REMARKS OF
FCC CHAIRWOMAN JESSICA ROSENWORCEL
TO THE CENTER FOR DEMOCRACY AND TECHNOLOGY
FORUM ON DATA PRIVACY
JUNE 14, 2023

Good afternoon. Thank you all for joining us.

Thank you to the Center for Democracy and Technology for hosting today's forum. Thank you also to the panel of experts joining us for today's discussion. I look forward to hearing your insights because I believe we have work to do to address communications privacy in the digital world.

To understand just what is at stake with communications privacy, I think it is important to begin by recognizing 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 means shutting yourself off from any shot at 21st century success. But too often this always-on connectivity—which has brought so many benefits—can mean a sacrifice of our privacy.

Second, 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 only growing.

Third, more money means more players. It used to be that in communications the relationship was primarily between a customer and his or her service provider. But the number of third parties participating in our digital age connections 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.

We see these three forces over and over again at the FCC.

Let me give you one example. Back in May of 2018, *The New York Times* first reported that the country's largest wireless carriers were selling real-time location information—where we are with our phones and when—to data aggregators. It was alarming stuff. Over time, with additional reporting, and an investigation from the FCC, a fuller picture of just what was going on started to emerge.

It turns out wireless carriers had sold access to individual, real-time geolocation data—again, where we are with are phones and when—to data aggregators. These aggregators then sold it to a skip-tracing firm, who then sold it to a bail-bond company, who then sold it off to individual bounty hunters.

Got that? Yeah, it sounds crazy. But what it means is that when this article was written just about anyone could pay $300 to a bounty hunter and get information about when and where you were using your mobile phone. That is the kind of sacrifice of privacy no one should expect when they sign up for wireless service. But it does show those three forces at work—how our most important connections can be monetized and how the business of gathering our data has expanded—exponentially.

Let me give you another example. Over and over again we are seeing reports of data breaches involving the data carriers have about their customers. Just three months ago, one carrier notified 9 million customers that some of their personal information had been accessed by an unauthorized party. The hacker got this information by compromising the system of a vendor used for marketing. At the start of the year, yet another carrier reported that an intruder in its system had stolen data on 37 million of its customers. And this report came on the heels of an earlier breach of the personal information of more than 75 million current, former, and prospective customers from the same carrier. That's a lot. These forces are powerful; the numbers add up.

One more example. Late last year we had a carrier notify an undisclosed number of its prepaid wireless customers that they had been targeted by SIM-swapping attacks. As most of this audience knows, SIM swapping is an increasingly popular scam. But for the uninitiated, SIM cards are small plastic chips, about the size of a dime, that are inserted into a mobile phone to identify and authenticate the subscriber. Here's how this scam works: A bad actor, often using sensitive information stolen through a data breach, calls up your wireless provider and uses this information to convince the customer service representative that they really are you and that you need your phone number switched to a new SIM card that they control. If they are successful, they can use your phone number to divert your incoming messages and easily complete the kind of two-factor authentication checks that financial institutions and social media companies use to provide service. That means they can then take over your e-mail and drain your bank accounts. Again, this kind of fraud demonstrates how powerful these forces are and how privacy is so important for communications—and digital-age trust.

If you need further evidence, consider this: a recent Pew survey found that half of Americans have chosen not to use a product or service because of privacy concerns. That's a problem, and it is incumbent on policymakers to take action—using whatever tools they have—to improve privacy and enhance digital-age trust.

So here is what we are working on right now at the Federal Communications Commission to do just that.

I believe the agency has an important role to play ensuring the privacy of consumer communications. The law provides us with clear communications privacy authority, including Section 222 and Section 631 of the Communications Act. But in light of the magnitude of the privacy challenges we face, I think we need to concentrate our efforts at the agency and give them focus.

That's why I am pleased to announce that we are creating a first-ever Privacy and Data Protection Task Force at the Commission. We are going to bring all of our technical and legal experts together from across the agency to maximize coordination and use the law to get results—by evolving our policies and taking enforcement action. This task force will be led by Loyaan Egal, Chief of the Enforcement Bureau. And under his watch already we have doubled the number of people working on privacy and data security investigations. Now we are bringing new form to these efforts.

The Task Force will have input in several ongoing efforts at the agency. These include an effort to modernize the FCC's data breach rules. They are due for a digital age update, which

we proposed in a recent rulemaking. And they need to be fine-tuned to address the kind of breaches we are seeing all too often now—the kinds that affect millions of customers and make vulnerable their sensitive data. We will also charge this group with overseeing the investigations and enforcement actions that follow these data breaches.

On top of that, the Task Force will help with the development of rules to crack down on SIM-swapping fraud. We have a rulemaking proposing standards for carriers to authenticate a customer before transferring a number to a new device or carrier. We will follow up with an effort to adopt new rules in place to put a stop to these scams.

The Task Force will also play a role in our work under the Safe Connections Act. This was a law passed last year to help support access to communications for survivors of domestic violence. This is so important because survivors face unique privacy challenges securely reaching hotlines and shelters and setting up new service accounts.

And we will be asking the Task Force to take a look at the data we amassed last year when I wrote the 15 largest mobile carriers seeking information about their geolocation data retention and privacy practices. The FCC had never done this before. So when we got the responses I did something new. I made their responses public. We have investigations underway to follow up on this data gathering, and the Task Force will assume responsibility for this effort.

Finally, today, with the help of the Task Force, I am sharing with my colleagues a proposed enforcement action against two companies that have put the security of communications customers at risk. It's an enforcement action, so I can't say more right now. But I can say this: right out of the gate, we are showing that this Task Force means business.

Now let me close out with something I mentioned when I began—and that's holding wireless carriers accountable for allowing our location data to be bought and sold on the black market. This is so important. The devices we carry in our palms, pockets, and purses know a lot about us. They know our whereabouts at any moment. This geolocation data is especially sensitive. It is a record of where we have been and who we are. In the wrong hands—a stalker, a criminal—it can put our privacy and physical security at risk.

In 2020, the FCC took enforcement action against the carriers for selling and sharing this geolocation data. It issued Notices of Apparent Liability that helped stop this ugly practice. But it is time to back that up with Forfeiture Orders and fines. It is time to hold them accountable and make them pay up for this behavior—and by that, I mean the more than $200 million in fines proposed by the prior administration. So let me call on my colleagues to bring this chapter to a close by finalizing these fines and voting for the Forfeiture Orders I have shared with them. We need to make clear that when you violate consumer communications privacy, there are consequences.

In the end, I believe the most consequential thing we can do is keep working on this issue. Because the digital-age privacy challenges we face are not going away. The forces behind them are too powerful and move too much of modern life. That means right now we need to use the law, evolve our policies, and approach consumer privacy and data security with new vigor. We need to look for every way to increase consumer trust and confidence, because if we do, we can ensure the benefits of this new digital world do more than just exceed its burdens, we can make communications private, safe, and secure. So let's do it.

Thank you.