STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

Re: Data Breach Reporting Requirements, WC Docket No. 22-21, Report and Order
(December 13, 2023)

It has been sixteen years since the Federal Communications Commission last updated its policies
to protect consumers from data breaches. Sixteen years! To be clear, that was before the iPhone was
introduced. There were no smart phones, there was no app store, there were no blue and green bubbles
for text. It was a long time ago. In the intervening years a lot has changed about when, where, and how
we use our phones, and what data our providers collect about us when we do. But not the FCC’s data
breach rules; they remain stuck in the analog age.

Today we fix this problem. We update our policies to protect consumers from digital age data
breaches. We make clear that under the Communications Act carriers have a duty to protect the privacy
and security of consumer data.

First, we modernize our data breach rules to make clear they include all personally identifiable
information. In the past, these rules have only prohibited the disclosure of information about who we call
and when. But consumers also deserve to know if their carrier has disclosed their social security number
or financial data or other sensitive information that could put them in harm’s way. We fix that today—
and it is overdue.

Second, we modernize our data breach rules to make clear they cover intentional and inadvertent
disclosure of customer information. Consumers deserve protection regardless of whether the release of
their personally identifiable information was intentional or accidental. Either way, they could find
themselves in trouble, so our rules need to address both.

Third, we modernize our standards for notification. That means in the event of a data breach,
your carrier has to tell the FCC and tell you in a timely way just what happened and what personal
information may be at risk. Our old rules required carriers to wait seven business days before telling
consumers what breaches had taken place. But there is no reason why consumers should have to wait that
long before learning that their personal information has been stolen or misused.

Finally, we update reporting requirements associated with data breaches. We also make clear our
policies apply to telecommunications relay service providers, so that those with disabilities get the same
protections as everyone else.

These are necessary updates. Find a consumer with a phone anywhere and they would tell you
every one of these changes make sense. What makes no sense is leaving our policies stuck in the analog
era. Our phones now know so much about where we go and who we are, we need rules on the books that
make sure carriers keep our information safe and cybersecure.

I want to thank the Commission’s Privacy and Data Protection Task Force for their input into this
effort and work to update our privacy and security policies across the board. I also want to note that with
the help of the task force, for the first time ever the FCC has signed Memoranda of Understanding with
Attorneys General from Pennsylvania, Illinois, Connecticut, and New York who are committing to work
with us on privacy, data protection, and cybersecurity enforcement matters.

A thank you also goes to our colleagues at the U.S. Secret Service and Federal Bureau of
Investigation for their input and support on this effort. Let me also commend staff at the agency for their
work, including Callie Coker, Adam Copeland, Trent Harkrader, Melissa Kirkel, Jodie May, Kimia
Nikseresht, Zach Ross, Mason Shefâ, and John Visclosky from the Wireline Competition Bureau; Robert