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

September 13, 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 September 9, 2016, Cathleen Massey, Christopher Koegel, and Michelle Rosenthal from T-Mobile USA, Inc.'s Government Affairs Office met with Lisa Hone and David Brody of the Wireline Competition Bureau of the Federal Communications Commission (FCC) and Alison Nemeth and Karen Sprung of the FCC's Wireless Telecommunications Bureau with regard to the FCC's broadband privacy rulemaking proceeding, WC Docket No. 16-106.

We discussed T-Mobile's history and its role as a maverick in the wireless industry. For healthy competition in the wireless telecommunications marketplace to continue to flourish and provide consumer benefits, the FCC must give T-Mobile and other carriers freedom to innovate and compete with each other and with edge providers. At the same time, privacy and security is very important to T-Mobile. We are concerned, however, that an overly prescriptive regime, including broad scope and expansive notice and opt-in requirements, may prevent consumer-friendly innovation without offering any significant corresponding privacy benefit to consumers.

<u>Implementation Period</u>

We asked the Commission to consider a 12-18 month implementation time period after rules are adopted. It will take a significant amount of time for companies to implement entirely new rules in this space, and even if the Commission adopts a regime consistent with that of the Federal Trade Commission (FTC), which we urge the FCC to do, any small deviations could result in significant operational changes. Moreover, if the FCC were to adopt the proposed rules, this would represent a significant shift in the status quo. We also described the lengthy list of actions companies must

undertake when new rules are adopted.[1] We urged the FCC to establish an implementation period that would account for such a large undertaking.

Scope of the Rules

We reiterated our position set forth in our comments to the proceeding that the FCC has no legal authority to regulate personally-identifiable information (PII), and that any rules should be limited to customer proprietary network information (CPNI), as Congress intended. *See* Comments of T-Mobile USA, Inc., WC Docket No. 16-106, at 16-24 (filed May 27, 2016). We noted that the FCC does not need to list all the possible types of CPNI, but should be clear about which categories are not included, such as any information contemplated by Section 222(e) and defined in Section 222(h)(3)(a) – *i.e.*, subscriber list information.

We stated that the broad definition of CPNI proposed in the NPRM (along with the broad definition of PII) would be far-reaching and provide innumerable unintended consequences. For this reason, any privacy rules should draw distinctions between sensitive and non-sensitive data. T-Mobile believes that any definition of sensitive CPNI should be consistent with the FTC's approach to sensitive information, so that consumers and businesses can rely on a consistent approach across the Internet ecosystem. An overly broad definition in one sector could have far-reaching negative consequences, such as hindering innovation and causing consumer frustration, among other things. We noted that this could be an area where NTIA's multi-stakeholder process could play a role.

We reiterated our position that the consent provision in 47 U.S.C. § 222(c)(1) is limited to "individually identifiable" data, and that excludes data that has been de-identified. Accordingly, de-identified data should be carved out of the scope of the rules as long as carriers comply with the FTC's three-part test, which significantly reduces any risk of harm from the use of de-identified data. *See* FTC 2012 Privacy Report, at 21-22. As the FTC recognized in its Privacy Report and Congress recognized with legislation like HIPAA, there are many beneficial uses of de-identified data. Often, de-identified data is used to ensure accuracy or de-duplicate information before creating an aggregate data set. For example, the FCC's speed test app appears to use de-identified data at time of collection to help paint a broader picture about mobile broadband performance. Beyond the policy considerations, including de-identified data or aggregate data in the scope of rules that implement a statute limited to "individually identifiable" data would be legally impermissible. And doing so only for telecommunications carriers would create a competitive disadvantage, and impede innovation, with no added benefit to consumers.

Consent

We emphasized that when carriers share customer information with third parties to perform services on behalf of the carrier and the third party is contractually bound not to use the information for any other purpose, this should constitute "use," not "sharing," under the FCC's consent regime. In such cases, the consent mechanism should be the same as that required if the carrier was using the information and no

[1] These include analyzing rules for changes and requirements; discussing with various segments of our business; updating privacy, data security, and other policies; updating programs and certifications; updating tools to track and administer compliance programs; developing and giving training updates to employees and vendors; working with business, information technology, and security to update systems and practices; updating customer facing information and user interfaces; updating customer care and retail practices and providing training; reviewing and updating vendor contracts; and developing and designing reporting mechanisms, among other things.

third party was involved. Considering such an arrangement to be "sharing" would create a competitive bias toward the largest broadband internet access service ("BIAS") providers, which may be able to perform more functions in-house. Further, third-party vendors are themselves regulated at the federal and state level and are accountable even apart from contractual obligations.

We reiterated our position, set forth more fully in our comments, that the consent regime should be based on the sensitivity of the CPNI, rather than an arbitrary distinction between communications and non-communications related services. We agree with the Commission that inferred consent is sufficient for use and sharing of *any* CPNI pursuant to proposed Section 64.7002(a) in the NPRM, such as for the provision of broadband service, rendering a bill, etc. We also made the following points:

- For use of non-sensitive CPNI, inferred consent is also sufficient when the carrier is using the information for first-party marketing of any kind (unless opt-out is required under a separate regime like CAN-SPAM, the TCPA, or state statutes).
- To the extent a carrier is delivering third-party marketing using non-sensitive data, an opt-out is appropriate.
- For sharing of non-sensitive CPNI with affiliates, inferred consent is appropriate.
- For sharing of non-sensitive CPNI beyond sharing with an affiliate or vendor and beyond the uses listed in Section 64.7002, an opt-out is appropriate, but the Commission should consider an alternative approach for practices that benefit the public, such as the use of non-sensitive CPNI to prevent fraud on the carrier's network or elsewhere.
- For use of sensitive CPNI, an opt-out is appropriate for first-party marketing specifically designed to target consumers based on that sensitive CPNI and inferred consent is sufficient for first-party marketing that is not designed to target consumers based on sensitive CPNI.[2]
- For delivery of third-party marketing based on sensitive CPNI, this is an area where opt-in may be appropriate.
- For sharing of sensitive CPNI with non-affiliated third parties, this is another area where opt-in may be appropriate.[3] For sharing of sensitive CPNI with affiliated parties, an opt-out or implied consent is appropriate, depending on the circumstances.

We explained that the current distinction between communications and non-communications related services is arbitrary and no longer works in today's innovative marketplace. Under the FTC's approach, non-carriers are free to explore different lines of business, and it is considered first-party marketing.[4]

---

[2] This approach is explained in the FTC's Privacy Report where the agency recognized that, with respect to first-party marketing, "the risks to consumers may not justify the potential burdens on general audience businesses that incidentally collect and use sensitive information." *See* FTC Privacy Report at 47-48. An example might be that a carrier advertises new devices when a customer's device is 2-years old. If the carrier does this for all customers (*i.e.*, a "general audience"), but some consumers happen to have special devices or accessories for the hearing impaired, the carrier should not have to take a different approach for those customers.

[3] As discussed above, any sharing with a vendor in these contexts, where the vendor is contractually bound only to use the information on the carrier's behalf, should not be considered "sharing" under this consent regime, and therefore should not alter the required consent mechanism.

[4] For example, if a transportation business decides to start a food delivery service, they can market that new service to their transportation customers. In that case, the FTC would not require opt-in consent to market a new business that falls outside the "transportation" category.

We ask for the same flexibility so we can offer new products, services, conveniences, and other benefits to our customers.

Notice

The proposed transparency obligations would cause notice fatigue and consumer confusion. Further, prescriptive transparency requirements will prevent us from adapting to changing consumer expectations and delivering notice at a time that is most relevant to them. We have a strong relationship with our customers, and our reputation is extremely important to us. We urged the FCC to give carriers the flexibility to make a reasonable determination about when and how to offer notice to consumers.

Data Security

We reiterated that any data security standard should be based on reasonableness and not strict liability. In addition, the Commission should not apply its data security standard to the large breadth of data included in the NPRM. The standard should be limited to either sensitive CPNI or CPNI that is likely to lead to an economic or physical harm in the event of an unauthorized disclosure. As the NPRM stated, data security should be appropriately calibrated to the nature and scope of BIAS providers' activities and the sensitivity of the underlying data. *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500, ¶ 170 (2016). There should not be baseline requirements under any standard, because technology and threats continuously evolve. The final rule should include a reasonableness standard that can be supplemented by further FCC guidance as to what constitutes "reasonable security," and that can evolve with changing technology and threat environments.

Data Breach Notification

Data breach notification or reporting requirements should not be triggered unless there is a likelihood of economic or physical harm from the unauthorized disclosure. Otherwise, we risk inundating consumers and the federal government with notices that are not materially useful, and which may be confusing to consumers seeking to understand applicable risks.

Further, we raised concerns that the NPRM's proposed time period for breach notification is far too short given all of the steps that must be undertaken to responsibly address a breach, whether large or small.[5] Breach investigations often uncover additional facts as the case unfolds and need sufficient time to be thorough. Even with a huge team working around the clock, this can take a significant amount of time, particularly if a vendor is involved. We urged FCC staff to consider hinging any reporting or notification timeline on the *confirmation*, and not the *discovery*, of a covered breach.

[5] After a breach, a company must identify the vulnerability that caused the breach, patch the vulnerability, determine which customers were affected, determine which data was accessed, gather appropriate contact information for affected customers, draft letters to customers that comply with varying state laws, put remedies in place (such as identity restoration services, should the company find that to be appropriate), draft FAQs and other materials to ensure that we can answer the many customer inquiries that will follow, potentially hire additional customer care reps to the extent necessary, and train reps to answer questions related to the breach, among other things.

Although our policy is to report and notify customers of breaches as soon as possible, there should be a minimum of 10 days from confirmation of a breach to report the breach to the portal, and, consistent with the FTC's comments in this proceeding, 30-60 days to notify customers. *See* Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16-106, at 36 (filed May 27, 2016). Ultimately, companies have many incentives to notify customers as soon as possible and usually will do this well before 30-60 days. For that reason, the FCC also should shorten the 7-day waiting period before carriers can notify customers. In addition, alternative methods of breach notification (like SMS) should be allowed in the event the consumer is a prepaid customer and the carrier doesn't have his or her address. Otherwise, the FCC would be requiring carriers to collect more information than necessary.

Harmonization

T-Mobile supports harmonization of the voice and broadband rules, as long as the FCC takes a flexible approach with the broadband rules, as discussed.

Financial Incentives

We urged the FCC to think carefully about any rules around financial incentives or inducements. We do not support a ban on any practices, as we don't think bans are authorized under Section 222's consent regime. Specifically, rules should not prohibit the use of financial offerings, like rewards programs, to incentivize consumers to opt in to marketing programs. Rewards programs should be an acceptable means of achieving opt-in, particularly if the FCC's final broadband privacy rule requires BIAS providers to find new ways to offer innovative products and services to their customers.

Conclusion

No set of regulations will eliminate every privacy and security risk, but the FCC's focus should be to eliminate the risks that are likely to cause substantial harm to consumers. Beyond that, any regulation would be overly broad, legally and constitutionally impermissible, and would have a significant effect on carrier operations and their ability to innovate and offer new products and services to consumers – all without meaningfully enhancing consumer privacy.

Respectfully Submitted,

/s/ Michelle R. Rosenthal

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