STATEMENT OF
CHAIRMAN TOM WHEELER

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.

Privacy is important to consumers and we at the FCC have been given special responsibility to safeguard privacy in the use of communications networks. That makes just as much sense in the world of broadband as it has for the past 20 years in the world of telephone calls – where the FCC has steadfastly protected consumers against misuse of their information by requiring that networks obtain their customers' approval before repurposing or reselling customer information.

Section 222 of the Communications Act expressly grants the Commission the authority it has used to protect the privacy of customer information that phone companies collect. Today, with this Notice of Proposed Rulemaking or NPRM, we start down a path that will provide clear guidance to Internet Service Providers (ISPs) and their customers about how the privacy requirements of the Communications Act apply to the most significant communications technology of today: broadband Internet access service. If anything, privacy issues are even more important when consumers use broadband connections to reach the Internet. And, when consumers sign up for Internet service, they shouldn't have to sign away their right to privacy.

Most of us understand that the social media we join and the websites we visit collect our personal information, and use it for advertising purposes. Seldom, however, do we stop to realize that our ISP is also collecting information about us. What's more, we can choose not to visit a website or not to sign up for a social network, or we can choose to drop one and switch to another in milliseconds. But broadband service is different. Once we subscribe to an ISP—for our home or for our smartphone—most of us have little flexibility to change our mind or avoid that network rapidly.

Our ISPs handle *all* of our network traffic. That means an ISP has a broad view of all of its customers' unencrypted online activity – when we are online, the websites we visit, and the apps we use. If we have mobile devices – and I have had a mobile device since 1983 – our providers can track our physical location throughout the day in real time. Even when data is encrypted, our broadband providers can piece together significant amounts of information about us – including private information such as a chronic medical condition or financial problems – based on our online activity.

Today's proposal would give all consumers the tools we need to make informed decisions about how our ISPs use and share our data, and confidence that ISPs are keeping their customers' data secure.

Today's proposal is built on three core principles – choice, transparency, and security.

It separates the use and sharing of customer information into three categories and crafts clear expectations for both ISPs and customers. Under this proposal, information necessary to deliver broadband services could still be used by ISPs without additional consumer consent, so treatment of that data is largely unchanged. The ISP also has the right to use your name, address, IP address, and other information necessary to establish a business relationship with you, to provide the broadband service you have contracted for, for example, to market higher speeds and lower rates for the type of broadband services that you already purchase.

Under this proposal, ISPs and their affiliates that offer communications-related services would be able to market other communications-related services unless the consumer affirmatively opts out.

Under this proposal, all other uses and sharing of consumer data would require affirmative "opt-in" consent from customers -- in other words, the affirmative choice of a consumer to decide how his or her information should be used.

If this plan is adopted, each of us will have the right to exercise control over what personal data our broadband provider uses and under what circumstances it shares our personal information with third parties or affiliated companies. We will know what information is being collected about us and how it's being used. That information must be provided by our broadband service providers in an easily understandable and accessible manner. And if our broadband provider is collecting and storing information about us, it will have a responsibility to make sure that information is secure.

To be clear, this is not regulating what we often refer to as the edge – meaning the online applications and services that you access over the Internet, like Twitter and Uber. It is narrowly focused on the personal information collected by broadband providers as a function of providing you with broadband connectivity, not the privacy practices of the websites and other online services that you choose to visit.

Nor does this proposal wade into government surveillance, encryption or other law enforcement issues. Again, this is about ISPs and only ISPs.

And this proposal does not prohibit ISPs from using and sharing customer data – it simply proposes that the ISP *first* obtain customers' express permission before doing so.

I expect that many consumers will agree. After all, many of us find targeted advertising very valuable. Many people like to have recommendations made that reflect their personal interests or their current location. Think about all the mobile apps that ask for – and receive – permission to use location data. My simple point is this – people should have the ability to decide in the first instance.

Today's NPRM reflects widespread agreement among ISPs, public interest groups, and others about the importance of choice, transparency, and data security of confidential customer information. It also reflects lessons learned from the FCC's privacy work, and from other agencies' implementation of sector-specific privacy legislation, and it is firmly rooted in the privacy protection work done by the Federal Trade Commission (FTC) in the exercise of the FTC's general consumer protection jurisdiction.

While today's NPRM sets forth a clear path forward towards final rules, it also seeks comment on a range of issues, including additional or alternative paths to achieve pro-consumer, pro-privacy goals, to ensure the development of a robust record upon which the Commission can rely in adopting final rules. Moving forward, we want to listen and learn from the public and ISPs before we adopt final, enforceable, rules of the road.

In the end, this proceeding isn't about any particular company or practice. It's about providing baseline protections for consumers. After all, it's our data. We all deserve information about and control over how our data is used.