September 16, 2016

***Ex Parte* Notice**

Marlene Dortch, Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: ***Protection the Privacy of Customers of Broadband and Other Telecommunications Services,* Docket No. 16-106**

Dear Ms. Dortch:

On Wednesday, September 14, 2016, Brian Ford and Jesse Ward of NTCA–The Rural Broadband Association (NTCA), along with the undersigned, met with Matthew DelNero, Lisa Hone, Daniel Kahn, and Sherwin Siy of the Wireline Competition Bureau (WCB); Melissa Kirkel of the WCB participated by telephone. NTCA addressed several issues implicated by the above-captioned proceeding, and explained the potential impact on the small, facilities-based rural broadband provider members of NTCA.

At the outset, NTCA reiterated its commitment to data protection. NTCA explained that its concerns are rooted in both the type of information the Commission proposes to protect, and the manner in which data could require protection. NTCA's perspectives were informed by a plain reading of the Notice of Proposed Rulemaking (NPRM) in this docket and the breadth of issues upon which the Commission sought comment. NTCA proposed that Commission rules recognize the difference between: (1) data that is analogous to that which is protected currently under Customer Proprietary Network Information (CPNI) rules and is uniquely available to telecommunications carriers (including broadband Internet access service providers), and (2) other data that is typically available to multiple kinds of entities in the Internet ecosphere and already subject to other kinds of protections and frameworks. In these regards, an approach that mirrors current CPNI rules would govern information within category (1), above; the expanded universe of data that is consistent with category (2), above, would be managed under a rubric of a standard consistent with the approach of the Federal Trade Commission (FTC)- that looks toward unfair or deceptive practices; and, data security obligations, generally, would be grounded in standards arising out of those same FTC principles, and whose articulation would be consistent with the approaches of the NIST Cybersecurity Framework and CSRIC IV Working Group efforts.

NTCA–The Rural Broadband Association
4121 Wilson Boulevard, Suite 1000, Arlington, Virginia 22203
(703) 351-2000 (Tel) ● (703) 351-2001 (Fax)

Opt-In

As a threshold consideration, NTCA proposed that broadband Internet access service (BIAS) providers should not be prohibited from acting in a manner that is permitted to other firms in the broadband ecosphere.[1] Significant data sets purported to be protected by the proposed category of personal identifiable information (PII) are either publicly available or accessed by and available to edge and application providers. NTCA explained its interest in avoiding regulatory disparity among BIAS providers and edge/application providers who have access to the same information.

Toward this end, NTCA explained the "opportunity costs" to its members if an opt-in regime that limits the ability of a BIAS provider to share information among affiliates is adopted. The proposal to require opt-in authorization could stymie NTCA member efforts to market services that are related to the core broadband offering, including, but not limited to, technical support, hardware/software systems, and alarm/security monitoring services. NTCA explained that the perception of what is a "communications related service" is expanding and evolving as education, health care and economic development all become more deeply entrenched in and enabled by broadband. Customers expect fairly a broadband provider to share with them the full scope of offerings that can be accessed and augmented by the core Internet access service. NTCA therefore suggested an approach that enables BIAS providers to share information with affiliates in order to promote services that rely upon the broadband offering.

Data Security

NTCA explained its concerns with the data security requirements set forth in the NPRM. NTCA's understanding of the potential impacts was informed by the broad set of possibilities upon which the Commission sought comment.

NTCA emphasized its and its members' commitment to the protection of networks and customer data. NTCA described its commitment to the evolutionary development of voluntary industry standards and practices that meet the changing face of technology and threats, rooted in the development of the NIST Cybersecurity Framework, NTCA's role as a co-lead for the CSRIC IV Working Group 4 Small and Mid-Size Business Group (CSRIC IV WG4 SMB Group), and its on-going efforts to further member awareness and education.

As a starting point, NTCA explained its principal philosophy that perfect security can be neither promised nor obtained. Rather, the driving goal in network security, as the NIST Framework rightly observes, is to identify, assess and prioritize cyber risks, mitigate threats, and respond rapidly and in an on-going manner to manage a company's cybersecurity preparedness in an ever-evolving environment. NTCA explained that voluntary industry efforts such as those crafted by CSRIC IV WG 4 are best-suited to respond rapidly and flexibly to technological and threat developments. Finally, NTCA emphasized that economic feasibility is a core aspect of the

[1] By way of illustration, NTCA refers to its comments which describe the extent to which broadband-related firms that are not regulated by the Commission access and use consumer data subject to Federal Trade Commission principles. *See NTCA Comments* at pp. 8, 9.

CSRIC IV WG4 approach. Indeed, CSRIC IV WG4 acknowledged that small and mid-size communications operators face significant resource limitations and additional challenges to security implementation, and therefore included a sub-group effort focused on providing scalable and flexible guidance to small businesses within the sector. At a minimum, these same tenets of economic flexibility, scalability and feasibility must similarly attend the Commission's examination of network security practices.

NTCA explained its understanding, based upon the NPRM, that the expanded universe of data envisioned in the proposed rules (including, but not limited to, the new category of PII) could require providers to implement new protocols that may include new hardware and software to monitor every transaction and transportation event, *i.e.*, data stored and data in transit. NTCA described certain of the estimates that its members developed in response to the possibilities opened by the NPRM.

By way of example, NTCA referenced the expense of retrofitting networks with "air gap" security measures. NTCA explained the experience of one its members, whose subscribers cannot access the corporate network without a specific access solution, but whose computers and devices that help manage and support the network can access customer data. NTCA noted that if the Commission's network security guidelines would effectively require an "air gap," then a large and expensive retrofitting would be required for this company, which already maintains a logical separation of traffic among its BIAS and corporate network, with traffic mediating devices such as firewalls and access control lists in place.[2]

NTCA also discussed potential encryption requirements. NTCA explained that the costs of encryption depend upon *when* the data must be encrypted, and *what data* must be encrypted. Encrypting data before it is transported over the network increases complexity over encryption that occurs when the data is stored. And, if all data, including personal information such as name, address, telephone numbers and email addresses (*i.e.*, such as included in the new category of PII) require encryption, then the costs could reach hundreds of thousands of dollars, if not into the millions, for a multi-exchange, multi-city company.[3] To supplement the examples that NTCA shared with Staff at the meeting, the following are provided for consideration in these regards:

> *Example 1:* An NTCA member estimates that the task of working with vendors to encrypt all databases and communications between clients and servers, as well as spreadsheets that are created, maintained and shared internally and externally would implicate a five-to-six digit dollar impact for a company with a staff of about 70.
>
> *Example 2:* An NTCA member predicts that the task of implementing encryption processes across a network of many connections and many storage databases could take

[2] Specifically, this company serves nine exchanges with a population density that ranges between 2.5 to 12.5 people per square mile.

[3] These possibilities, specifically, requirements to encrypt data in transit and storage and against which NTCA would advocate, could be inferred from the NPRM's broad inquiries regarding protection of PII against all cyber risks, regardless of whether a specific mandate to do so is included.

at least five years to work with the various equipment and software vendors to replace systems or incorporate changes into existing systems.

Example 3: An NTCA member reported that it already segments its external ISP network from the internal corporate network, but that if that had not already been done, it would cost tens of thousands of dollars in equipment and labor. However, a requirement to segment customer information on its own network at both the corporate and ISP level could run into the hundreds of thousands of dollars.

Example 4: An NTCA member with approximately 10,000 access lines and 7,500 fixed (wired) broadband accounts estimates that initial steps to implement the security requirements of the NPRM would reach about $100,000 in initial investment and $10,000 annually in service contracts. Software to automate various security processes is estimated at an additional $20,000 initial investment with annual service fees to follow.

Beyond the discrete costs of equipment and implementation measures, NTCA explained that the breadth of proposals in the NPRM triggered concerns among its members that requirements could also short-circuit anticipated replacement cycles for existing equipment. Although the companies currently engage network security costs, a comprehensive transition that imposes a "*supra*-CSRIC" environment would implicate equipment as varied as firewalls and bandwidth detectors. Every segment of the network, from the corporate LAN to branch offices, could require replacement. "Bolt-on" solutions may or may not be available. Up-front costs would include substantial capital investments, and could include multiple software stacks if integrated solutions are not available. Expanded maintenance costs would also arise. Subscription services costs would increase. The burden on small providers (and, by extension, their customers) would be excessive, and would include little margin for relief that might be obtained by larger providers who can exercise negotiating latitude through large-scale purchasing. These expenses would be compounded further where no economies of scale would be realized through the application of new standards to relatively small customer bases.[4] Avalanches of new costs would predictably be avoided if companies continued to apply industry-established guidelines that contemplate a balance of risk mitigation and economic feasibility.

In its discussion with Staff, NTCA emphasized the usefulness, suitability, and appropriateness of a CISRIC-based approach to network security. However, NTCA noted twin core values of CSRIC: (a) the industry-driven nature of the program that enables rapid flexibility to respond to evolving technology and threats, and (b) the recognition that economic feasibility plays a determinative role in managing risk. As described above, the potential burden on small providers must be considered within this topic.[5]

[4] These data support the positions expressed in NTCA's Reply Comments regarding the analyses required by the Regulatory Flexibility Act.

[5] In paragraph 169 of the NPRM, the Commission offers that its proposals are intended to be "calibrated to the nature and scope of the BIAS provider's activities, the sensitivity of the underlying data, and technical feasibility." NTCA appreciates and agrees with the need to calibrate requirements to risk.

Liability for Third Party Actions

NTCA expressed its concerns that BIAS providers should not be subject to liability for acts of a third party where the provision of data was undertaken lawfully and with legally sufficient guidance as to appropriate use.

Conclusion

In summary, NTCA reiterated its positions that to the extent the Commission crafts new rules, the ultimate standard for small companies must be grounded in the principles that NTCA set forth in its comments: an FTC standard focused on avoiding unfair and deceptive practices that is consistent with the NIST Cybersecurity Framework and the subsequent CSRIC IV WG4 approach. This approach must contemplate the economic feasibility of any measure. When something becomes technically or economically feasible, then *not* engaging that process could, in fact, be an unfair or deceptive practice.[6] But, until that practice becomes technically *and* economically feasible (which may exist on a sliding scale, depending on whether a large national firm or a community co-op is involved) there is insufficient basis to require the practice.

Therefore, and without waiving any legal claims that NTCA may assert in regard to the above-captioned docket, NTCA proposes that to the extent the Commission introduces new requirements, any rules must include a standard of financial feasibility, as well as a sufficient deferral period so that the tasks and costs of implementation can be evaluated prior to the imposition of new requirements on smaller providers.

Respectfully submitted,

/s/ *Joshua Seidemann*
Joshua Seidemann
Vice President of Policy

cc: Matthew DelNero
Lisa Hone
Daniel Kahn
Melissa Kirkel
Sherwin Siy

However, NTCA notes that the Clean Water Act standards (cited by the NPRM at footnote 321 as the issue of calibration is discussed) explicitly include "economic feasibility." NTCA urges the Commission to similarly recognize explicitly the issue of economic feasibility.

[6] *See, i.e., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 326 (3d. Cir. 2015).