

**Opening Statement of Chairman Marsha Blackburn
Subcommittee on Communications and Technology
“Protecting Customer Proprietary Network Information in the Internet Age.”
July 11, 2018**

(As prepared for delivery)

Good morning and welcome to today’s hearing on protecting consumer privacy. This is a topic that has attracted attention in a variety of contexts, and one that I am glad to discuss today. Thank you to our witnesses for sharing your expertise with us today as we strive to protect customer privacy when communicating in the Internet age.

Over 20 years ago, Congress realized the importance of protecting the confidentiality of *customer proprietary network information*, or CPNI, when consumers used the primary method for instantaneous communication: telephone calls. The rules that the FCC initially adopted to implement the statutory CPNI requirements only covered information from traditional call records, but over time, these protections have evolved to cover new forms of communication—like interconnected voice over IP (VoIP) calls and even information collected by telecommunications carriers on mobile devices.

By enacting Section 222, Congress established a specific statutory structure that acknowledged that consumers share sensitive data when they communicate over the phone. This was based on the assumption that only the telecommunications carrier had access to that data. In the

Internet age, telecommunications laws have been disrupted just like everything else. In some cases, app developers, operating systems, and edge providers have access to the same exact CPNI that telecommunications carriers are required to protect in various ways. Consumers now use these different forms of communication interchangeably to serve the same purpose.

For example, if a consumer uses his or her mobile phone to call someone using the standard telephone function on their cell phone, that call is traveling over the public switched telecommunications network and would be protected by the current CPNI rules, and enforced by the FCC. If that same consumer uses the exact same cell phone to call the exact same person, but uses a voice-based app to place the call, the communication would not be going over the PSTN and not be protected by the CPNI rules. Both calls are conveying the same information, but the consumer's information in the second scenario is not protected in the same manner as in the first scenario.

This leads to a problem where consumers do not have the same privacy protections when using the same device for essentially the same purpose. This is why the FCC's 2016 privacy order was a consumer protection vehicle that drove at the wrong target. The commission's inability to locate all the other traffic out there is precisely why the wheels came off it. As I have suggested before, the solution to this

problem is broad privacy legislation, which is why I introduced legislation on this subject almost a year ago that steers us in the right direction — the BROWSER Act is a comprehensive, bipartisan privacy bill that will give Americans seamless protection across all their electronic communications.

As we discuss these important issues today, we need to consider innovation and consumer privacy needs across the entire Internet ecosystem so we can arrive at a solution that works for everyone.

At this time, I will yield to the remainder of my time to Mr. Lance for an opening statement.