August 26, 2018

Office of Cable Television, Film,
Music, & Entertainment (OCTFME)
Attn: Lawrence Cooper, General Counsel
1899 9th Street, NE
Washington, DC 20018

Re: Notice of Proposed Rulemaking—Privacy Protections for Cable and Internet Customers, N0071499

Dear Mr. Lawrence Cooper,

We, the undersigned privacy and consumer protection organizations, write to respond to the notice of proposed rulemaking from the Office of Cable Television, Film, Music, and Entertainment (hereinafter the "Agency") on the issue of broadband privacy rules for internet service providers (ISPs) operating in the District of Columbia.

We support the passage of these rules, which would provide consumers increased choice, security, and transparency over the data their internet service providers (ISPs) collect from and about them. In light of the decision by Congress to repeal the Federal Communications Commission's (FCC's) Broadband Privacy Rule under the Congressional Review Act, it is incumbent upon local governments to fill that gap. We applaud the Agency for their leadership on this issue, and we urge the Agency to pass strong rules to protect DC residents.

Residents of the District of Columbia need strong privacy protections over how ISPs treat their data. ISPs have a unique insight into customer activity because they provide internet service, for which they charge a substantial subscription fee, that requires them to collect a vast amount of data from and about their customers. While it is possible for consumers to take actions to protect themselves against certain edge providers who collect data—by blocking browser connections to those sites—they have no choice but to use an ISP to access the internet and thus share data with the ISP. And *all* of a consumer's traffic flows over that internet connection. Even if traffic is encrypted, ISPs still know the sites and services their customers use, which can convey very sensitive information such as race or nationality, sexual preference, religion, physical location, presence at home, personal banking details, and physical ailments.[1]

With such comprehensive data, ISPs can create intricately detailed profiles of their customers to sell to the highest bidder for a variety of purposes, including targeted digital advertisements for

[1] *See What ISPs Can See*, Upturn (Mar. 2016), https://www.teamupturn.com/reports/2016/what-isps-can-see.

products like payday loans or expensive and unnecessary medications. DC residents should have options over whether their ISP monetizes the data it collects to provide them internet service. These proposed rules ensure they have those choices.

In the wake of Congress' decision to repeal the Broadband Privacy Rule, there are no clear rules governing what ISPs can do with customer data. But DC consumers often pay well over $100 per month for internet service at home and on their devices. They should be entitled to a reasonable expectation of privacy in the use of these services. Just as we do not expect a cell carrier to listen to our phone calls, we should not expect them to watch and sell our web browsing and app usage. Thus, it is even more important for the District of Columbia to stand up and protect its citizens' privacy rights.

For these reasons, we urge the Agency to pass these rules and incorporate feedback from consumer and privacy advocacy groups on how to strengthen them.

Signed,

Access Humboldt
Center for Democracy & Technology
Consumer Action
Consumer Federation of America
Consumers Union
Institute for Local Self-Reliance
Vermont Mutual Aid Society