Opening Statement of Chairman Greg Walden
Subcommittee on Communications and Technology
"Protecting Customer Proprietary Network Information in the Internet Age"
July 11, 2018

Good morning. As questions continue to arise surrounding the exchange between consumers and the technology platforms and services they use on a daily basis, the Energy and Commerce Committee has focused its attention on the protection, transparency, and use of consumer data. Earlier this week, Chairman Blackburn and I, along with Chairman Latta and Chairman Harper, sent letters to Apple and Google to inquire about their data collection and sharing practices.

We continue this important conversation today in the context of protecting customer proprietary network information, or CPNI. We can all recognize the importance of protecting consumers' personal information, no matter what kind of network they are using for communication.

In the decades since Congress enacted the Communications Act of 1996, requiring telecommunications carriers to protect the confidentiality of CPNI, the Federal Communications Commission (FCC) has updated CPNI rules to address evolving technology, practices, and consumer expectations.

For example, in 2007, the FCC extended the CPNI rules to cover voice calls made over the IP network that interconnected with the traditional telephone network. At that time, the FCC also beefed up its authentication provisions under the CPNI rules so third parties could not fraudulently obtain access to protected consumer data.

Again, in 2013, consumer expectations and changes in technology led the FCC to extend CPNI protections to data collected on mobile devices under the direction or control of a telecommunications carrier.

These were important advancements, and reflected the seriousness attached to how a customer's sensitive information, such as location data, is managed. Location information when attached to a call that touches the telephone network is considered to be "call detail information" and is thus protected under the CPNI rules. But, increasingly, other entities are utilizing location data to provide services on a mobile device that may not cross the public switched telephone network.

New applications that rely on location-based services can be useful, efficient, and even potentially life-saving for consumers. We're hearing of new innovations in ride-sharing where an emergency button within an app will connect you with a 911 call center. There are new partnerships forming to share phone device location data directly to 911 public safety answering points, separate from and in addition to carrier location information.

However, consumers deserve to know that an app that collects location information from a mobile device might not have to abide by the same rules as a telecommunications provider, and that their location information might not be as secure.

While these entities are outside of the scope of the current CPNI rules, we must consider the entire internet ecosystem as we continue to work on comprehensive solutions. We have companies now that provide live communication, act as content producers and publishers, and aggregate data – all in one package – and the old rules just don't fit the today's paradigms.

That is why the FCC's 2016 broadband privacy order was the wrong policy; we knew it wouldn't increase protections. That is why the 2015 net neutrality order was the wrong policy; we knew it wouldn't facilitate an environment to incentivize the next generation of services to close the close the broadband divide and deliver consumers smart cities, telemedicine, distance learning, and more.

Today, we need to thoughtfully consider how effective the old protections under CPNI are in today's information sharing world.

I'd like to thank our witnesses for joining us today. I look forward to hearing from you and hearing your insights.