**DISSENTING STATEMENT OF**
**COMMISSIONER NATHAN SIMINGTON**

Re: *In the Matter of Data Breach Reporting Requirements*, WC Docket No. 22-21

My primary objection to the order we adopt today is not that it is necessarily bad policy—even though it could benefit from greater clarity and specificity, as well as better targeting—but that it is part of an effort to nullify the 2017 Congressional Review Act resolution that overturned the *2016 Privacy Order*, which this order reimplements various provisions of.

The CRA prohibits an agency from adopting a rule that is "substantially the same" as a previous rule that was overturned by a CRA resolution. A wooden reading of the statute—that an order does not reissue "substantially the same" rule unless the individual order has almost all of the same provisions of the overturned rule—would turn the CRA's prohibition into a nullity. An agency seeking to circumvent a previous CRA resolution could just split the desired regulations into several orders and pass it piecemeal. To give the CRA meaningful effect, we must look at not just the content of any one order, but the totality of related orders adopted subsequent to a CRA resolution.

Readopting the *2016 Privacy Order* in piecemeal is exactly what the Commission is doing. Today, we adopt a breach notification rule for Title II providers, which right now, mostly means telephone companies. But two months ago, this Commission began the process of reclassifying broadband as a Title II service, which when complete, will subject broadband providers to these new rules as well, just as the 2016 order did. Last month, we adopted data security, customer authentication, employee training, and other requirements that mirror provisions of the 2016 order.[1] And I have no doubt that this Commission will, if given the chance, adopt even more aspects of the 2016 order.

In a further similarity, the order we adopt today dramatically expands the kinds of data that the FCC has jurisdiction over, exactly like the *2016 Privacy Order*. And it relies on the same dubious legal theory as the 2016 order. Traditionally, the FCC's privacy authority has been limited to "Customer Proprietary Network Information" (CPNI), a term of art defined and used in Section 222's grants of authority. CPNI is limited to " quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service." The majority is not satisfied with jurisdiction over only this data, and instead asserts jurisdiction over all personally identifiable information (PII). To justify this, it relies on the omission of the word "network" from the introductory sentence at Section 222(a). But this interpretation is inconsistent with decades of FCC interpretation and practice. The best interpretation of Section 222(a) is that it is not an independent source of authority, but a high-level summary of the more specific provisions that follow it.

With this order today, has the Commission reissued "substantially the same" rule as the 2016

[1] The majority argues that the requirements imposed by our *SIM Swap Order* are substantially different from similar requirements in the 2016 order because they are motivated by the prevention of SIM swap and port-out fraud, while the 2016 order was motivated by more general privacy and data security concerns. But the purposes which motivate our rulemakings are irrelevant, and only the actual scope of the adopted rules matters. The *SIM Swap Order* requires that "employees who receive inbound customer communications" be unable to access CPNI until the customer has been "properly authenticated." Nothing about this requirement is limited to the prevention of SIM swap or port-out fraud, and it is very similar to the 2016 order's requirement for providers to "take reasonable measures to secure PI," which was accompanied by a list of practices the FCC deemed "exemplary of reasonable data security" that included "robust customer authentication." And while other elements of the *SIM Swap Order*, like employee training and customer notification requirements, are in fact limited to SIM swap and port-out procedures, they nonetheless mirror employee training and customer notification requirements in the 2016 order. Taken with this order today and likely future Commission action, this looks like exactly the kind of piecemeal readoption of the *2016 Privacy Order* that I am concerned is underway.

Privacy Order? Quite possibly. And I am sure that this item is at least a major step toward doing that, which I cannot support. Therefore, I must dissent.