

**STATEMENT OF  
COMMISSIONER JESSICA ROSENWORCEL**

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

To understand the future of privacy, I think it is important to begin by focusing on the forces shaping our new digital world. I see three.

First, we live in an era of always-on connectivity. Connection is no longer just convenient. It fuels every aspect of modern civic and commercial life. Sitting outside this connectivity is consigning yourself to the wrong side of the digital divide—and that has a cost because it hampers any shot at 21<sup>st</sup> century success.

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, update a profile, peruse a news site, store 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. For a long time. Our digital footprints are no longer in sand; they are 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—and they are going to grow.

Today these forces collide for all of us in our lives lived online, where what we download, post, say and do says so much about who we are to the world.

But the truth is we are just getting started. Because the future will feature a whole new world of the Internet of Things, where the connectivity we have today will look quaint. Every piece of machinery, pallet of equipment, thermostat, smoke detector, street light, garbage pail, parking meter—you name it—will be a connected device. This creates powerful opportunities that will make us more effective and more efficient, our cities smarter and our communities more connected. But these benefits come with big security challenges. We had an object lesson in these challenges last weekend, with one of the largest Distributed Denial of Service attacks in history, with botnets taking control of insecure connected devices, and compromising them by flooding servers and sites with overwhelming traffic.

So when consumers survey this new digital landscape they wonder what privacy means. They do not want the digital age to decimate their fabled right to be left alone. They want privacy—but more importantly they want control. They want to control the whiplash from these new digital forces—and take some ownership of what is done with their personal information.

Today, the Commission provides consumers with the tools to do just that. We update—for the first time in nearly a decade—our privacy policies under Section 222 of the Communications Act. We establish new rules protecting the privacy of broadband customers. We adopt an opt-in regime for use and sharing of sensitive customer personal information and an opt-out regime for use and sharing of non-sensitive customer personal information. We put in place data security and breach notification policies so every consumer has confidence that efforts are in place to prevent harm from unlawful access to their data.

This is real privacy control for consumers. It helps in the here and now. But with respect to the future of privacy, I think we still have work to do.

Our domestic privacy policies largely rest on a foundation of old sector-specific laws. So continuing work to harmonize our privacy frameworks is hard—but deserves time and attention. To this end, the policies we adopt today are in many ways in sync with the approach taken by our colleagues at the Federal Trade Commission under Section 5 of the Federal Trade Commission Act. To the extent

they are not, let's face the facts—we are dealing with old laws, new technologies, and hard choices about existing regulatory schemes.

Privacy policy discussion, including ours here today, frequently focuses on three values—transparency, choice, and security. But I think it is time to introduce a fourth—simplicity. The forces at work in the digital world today are only going to make privacy more complex for all of us to control. But consumers should not have to be network engineers to understand who is collecting their data and they should not have to be lawyers to understand if their information is protected. So it is incumbent on every policymaker with privacy authority to think about how to make our policies more simple and more consistent. In fact, I think it is time for a 21<sup>st</sup> century inter-agency privacy council, where this Commission and our colleagues across government can do a better job of aligning privacy policies across the board. That won't be easy. But for the future of privacy, future of consumer control, and future of the digital economy—it will be worth the effort.