October 20, 2016

***Ex Parte* Notice**

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

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

Dear Ms. Dortch:

On Tuesday, October 18, 2016, the undersigned, along with Jill Canfield and Jesse Ward on behalf of NTCA–The Rural Broadband Association ("NTCA"),[1] as well as Jefferson England, Chief Financial Officer with Silver Star Communications in Freedom, Wyoming ("the Rural Representatives"), met with Stephanie Weiner, Senior Legal Advisor to Federal Communications Commission ("Commission") Chairman Tom Wheeler and Lisa Hone, Wireline Competition Bureau Associate Bureau Chief. The parties discussed NTCA's position in this proceeding as set forth in its comments and reply comments filed in the docket, as well as the "Fact Sheet"[2] as released by Commission on October 6, 2016.

The Rural Representatives highlighted several key issues in the discussion:

1. The Commission should seek to adopt regulations in this proceeding that are consistent across the board as to *all* industry actors with access to substantively similar (if not identical) data; regulatory disparity and ensuing customer confusion must be avoided.

2. As opt-in requirements may be implemented for certain sensitive sets of data, those requirements should neither initiate nor perpetuate regulatory disparity.

[1] NTCA represents nearly 900 rural rate-of-return regulated telecommunications providers ("RLECs"). All of NTCA's members are full service local exchange carriers and broadband providers, and many of its members provide wireless, cable, satellite, and long distance and other competitive services to their communities.

[2] "Fact Sheet: Chairman Wheeler's Proposal to Give Broadband Consumers Increased Choice Over their Personal Information." (rel. Oct. 6, 2016) (http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1006/ DOC-341633A1.pdf) (last viewed Oct. 13, 2016, 9:27) (Fact Sheet).

3. Voluntary industry guidelines to address data security that incorporate scalability, flexibility, and technical and economic feasibility are best suited to respond effectively to evolving threats.

4. A sufficient delayed implementation period should be established for small providers.

Consistent Form of Regulation

NTCA noted at the outset the commitment of its members to safeguard the privacy of their customers' data. Toward that end, and as set forth in NTCA comments and reply comments, privacy rules for Internet service providers ("ISPs") should focus on those data sets that arise solely out of an ISP's provision of broadband Internet access service, similar to the narrow scope of customer proprietary network information ("CPNI") that is protected under Section 222 in the telephone environment. Other data that are substantively similar (and in many instances identical) to that which are available to edge and application providers and other firms should be treated according to a standard that is consistent with Federal Trade Commission ("FTC") principles to which those other firms are subject. The Commission's proposal, as reflected in the Fact Sheet description that "web browsing history" and "app usage data" would be included in information that would be subject to opt-in requirements would depart from that principle, as edge and application providers rely routinely upon web browsing and app usage information to market goods and services. The Commission should avoid regulatory disparity that is unequally applied to market participants and confusing to consumers.

In addition, opt-in requirements for broadly construed data sets will impede ISP and customer opportunities to enjoy the full advantages of services including those that are related to the core broadband offering such as technical support, hardware/software systems, and alarm/security monitoring services. As critically, if not more so, the Commission must ensure that the categories of information that are subject to opt-in authorization neither impede nor disrupt an ISP's ability to share information with an affiliate or a third party for billing or other similar functions without the need to obtain opt-in authorization. The Commission must ensure that billing, management, operational and other support are included within the set of functions that are defined as "necessary to provide the service." This is crucial for small providers that may outsource certain of these functions to affiliates or third parties.

Breach Notification Procedures and Triggers

The Rural Representatives further noted their support for common-sense breach notification rules of the type discussed in the Fact Sheet. Specifically, the Rural Representatives stated that while it is indeed critical to ensure that both affected customers and law enforcement are notified as promptly as possible of any data breach, market forces and consumer expectations already operate as a strong incentive on ISPs to promptly inform their customers. With respect to the definition of "breach," the duty to inform customers of data breaches should calibrated to the sensitivity of the data and enable ISPs to notify customers only to the extent that harm is reasonably likely to occur. Additionally, because mitigation of a security breach should be the ISP's primary concern, a "soon as is reasonably practicable" standard for the timing of notification to customers after a breach is discovered is preferable to a rigid time frame.

Data Security

With respect to the data security provisions at issue in this proceeding, the Rural Representatives first noted that perfect network security can be neither promised nor obtained. The driving goal in network security matters is to create a situation that is less imperfect. Voluntary industry guidelines that recognize and incorporate scalability, flexibility, and economic feasibility are best suited to respond effectively to technological and threat developments. To the extent that any guidelines are deemed necessary with respect to data security, they should explicitly note the voluntary, flexible nature of the NIST Cyber Security Framework (including the work of CSRIC IV and its working groups), and they should also include the establishment, implementation and maintenance of reasonable physical, technical and administrative security safeguards that contemplate the volume and sensitivity of the data held by the ISP.

From the perspective of a company operating in a difficult to serve rural environment, Mr. England explained that his small, rural company has been a proactive early adopter of the NIST Cybersecurity Framework, using the Framework to assess and then mitigate cyber risks to its critical assets, infrastructure, and services. As Mr. England explained, the Framework is a tool that allows a small operator to evaluate threats to its network relative to its current cybersecurity posture, and then create a long-term plan – in context of what is technically and economically feasible for the company – to either reduce the likelihood of or consequence of those threats occurring, or transfer the risk to another entity such as a vendor, consultant, or insurance provider.

With that said, the Rural Representatives expressed their appreciation that the Commission recently modified its approach to data security (in the recently released Fact Sheet) to an approach that tracks more closely with the FTC's approach to "reasonable" data security. NTCA also expressed an appreciation that the Commission understands the importance of cybersecurity risk management and its advantages over a traditional, prescriptive checklist. However, given the need for scalability, flexibility, and individual adaptions of the Framework based upon technical and economic feasibility, voluntary industry guidelines and a public-private collaboration approach are best suited to respond effectively to evolving threats. To the extent that any guidelines are deemed necessary with respect to data security, NTCA reiterated specific and explicit reference to "economic feasibility" when determining what measures are either necessary or considered "reasonable."

Delayed Implementation Period for Small Providers

As described in the NTCA advocacy in this proceeding and as supported by small cable and wireless providers,[3] a delayed implementation schedule for small ISPs that will accommodate a sufficient period to gather information about the impact of the rules on larger providers should be

[3] *See*, Letter from Thomas Cohen, Counsel to American Cable Association, to Marlene H. Dortch, Secretary, Federal Communications Commission, WC Docket No. 16-106 (Oct. 18, 2016), p. 3; Letter from Rebecca Murphy Thompson, Competitive Carriers Association to Marlene H. Dortch, Secretary, Federal Communications Commission, WC Docket No. 16-106 (Oct. 13, 2016), p. 1.

provided. This delayed implementation will also accommodate market demands on network security products that could increase prices during the initial period of implementation; these market forces would be particularly burdensome for small providers who lack negotiating power. Moreover, implementation of a new regulatory regime for small businesses will be aided by observing and learning from the experiences of larger firms who are by virtue of their size and scale are better positioned to absorb the learning curve. The period of observation will be useful to the Commission, as well, in determining whether additional tailoring of requirements for small providers is warranted. NTCA notes that the incorporation of a "reasonableness" standard alongside recognition of technical and economic feasibility can provide substantial guidance in these regards. In addition to the issues highlighted above, NTCA also addressed the usefulness of safe harbor or other guidance for providers that offer discounted service rates in exchange for customers' allowances to access and use data. NTCA also discussed the need to provide smaller providers with a notification period deadline longer than seven (7) business days as reflected in the Fact Sheet. For small companies with limited staff, that time can be consumed by initial inquires to determine the scope and extent of the breach, and whether, in fact, a reportable breach has occurred. NTCA staff noted that even the largest of commercial firms and government entities often need extensive time to identify and determine the parameters of a suspected breach. An extended period for small providers would enable greater confidence in the usefulness and accuracy of such reports

Thank you for your attention to this correspondence. Pursuant to Section 1.1206 of the Commission's rules, a copy of this letter is being filed via ECFS.

Sincerely,
/s/ *Brian Ford*
Brian Ford
Senior Regulatory Counsel

cc: Stephanie Weiner
Lisa Hone