prompt[]" resolution of problems[138] implicates a figurative dodecahedron of assumptions about unknown situations. Alternatively, NTCA submits that standards relating to time be tied to "reasonable" durations.

Likewise, the Commission should not require specified technical audits.[139] In the first instance, the notion of prescriptive technical measures to address evolving cybersecurity threats risks obsolescence. More generally, however, while a general instruction for risk management can be made, the specifics of how companies do this will depend upon their unique operations and needs. The Commission must remain sensitive to the impact on small businesses, whose networks may warrant a security approach different than that which would be more suitable to a larger firm, consistent with the voluntary, flexible, and scalable approach to cybersecurity as first espoused by the Framework, and then subsequently by the Commission's CSRIC IV WG4.[140] At best, the Commission may consider specific criteria that can be included in a safe harbor.[141] These criteria may include the frequency of risk assessments,[142] but consistent with the

[138] NPRM at para. 184.

[139] NPRM at para. 181.

[140] The CSRIC IV WG4 Report contains specific implementation guidance for small and mid-sized businesses within the communications sector which invokes a voluntary, flexible, and scalable risk management approach: https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[141] *See*, NPRM at para. 182.

[142] *See*, NPRM at para. 183.

recognition of individual company needs coupled with technological evolution, the Commission should limit prescriptive specifics to voluntary safe harbors.

As described above, industry has undertaken numerous steps in good faith and in concert with Federal bodies to identify and design industry best practices. These measures consider consumer safety, cyber-security, technical implications and a balance of needs that arise respectively from the provider, user, law enforcement and regulatory communities. Moreover, these efforts incorporate an implicit recognition that technology and threats to compromise networks and information are evolving rapidly and will require tailored and individualized approaches that best meet the need of each provider and its consumers. Prescribed administrative, technical, and physical conditions will likely fail to be as effective as best practices that are developed by the industry in concert with market developments. At most, prescribed conditions could serve only as a safe harbor for providers, thought the efficacy of such an approach as compared to industry-developed best practices remains in question.

Each firm is best suited to identify the processes best suited to ensuring compliance. BIAS providers committed to lawful protection of customer information will necessarily train their employees, agents, and contractors that handle "customer proprietary information." The Commission's proposal that providers "sanction[]" employees, agents, or contractors for violations of security measures[143] is wholly unnecessary and unreasonably nettlesome. The matter of employee discipline is within purview of company management; the Commission's recommendation begs the question of whether an affirmative implementation of this proposal would include specification of financial penalties or other disciplinary measures. Similarly, the

[143] NPRM at para. 185.

Commission should refrain from implementing requirements that speak to the specific credentials possessed by any senior management official overseeing the implementation of these policies.[144] The Commission would be ill-placed to prescribe the various academic degrees or years of experience, or any other innumerable qualifications such a manager might be required to possess.

The imperative to enable providers to select the methods best suited to their markets and companies extends to other of the Commission's proposals, as well. To wit, the Commission should permit providers the flexibility to determine how they will best protect consumer data (and their own liabilities), and should refrain from imposing multi-factor authentication requirements.[145] For small providers like NTCA members, especially, these prescriptions would be unnecessary in many instances in which the providers and their staff know personally many of the customers. Where necessary, potential liability is sufficient incentive to encourage suitable measures. Moreover, the continuing debate on the usefulness of passwords and other personal security protocols as relate to data lead to a conclusion that a flexible approach is best suited to the dynamic industry. Already, many private firms and operators mandate requirements for password composition, based upon their perception of best practices within that context. The Commission should likewise leave the BIAS industry to assess and implement the most suitable measures necessary to meet market and customer expectations. As the Commission comments on whether it should harmonize the existing authentication requirements for voice providers with the authentication method it might ultimately adopt for BIAS providers,[146] the finer tuned

[144] *See*, NPRM at para. 190.

[145] *See*, NPRM at para. 192.

[146] NPRM at para. 200.

question is whether the BIAS rules should simply be made consistent with existing CPNI requirements. These requirements are already robust, as illustrated by the Commission's acknowledgement that requiring BIAS providers to notify customers of account changes would be consistent with existing requirements to "notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed."[147] However, NTCA notes that the providers should not be required to inform customers of *unsuccessful attempts* to change passcodes, since that could precipitate an unending cycle of notices to customers as security measures prove their effectiveness. These notices could well cause "notice fatigue" and ultimately discourage notice of messages that impart actually important information. These would be especially burdensome to small providers who would need to divert resources from protecting data to informing customers of unsuccessful attempts to compromise that data. Providers who notice consistent and persistent attempts to unlawfully access the account of a particular subscriber may be inclined from a customer service perspective to notify that customer of those specific circumstances. In that limited regard, notification of so-called "false positives" may be useful. In contrast, notifying every customer of every failed attempt would be of comparatively little value.

2. Customer Access to Customer Proprietary Information

NTCA opposes any recommendations that providers be required to provide customers with access to all "customer proprietary information" in their possession, including all CPNI, and a right to correct that information.[148] In the first instance, information generated by users by

[147] NPRM at para. 200.

[148] NPRM at para. 205.

definition initiates with the user; there is no compelling reason to cast the BIAS provider as a librarian whose job is to collect, collate and provide upon request that information back to the user. Moreover, it is not clear that information within the possession of the provider would be in format that is usable to the customer, and in all instances any recommendation that a provider be required to convert its records into other formats should be rejected.[149] The Commission notes correctly that "edge providers, data brokers, and other entities in the Internet ecosystem also collect, process, retain, and distribute large quantities of sensitive consumer data."[150] BIAS providers should be subject to no greater nor lesser form of requirements in these regards. The Commission has oft stated the need for competition in the broadband marketplace, and regulatory disparity among those with access to same information should be eschewed.

3. Accountability for Third Parties

Providers that effect proper contractual agreements with third parties should not be liable for the failings of those third parties.[151] The proposal that BIAS providers be held accountable for third party recipients' handling of "customer proprietary information" for the entire lifecycle of the data, or even any duration of it once it properly leaves the hands of the provider, should be rejected. Providers that take reasonable steps to protect data will undertake due diligence in their selection of partners; instances in which a breach cannot be tied to negligence or unreasonable practice on the part of the broadband provider should not create an actionable liability for that provider.

[149] NPRM at para. 206.

[150] *Id.*

[151] *See*, NPRM at para. 210.

NTCA supports the Commission's recognition that security measures employed by a BIAS provider should take into consideration the nature and scope of the BIAS provider's activities.[152] Likewise, NTCA supports the Commission's proposal that the security measures a BIAS provider employs should consider the sensitivity of the underlying customer information.[153] These are consistent with the recognition that so-called "one size fits all" solutions are not suited to a dynamic marketplace in which providers undertake industry-driven efforts toward best practices.

4. Destruction of "Customer Proprietary Information"

The Commission seeks comment on whether it should implement specific measures for BIAS providers when disposing of "customer proprietary information."[154] NTCA supports an FTC-like approach, which would offers a non-exhaustive list of such reasonable measures that includes burning, pulverizing, or shredding paper so that they are unreadable and cannot be practicably reconstructed and destroying or erasing electronic media such that it cannot be practicably read or reconstructed.[155] The Commission must ensure that any requirements do not impose costly or burdensome obligations on small providers. In all likelihood, these costs would be absorbed into the general "cost of doing business" and would be borne ultimately by consumers. Accordingly, the Commission should enable the market, and particularly small providers, to identify the most suitable methods for data destruction.

[152] NPRM at para. 217.

[153] NPRM at para. 218.

[154] NPRM at para. 230.

[155] *See*, NPRM at para. 230.

F. DATA BREACH NOTIFICATION REQUIREMENTS

1. Customer Notification

The Commission proposes to require BIAS providers and other telecommunications carriers to notify customers of breaches of "customer proprietary information" no later than 10 days after discovery of the breach, absent a request by Federal law enforcement to delay customer notification.[156] NTCA supports various limitations and nuances that will ensure this rule meets its goal. For example, breach reporting requirements should be based on the likelihood of misuse of the data that has been breached or of harm to the consumer. Providers should not be required to consult with Federal law enforcement when determining whether there is a reasonable likelihood of harm or misuse.

The timing of notifications should similarly be calibrated to the particular type of misuse or harm.[157] Providers should have a reasonable and appropriate amount of time to conduct investigations, and the duration of those periods will depend upon the particular circumstances of any event. In fact, the existing Section 222 rule does not specify how quickly affected customers must be notified of a data breach involving CPNI. While earlier notice could potentially enable customers to take action, a longer time-frame could give the provider sufficient time to determine the cause of the breach or other factors with greater certainty. Moreover, "discovery" of the breach must be defined as "a reasonable understanding of the nature and scope of the breach." Such notice would accommodate a sensible standard of "without unreasonable

[156] NPRM at para. 236.

[157] *See*, NPRM at para. 238.

delay,"[158] which contemplates the many facets that may attend a breach. The Commission should not impose obligations relating to conduct that would reasonably lead to exposure of "customer proprietary information."[159] Rather, providers noting potential developments on their end will be motivated sufficiently by their legal obligations to update any processes, while providers with insight into customer practices may well be encouraged to seize the initiative and obtain good-will by alerting the consumer.

NTCA submits that the Commission's recommended contents of breach notification are sufficient. They are:

> The date, estimated date, or estimated date range of the breach;
>
> A description of the "customer proprietary information" that was used, disclosed, or accessed, or reasonably believed to have been used, disclosed, or accessed, by a person without authorization or exceeding authorization as a part of the breach of security;
>
> Information the customer can use to contact the telecommunications provider to inquire about the breach of security and the "customer proprietary information" that the carrier maintains about the customer;
>
> Information about how to contact the Federal Communications Commission and any state regulatory agencies relevant to the customer and the service; and
>
> Information about national credit-reporting agencies and the steps customers can take to guard against identity theft, including any credit monitoring or reporting the telecommunications provider is offering customers affected by the breach of security.

NTCA concurs that "[s]ervice providers should be in the best position to know how to reach their customers with important notifications."[160]

---

[158] *See*, NPRM at para. 241.

[159] *See*, NPRM at para. 242.

[160] NPRM at para. 244.

2. Notification to Federal Law Enforcement and the Commission

The Commission proposes to require telecommunications providers to notify the Commission no later than seven days after discovering any breach of "customer proprietary information", and to notify the FBI and the Secret Service no later than seven days after discovery a breach of "customer proprietary information" reasonably believed to have affected at least 5,000 customers.[161] With regard to Federal law enforcement notification, the Commission requires that such notifications occur at least three days before a provider notifies its affected customers, unless law enforcement directs the provider to stand down from that notice.

NTCA suggests that proposed threshold of 5,000 affected customers for reporting requirements should *at the least* be aligned to states that have a minimum threshold of 10,000 affected customers for reporting to the consumer reporting agencies; alternatively, and more preferable, aligning the rule to incorporate respective local requirements will help ensure that consumers receive timely notification by establishing a uniform code of conduct for providers who will look toward a single threshold trigger for both notifications.[162] NTCA disagrees with the Commission's proposal that it be notified of all data breaches.[163] It is not likely that scattered reports of single breaches from across the country will provide the Commission with "a strong indication to Commission staff about existing data security vulnerabilities that Commission staff can help providers address through informal coordination and guidance."[164] It is not clear that the value of these disparate reports would approach the Commission's cost in collecting,

[161] NPRM at para. 246.

[162] NPRM at para. 245.

[163] NPRM at para. 248.

[164] NPRM at para. 248.

categorizing, and cataloguing the information. And, this is apart from any resources the Commission would spend considering the information. A single breach may be the result of an administrative error, unfortunate happenstance, or some other condition wholly unrelated to any significant or meaningful data that would inform the Commission process. Rather, the rules should require notification of breaches that implicate a defined number of customers, or a defined proportion of a provider's customers.

The Commission should reject the proposal to require notice when the telecommunications provider discovers conduct that would reasonably lead to exposure of "customer proprietary information."[165] All firms occasionally encounter the moment at which they discern an opportunity to improve a process. There should be no on-going obligation of providers to report every possible miscue or near-miss.

3. Third-Party Data Breach Notification

NTCA supports proposals that BIAS providers contractually require third parties which they share "customer proprietary information" to follow the same breach notification rules adopted for BIAS[166] *only* if that requirement indemnifies the BIAS provider from liability should a breach occur. Generally, third parties that are not subject to the jurisdiction of the Commission should not be "bootstrapped" to Commission regulations by dint of contract. To the extent, however, that any policy would attempt to accrue a third party's improper actions to the BIAS provider, however, opportunities to preempt that outcome by contract would be desired. The proper contractual agreement defining accepted use of the information under the terms of the

[165] NPRM at para. 250.

[166] NPRM at para. 255.

agreement ends the BIAS provider's liability, and commences the responsibility of the third party. The Commission's proposal in this regard underscores again the difficulty of imposing upon one industry standards to which others utilizing the same information in the same manner are not held.

G. PRIVACY REQUIREMENTS AND CUSTOMER RELATIONSHIPS

The Commission seeks comment on whether there are certain BIAS provider practices implicating privacy that our rules should prohibit, or to which we should apply heightened notice and choice requirements. In particular, the Commission proposes to prohibit the offering of broadband services contingent on the waiver of privacy rights by consumers, and seeks comment on, *inter alia,* practices involving the offering of higher-priced broadband services for heightened privacy protections.

NTCA does not oppose disallowing practices that enable providers to deny service if customers do not relinquish certain rights. However, NTCA supports fully the proposition that price variances can be implemented for varying degrees of access to information. In the first instance, the relaxation of certain procedures for a customer base can decrease various operational costs, and those benefits should be permitted to flow to the customer. Moreover, many customers may be less sensitive to certain data than others, and they should not be proscribed from enjoying benefits that may be offered in regard thereto. In these regards, there is no need to create "privacy protection seals," since those could be interpreted to imply that providers who are acting fully within legal bounds, are not.[167] Providers should have the flexibility, within the boundaries of notice, choice and security, to offer consumers packages that

[167] *See,* NPRM at para. 257.

meet their needs. Financial inducement packages are fundamentally no different than any other discount offered by any manner of firms in exchange for an offering of the consumer. The Commission itself recognizes "[i]n the brick-and-mortar world, loyalty programs that track consumers purchasing habits and provide rewards in exchange for that information are common."[168] The imperative of FTC "fair practices" ensures for the customer the obligation of the provider in these regards to provide clarity; the Commission here must ensure parity.

III. CONCLUSION

As described above, rules based upon Section 222 should hew to the language and intent of the statute and address those aspects of BIAS that arise specifically out BIAS. Other data sets that are common to both BIAS and other firms, include edge and app providers, should be governed by a uniform standard rooted in the FTC Act. This will ensure that consumers enjoy a uniform expectation of privacy, and that regulatory parity among market players will enable a level field of competition.

Respectfully submitted,

By:
/s/ Joshua Seidemann
Joshua Seidemann
Vice President of Policy
4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203
jseidemann@ntca@ntca.org
703-351-2000 (Tel)

[168] NPRM at para. 260.