Public Knowledge

October 18, 2016

Ms. Marlene H. 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 14, 2016, Dallas Harris of Public Knowledge, Gaurav Laroia of Free Press, Natasha Duarte of Center for Democracy and Technology, Susan Grant of Consumer Federation of America, and Claire Gartland of Electronic Privacy Information Center (collectively referred to as privacy advocates), met with Claude Aiken, Legal Adviser to Commissioner Clyburn, with regard to the above captioned proceeding.

Privacy advocates expressed concern around the Commission's proposal to require opt-in consent for sensitive information and opt-out consent for information deemed non sensitive. If the Commission proceeds with a sensitive/non sensitive framework, the sensitive category must be expansive as possible. Advocates laud the Commission for including web browsing and app usage history as sensitive information, and it is imperative that they remain sensitive. Many of the groups in the coalition cannot support a rule that does not treat web browsing and app history as sensitive. Further, advocates suggested that the Commission make information sensitive by default and narrowly define a category of non-sensitive information. The intent of the rule, to place consumers in charge of their information, would be defeated if the sensitive category is too narrowly defined.

In addition, privacy advocates are concerned about the lack of consent required for the use of de-identified information. The Commission should require some form of consumer consent for the use of de-identified data and to require greater transparency of de-identification techniques. If the Commission does proceed with this exception, the Commission must maintain oversight authority and ensure de-identification technologies/techniques are available for independent verification. Independent verification is imperative because of the ease of re-identification. Independent verification is the best way to ensure that de-identification techniques actually work. Privacy advocates also proposed expanding the definition of de-identified data to require that information is not linked or linkable to any unique identifier, including IP address. Further, the FCC should explicitly state that ISPs would be held liable if third party contractors fail to properly de-identify consumer information.

It is also important that the Commission require opt-in consent for any material changes to privacy policies. When ISPs collect data from customers that wasn't collected before and use data

for new purposes, consumers should be asked for their consent. Moreover, each consumer should be allowed to decline consent to the new terms and retain service.

Because of the evolving nature of the internet ecosystem, the Commission must make sure that the rules are flexible enough to be reexamined as necessary. Information that is not sensitive today could easily be deemed sensitive in the future. Similarly, de-identification techniques that are sufficient today may not be sufficient tomorrow. With the expansion of the "Internet of Things," the only way the Commission can properly protect consumers is by making today's rules flexible enough to deal with tomorrow's technologies.

Lastly, privacy advocates stressed the importance of the Commission's ability to enforce the privacy rules against "pay for privacy" schemes where the price differential makes it such that service is effectively conditioned on agreeing to give up privacy or violates the statutory prohibition on unjust and unreasonable practices.

Respectfully submitted,

/s/ Dallas Harris

Policy Fellow
Public Knowledge
1818 N St., NW
Suite 410
Washington, D.C. 20036
(202) 861-0020

Cc: Claude Aiken