October 14, 2016

Ex Parte Notice

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

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

Dear Ms. Dortch:

On October 13, 2016, Jesse Ward, Industry and Policy Analysis Manager, and the undersigned of NTCA-The Rural Broadband Association (NTCA) met with Amy Bender, legal advisor to Commissioner Michael O'Rielly, to discuss the above-captioned proceeding. In this discussion, NTCA referred to its comments and reply comments filed in the docket, as well as the "Fact Sheet"[1] as released by the Federal Communications Commission (Commission) on October 6, 2016. NTCA highlighted several key issues in the discussion. They included:

1. The imperative to ensure that a consistent form of regulation should apply to all firms with access to substantively similar (if not identical) data; regulatory disparity and ensuing customer confusion should 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.

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 deferral period should be established for small providers.

These principles were discussed at the meeting, consistent with the report provided below:

[1] *See,* "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).

Consistent Form of Regulation

NTCA recognizes the need to guard the privacy of user information. 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 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 unfair to market participants and confusing to consumers.

Particularly, 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 gambit 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.

Data Security

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. Although the Commission has discussed considerations based upon the size of an ISP, NTCA urges specific and explicit

reference to "economic feasibility" when determining what measures are either necessary or considered "reasonable."[2]

De-identified Information

In regard to de-identified information, NTCA discussed the proposed inclusion of a standard that would require ISPs to "[a]lter the customer information so that it can't be reasonably linked to a specific individual *or device."*[3] NTCA is concerned that this standard would require ISPs to treat IP and MAC addresses as protectable information.

In initial comments, NTCA explained that the Commission's comparison of IP addresses to telephone numbers in the voice telephony context is of limited application.[4] NTCA explained that 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 offenses could be addressed under applicable laws. The source IP address information *per se,* however, should not be protected information.

Regarding MAC addresses, NTCA explained in its initial comments that MAC addresses are assigned to network adapters, and do not reliably identify either users or a particular user's equipment:

> 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.[5]

De-identified information that could be reassembled to identify a device but not the user should not fall within the gambit of protection the Fact Sheet supposes. As NTCA stated in initial comments,

> 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

[2] Certain of the sources cited by the Commission in the NPRM include economic feasibility. *See, i.e.,* fn. 321, discussing Clean Water Act standards of the "best available technology economically achievable."

[3] *See,* Fact Sheet at 3 (emphasis added).
[4] NTCA Comments at 20.
[5] *Id.*

> 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.[6]

Deferral Period for Small Providers

As described in the NTCA reply comments, 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 provided.[7] 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.[8] 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.

Pursuant to Section 1.1206(b) of the Commission's Rules, this letter is filed for inclusion in the public record of the above-captioned proceeding.

Respectfully submitted,

/s/*Joshua Seidemann*
Joshua Seidemann
Vice President of Policy
NTCA–The Rural Broadband Association

cc: Amy Bender

[6] NTCA Comments at 53.
[7] Reply Comments at 14, 15.
[8] Fact Sheet at 4.