



*James J.R. Talbot*  
Executive Director-  
Senior Legal Counsel

AT&T Services, Inc.  
1120 20<sup>th</sup> Street NW Ste. 1000  
Washington, D.C. 20036

Phone: 202.457.3048  
Fax: 202.463.8066  
E-mail: [jjtalbot@att.com](mailto:jjtalbot@att.com)

August 23, 2016

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12<sup>th</sup> 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 August 19, 2016, Chris Boyer, Jeff Brueggeman, Joe Marx, Jonathan Zimmerman and the undersigned of AT&T met with Admiral David Simpson, Lisa Fowlkes, Jeffrey Goldthorp, Nicole McGinnis, and Peter Shroyer of the Public Safety and Homeland Security Bureau, and Matt DelNero, Brian Hurley and Daniel Kahn of the Wireline Competition Bureau, to discuss the Commission's broadband privacy proceeding. The discussion focused on the proposed data security and breach reporting rules.

During the discussion, and without waiving any legal claims AT&T may have with regard to any rules the Commission may adopt in this proceeding, AT&T noted that any rules that are adopted should incorporate a reasonableness standard, as suggested by the FTC staff and similar to the requirement of the current CPNI rules, rather than a strict liability standard. In addition, the Commission should incorporate the well-established reasonableness factors used by the FTC in its enforcement actions, including the sensitivity of the data, the seriousness of the threat or vulnerability and the cost of available tools. The Commission also should avoid prescriptive risk management or security requirements that would lock in static requirements that would fail to promote effective security as both security threats and vulnerabilities continue to evolve rapidly. Instead, any such rules should incorporate high level data security requirements focused on process and covering risk management assessments, employee and vendor training, and designation of a senior management official with responsibility for the program.

AT&T also emphasized its commitment to the public-private partnership model as the most effective approach to strengthen cybersecurity and respond to a changing threat environment and noted that prescriptive security rules would run counter to the Administration's longstanding support for such partnerships. Additionally, any rules adopted should expressly

support the ability of an ISP to use and share data in accordance with the Cybersecurity Information Sharing Act of 2015, including network monitoring, operating defensive measures and sharing cybersecurity threat information, and defensive measures for cybersecurity purposes.

AT&T also described the concerns by many commenters that the proposed reporting and notification of data breaches within 7-10 days after “discovery” of a breach would not allow sufficient time for providers to adequately investigate suspected breaches or to properly notify affected customers. Following its prior discussion on this subject with the Wireline Competition Bureau staff, AT&T has amended its reporting proposal to provide earlier notice of data breaches to the Commission without potentially encouraging premature and inaccurate reports that would not be helpful to the Commission or customers. Under this modified proposal, a provider would be required to notify the Commission without unreasonable delay and no later than seven (7) business days after the provider had determined with substantial certainty (or “reasonably determined”) that a breach had occurred and affected at least one customer. The notification would include the number of affected customers identified as of the date of the notification and would state whether the investigation was complete or ongoing. If the investigation was ongoing, the provider would update the notification every 30 days until the provider stated in an updated notification that the investigation was complete. The provider would notify each affected customer without unreasonable delay and no later than 20 business days after the date the customer was included in the provider’s initial or updated FCC notification (or 30 business days after that date for investigations affecting more than 500 customers).

AT&T also noted that some proposed or suggested reporting requirements would likely lead to excessive noticing that would not be helpful to customers, such as those requiring the reporting of inadvertent access or disclosure and conduct that “might reasonably lead to” a data breach. In addition to avoiding such requirements, the Commission should reduce excessive reporting by adopting the approach taken by many states of not requiring notification where a provider determines that there is no reasonable likelihood of harm to any customer resulting from the breach. As noted in AT&T’s comments (at 81, n. 162), the federal government uses a similar standard in determining whether notification is required of breaches of data held by federal agencies.

One electronic copy of this Notice is being submitted in the above-referenced proceeding in accordance with Section 1.1206 of the Commission’s rules.

Marlene Dortch  
August 23, 2016  
Page 3

Please contact the undersigned or Jackie Flemming on 202-457-3032 if you have any questions.

Respectfully submitted,

/s/James J.R. Talbot

James J.R. Talbot

Cc: Admiral David Simpson  
Matt DelNero  
Lisa Fowlkes  
Jeffrey Goldthorp  
Brian Hurley  
Daniel Kahn  
Nicole McGinnis  
Peter Shroyer