



601 Pennsylvania Ave., NW
Suite 800 – North Building
Washington, DC 20004
202-654-5900

October 14, 2016

SUBMITTED ELECTRONICALLY VIA ECFS

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

Re: Notice of *Ex Parte* Presentation, WC Docket No. 16-106

Dear Ms. Dortch:

On October 12, 2016, Kathleen Ham, Cathleen Massey, Christopher Koegel, and Michelle Rosenthal from T-Mobile USA, Inc.'s Government Affairs Office met with Travis Litman of Commissioner Rosenworcel's office with regard to the Federal Communications Commission's ("FCC") broadband privacy rulemaking proceeding, WC Docket No. 16-106.

On October 13, 2016, Cathleen Massey, Christopher Koegel, and Michelle Rosenthal from T-Mobile USA, Inc.'s Government Affairs Office met with Nick Degani and Kirk Arner of Commissioner Pai's office with regard to the FCC's broadband privacy rulemaking proceeding, WC Docket No. 16-106.

On October 13, 2016, Kathleen Ham, Cathleen Massey, Christopher Koegel, and Michelle Rosenthal from T-Mobile USA, Inc.'s Government Affairs Office met with Stephanie Weiner from Chairman Wheeler's office and Matt DeInero and Lisa Hone of the Wireline Competition Bureau of the FCC with regard to the FCC's broadband privacy rulemaking proceeding, WC Docket No. 16-106.

In these meetings, we discussed T-Mobile's role as a disruptor in the wireless industry and the need for a consistent privacy regime across the Internet ecosystem. An overly prescriptive privacy regime, including an unnecessarily broad scope of sensitive data subject to opt-in requirements, may prevent consumer-friendly innovation without offering any significant corresponding privacy benefit to consumers.

We commended the Commission on its movement to more flexible standards on data security and breach notification and the inclusion of the FTC's de-identified standard, and we discussed areas where the FCC could tailor current language to be more consistent with the FTC's approach, which has been working well to protect consumers while fostering innovation and competition. We asked the Commission to consider narrowing the scope of sensitive CPNI to the five FTC categories (health,

financial, children's, precise geolocation,¹ and social security numbers) and explained that any web browsing or app usage information that includes sensitive information relating to those categories would be covered by those five categories alone. To the extent the Commission has additional privacy concerns, they can be addressed through a more tailored approach, rather than including all web browsing or app usage data. Indeed, the FTC Report and the FTC's comments in this proceeding were consistent with this approach.² The inclusion of *all* web browsing and app usage data will have a significant impact on both interest-based advertising and first-party marketing programs, all of which provide great value to consumers in the form of discounts, convenient features, and other new and innovative services, and all of which will continue to be permissible for edge providers under the FTC's opt-out regime.

We also asked the Commission to ensure that any notice requirements, including those that relate to timing of notice, are flexible to ensure that consumers receive notice in a way and at a time that they are most able to consume the information. Finally, we requested a reasonable implementation period, given that even small changes to ISPs' current practices could require a significant amount of time to implement.

T-Mobile provided the attached presentation in the meetings.

Respectfully Submitted,

/s/ Michelle R. Rosenthal

Michelle R. Rosenthal
Senior Corporate Counsel
Government Affairs, Federal Regulatory
T-Mobile USA, Inc.

¹ We asked the Commission to clarify that sensitive CPNI definition include "precise geolocation," consistent with the FTC's Privacy Report, and not geolocation generally.

² See Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16-106, at 19-22, 35 (filed May 27, 2016) (noting that, beyond the five categories of sensitive data, only deep packet inspection for use of content, such as search terms or purchase history, should require opt-in consent).