

**STATEMENT OF
COMMISSIONER JESSICA ROSENWORCEL**

Re: *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Declaratory Ruling, CC Docket 96-115 (June 27, 2013)*

It has been over six years since the Commission last updated its customer proprietary network information (CPNI) rules. Think about that. Our last major decision was released before the introduction of the iPhone. Before any one of us thought it was normal to tap on a screen—any screen—and expect an Internet-enabled response based on the swipe of a finger. Before streaming any video in our palms and laps was even imaginable. Before the applications economy grew to provide 500,000 new jobs. It was a long time ago.

In the intervening years, several trends have collided to make the values that inform our CPNI rules both more important and more complicated.

First, connection is no longer merely convenient. We live in an age of always-on connectivity. We are a nation with more wireless phones than people. One in three adults now has a tablet computer. Our commercial and civic lives are migrating online with ferocious force and speed. Simply put, the opportunity to opt out of this new digital age is limited. Its advances are too bountiful, they save us time and money, and they inform and support all aspects of modern life.

Second, it used to be that the communications relationship was primarily between a customer and his or her carrier. But the number of third parties participating in our digital age connections and transactions has multiplied exponentially. Dial a call, write an e-mail, make a purchase, post an online update to a social network, read a news site, store your family photographs in the cloud, and you should assume that service providers, advertising networks, and companies specializing in analytics have access to your personal information. Lots of it—and for a long time. Our digital footprints are hardly in sand; they are effectively in wet cement.

Third, the monetization of data is big business. The cost of data storage has declined dramatically. The market incentives to keep our data and slice and dice it to inform commercial activity are enormous. They are only going to grow.

Going forward, I think the Commission needs to take note of these trends. They are the impetus, I believe, for last year's Administration blueprint for consumer data privacy in the 21st Century. It is a blueprint I support.

But against this background, we also need to do simple things at the Commission, like enforce our rules.

To this end, in Section 222 of the Communications Act, Congress sought to guard consumers by defining CPNI rights in their relationship with their telecommunications carriers: the right to know what information is being collected about them; the right to get notice when

information is being used for other purposes; and the right to be able to stop the reuse or sale of that information. Today's decision advances these principles. It clarifies that our CPNI rules and obligations apply to information that carriers cause to be stored on their customer's devices, like wireless phones. As a result, carriers may only use and disclose such information consistent with our rules. This means wireless carriers must protect CPNI data from unauthorized disclosure and inform subscribers in the event of a security breach.

However, it is also important to be clear about what our decision does not do. Our CPNI protections at issue in this decision involve carriers. They do not apply to the manufacturers of wireless phones. They do not apply to the developers of operating systems.

So let's be honest. Consumers can be confused by these distinctions. But the scope of this proceeding and Section 222 are limited. So I hope the agency can be proactive and help consumers better understand the different ways their personal data may be collected on a mobile phones, what rules apply, and how they can protect themselves. Furthermore, I think we should take on this task in cooperation with our colleagues at the Federal Trade Commission. Because consumers should not have to be network engineers to understand who is collecting their data and they should not have to be lawyers to determine if their information is protected. We should strive to simplify privacy policies across all platforms and aim for more consistency. But in the interim, it is also essential we enforce our rules. That is what we do here and that is why I am pleased to support this declaratory ruling.