DISSENTING STATEMENT OF
COMMISSIONER MICHAEL O'RIELLY

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

This Notice flows directly from last year's misguided *Net Neutrality Order* and its flawed decision to reclassify broadband as a Title II service, so I expected to have threshold concerns about the authority to regulate the privacy practices of Internet Service Providers (ISPs). I had hoped, however, that the agency would at least take the time to outline a thoughtful approach to privacy.[1] As someone who has spent a great deal of time on various privacy efforts and legislation, I know that these issues can be very complex. Therefore, it would make sense for an agency with so little expertise on privacy to engage in regulatory humility and proceed incrementally.

But instead of taking the time to understand the current privacy landscape, including the FTC's well-regarded standards and body of precedent, the Notice falls back on the familiar cut and paste job, attempting to force Customer Proprietary Network Information (CPNI) rules and definitions onto broadband. The Commission also sets off on a statutory fishing expedition to find new language to support additional privacy rules, before finally proposing to shift key functions of the Internet economy to an opt-in regime that previously has been reserved for the most sensitive of information. And that's just the privacy section. In an alarming display of doublethink, the Notice also proposes new data security risk management rules—at the same time that there is a Policy Statement circulating amongst the Commissioners that claims the FCC will take a voluntary approach in this area. Similarly, the item's approach to data breach notifications could result in consumers receiving inapplicable information, while at the same time, the FCC's approach to the Telephone Consumer Protection Act (TCPA) is preventing other consumers from receiving legitimate and necessary notifications.

Starting with legal authority, I opposed the decision to reclassify broadband ISPs as telecommunications carriers, and do not believe that they are subject to any regulation under Title II. Yet even if that decision holds up in court, I would still disagree with the Commission's authority to regulate broadband privacy practices.

The Commission begins by taking the CPNI framework and expanding it to broadband—potentially encompassing everything from domain names and traffic statistics to application usage and CPE. However, section 222(c) and the accompanying definition of CPNI found in section 222(h)(1) were designed to address specific concerns at the time about telephone call records and bill information. Having been there during the provision's inception, few of the staunchest supporters could have ever dreamt that the language could be stretched this far. The entire effort to do so brings to mind a certain expression about square pegs and round holes. And I had thought that the reason for conducting this rulemaking was that the Commission thought the current CPNI rules were not a good fit for broadband.

Not content to stop there, the Commission turns its regulatory attention to section 222(a). Unfortunately, the Notice accepts the faulty premise first advanced in the *TerraCom NAL* that section

[1] I strenuously object to the notion that this is just a simple NPRM to start the process and ask questions, as has been falsely yammered about other items. If that were the case, then just why would the Commission need to set such short comment dates and base them on the item's release as opposed to publication in the Federal Register? Instead, this entrée is a pre-cooked one, where the only reason for the NPRM is because the law requires it.

222(a) provides independent authority.[2] As I explained in more detail in my dissent on the *TerraCom NAL*, the purpose of section 222(a) was to set forth *who* would be covered by the new CPNI rules. Before the 1996 Act, the rules only applied to AT&T, the BOCs, and GTE. Section 222(a) changed that by extending the general duty to protect proprietary information to *all* telecommunications carriers, while sections 222(b) and (c) detail when and how that duty is to be exercised. Specifically, section 222(b) protects other carriers from anti-competitive practices by requiring the confidentiality of carrier proprietary information, while section 222(c) protects the privacy expectations of consumers with respect to their call records by requiring the confidentiality of customer proprietary network information.

Given this three-part structure, it is not surprising that section 222(a) employs a term—proprietary information—that encompasses both the carrier proprietary information used in 222(b) as well as the customer proprietary network information used in section 222(c). It does not give the Commission license to ignore its own history and read section 222(a) terminology out of context. But I guess I shouldn't be surprised that an offshoot of the *Net Neutrality Order* would contain its own catch-all provision.

This make-believe authority in section 222(a) could cover some of the same information that the Notice proposes to include as CPNI, as well as things like shopping records, biometric information, and information identifying personally owned property. In a footnote, the Notice acknowledges that broadband providers may not even collect such information. But this is not the first instance where this agency has engaged in regulation by speculation, and I'm sure it won't be the last, despite how insulting and deplorable it is for a regulatory agency to be so clueless just as it prepares to impose new burdens on U.S. industry and consumers. The ignorance is stunning and raises serious questions about the competency of the Commission's expertise in other, more justifiable areas.

The Notice also proposes a four-part test for the use and disclosure of aggregate customer information. Of course, this test has no basis in the statute. Section 222(c)(3) makes clear that carriers "may use, disclose, or permit access to aggregate customer information." The only condition on aggregate customer information is that it must be provided to other carriers or persons on reasonable and nondiscriminatory terms or conditions upon reasonable request, and that condition was included to address competitive concerns, not privacy. Therefore, the FCC has no authority to impose additional conditions on aggregate customer information, and certainly not ones related to privacy.[3]

The FCC's motivating concern seems to be that aggregate information could be re-identified. While that could occur in some instances, it certainly does not justify costly new FCC rules that carriers make public commitments, adopt contractual prohibitions, or engage in monitoring. Carriers already have a business and legal interest in ensuring that aggregate customer information is truly de-identified. If it is

---

[2] *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 (2014) (*TerraCom NAL*). My only consolation is that this Notice concedes that prior section 222 rulemakings had been confined to CPNI. Thus, parties had no notice that the Commission would find independent authority in section 222(a), and the *TerraCom NAL* was unlawful. Moreover, because the Commission cannot adopt rules solely on the basis of tentative conclusions in an NAL, the Lifeline privacy and security rules adopted last year must be reconsidered and discarded.

[3] I also disagree with the suggestion that all CPNI should be considered individually identifiable and, therefore, subject to the restrictions of section 222(c)(1). The plain language of section 222(c)(1) makes clear that there are different types of CPNI and they should be treated differently. Only the subset of CPNI that the statute calls "personally identifiable CPNI" is protected. De-identified CPNI, therefore, would not be subject to section 222(c)(1).

not, companies would lose the trust of their consumers and could be subject to enforcement actions for violating the law.

Just in case the authority provided by section 222 is insufficient, the Notice reverts to the familiar shotgun approach, referring to sections 201, 202, 303(b), 316, and 705 of the Communications Act, as well as Title 18 of the United States Code. The problem with citing original provisions of the Communications Act is that they were clearly never intended to cover such conduct. Moreover, why would Congress subsequently have adopted a privacy provision for telephone call records—section 222—if all of these other sections already contained the necessary authority to regulate privacy and security? Such a reading would render an entire provision superfluous. Of course, no controversial item would be complete without citing to section 706 of the 1996 Act and the virtuous cycle, and my views on that are well known. But it is particularly ludicrous here given that only one percent of broadband non-adopters listed privacy or security concerns as a primary reason for not using the Internet at home.[4]

Having mangled the statute, the Notice proceeds to upend existing privacy structures that, by most accounts, have been providing sufficient protections for consumers, including broadband customers. The only intervening change is that reclassification gave certain stakeholders another bite at the apple to achieve everything on their privacy wish lists. So in yet another proceeding, instead of making incremental changes, like those offered by industry groups to align any FCC rules with the well-established FTC standards and precedent, the Commission decides to go to the extreme, possibly jeopardizing the entire effort.

Under the FTC choice framework, the privacy baseline is set so that it is consistent with the privacy preferences of most consumers. Accordingly, "whether a practice requires choice turns on the extent to which the practice is consistent with the context of the transaction or the consumer's existing relationship with the business, or is required or specifically authorized by law."[5] Given the FTC's long history and expertise with consumers' privacy expectations, it has determined that consent is not needed for many common activities, while others require consumer choice.[6] However, the highest degree of protection, affirmative express consent (opt-in), is reserved for specific uses like making material retroactive changes to privacy representations or collecting sensitive information, such as information about children, financial and health information, Social Security numbers, and precise geolocation data.[7]

This stands in sharp contrast to the Notice, which seeks to override consumer preferences with the Commission's own policy choices. Moreover, instead of setting a baseline and making adjustments over time to address any actual instances of harm, the FCC would mandate specific practices upfront. The Notice proposes a rigid consent regime that assigns one of the three categories—inferred, opt-out, and opt-in—based on the entity accessing the information, irrespective of consumer expectations. Under the

---

[4] National Telecommunications and Information Administration, Exploring the Digital Nation: Embracing the Mobile Internet at 26 (2014), https://www.ntia.doc.gov/files/ntia/publications/exploring_the_digital_nation_embracing_the_mobile_internet_10162014.pdf.

[5] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers at 38-39 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[6] For example, no consent is needed for first party marketing by affiliates where the relationship is clear to consumers. *Id.* at 41-42.

[7] *Id*. at 57-60.

proposal, the bulk of activities would fall into opt-out and opt-in categories. In fact, opt-in would even be the default—another catch-all—for all situations not expressly discussed in the item, regardless of how most consumers would view such uses.

Additionally, the Notice goes so far as to suggest that some privacy practices "may be prohibited under the Act." That is, the FCC could take away consumer choice altogether. So much for the promise on the "fact" sheet that "[i]t's about permission and protection, not prohibition."

What are these practices that are so harmful that they might need to be banned? Well, contrary to certain statements to the press, one of them is a popular program offered by a major provider that enables consumers to receive a discounted price for a premium service if they agree to allow the company to use their web browsing information to provide tailored ads. The Notice acknowledges that a "substantial majority" of customers elected to participate in the program. However, it cautions that consumers in these types of situations may not understand what they are trading. Really?

To be fair, the Notice includes a token question on whether such practices should be subject to heightened notice and choice protections. But in light of the fact that these programs are singled out for a standalone section on practices that might be prohibited, and given that the Notice asks questions such as whether simply offering such practices violates providers' baseline duty under section 222(a) to protect the confidentiality of customers' proprietary information, anyone can see where this is headed.

The Notice makes no effort to explain why ISPs and their customers should be subject to more onerous consent requirements or no choice at all. Instead, the Commission simply assumes its conclusion and seeks confirmation that it is right. Indeed, there is no reason for the Notice to describe consumer expectations because it is irrelevant to the FCC's analysis. The agency knows best, and must save consumers from their poor privacy choices. I find this regulatory paternalism to be extremely offensive.

It is also unwarranted given that the FTC framework had protected broadband consumers' privacy until reclassification removed that authority. The Notice does not identify any flaws in that framework that would require a different approach here. The only answer seems to be that the FCC is seizing the chance to up the ante, whether consumers want it or not, in order to be seen as the true defender of consumer privacy.

I see little reason to believe that this new regime would not impede innovation and disrupt the interworking of the Internet. By mandating unnecessary—and for some consumers unwanted—privacy practices, the Commission increases costs for businesses. The opt-in regime, in particular, will impair the ability of companies to develop new uses for information—cutting them off before ever exploring the possibilities and positives in the marketplace—that could provide additional revenue streams and that consumers might find beneficial. That means less capital to invest in broadband deployment, higher prices and fewer choices for consumers, and slower adoption. In short, it would initiate a vicious cycle.

Additionally, applying heightened standards to one segment of the Internet economy will hamstring competition with the largest users of consumer data. The FCC seeks comment on the issue, but also notes that the FTC could simply vigorously enforce its own rules. That's not a fair suggestion because, as I already noted, it's a completely different rulebook.

To further increase costs, the Notice proposes to micromanage privacy notices. The Notice seeks comment on required disclosures, as well as the timing and placement of such notices. It could also include the creation of privacy dashboards that would enable consumers not only to adjust privacy settings but to even request deletion of data that the consumer no longer wants the provider to maintain.

And to ensure the providers are complying with these new mandates, the Notice proposes new recordkeeping requirements, supervisory review processes, and certifications.

Shifting gears a bit, I was not shocked to see that the Notice also addresses data security given prior enforcement actions on the subject. I was surprised, however, that it would contradict the other cybersecurity item already on circulation. That Policy Statement, which seems dubious in its own right, sets forth a process for carriers to meet with the Commission, supposedly on a voluntary basis, to discuss risk management practices. Ever since I watched one of the Advisory Committee meetings and heard how the term "voluntary" was being defined, I had deep suspicions about whether the process would truly be optional for providers.

Here, the Notice confirms my concerns by proposing that carriers conduct regular risk management assessments, and even seeks comment on whether the FCC should specify the manner in which the risk management assessments should be designed and conducted "instead of allowing the BIAS provider to determine the specifics." Notably, the Policy Statement also promised that, to further protect participants, none of the voluntary discussions would be used as part of a rulemaking proceeding. And some Advisory Committee participants agreed to support the Policy Statement process because, if they didn't, they recognized that the Commission might proceed to adopt rules. Well there's no need for the supposed "protection" now that the Commission has initiated the proceeding to adopt rules.

It is important to note that, while cybersecurity is important, the Act does not provide the FCC with any authority in this space. The Notice asserts that section 222(a) requires providers to protect the "security, confidentiality, and integrity" of customer data. But it says nothing of the sort. The FCC is simply inserting its own language into the Act. It is also worth noting that the FCC has not been included in any of the Congressional legislative efforts on this topic, not even as a consulting agency. Therefore, the Commission should not presume to freelance in this area.

The Commission also continues to struggle to find the right balance on data breach notifications. In last year's *TCPA Omnibus Order*, the Commission provided an extremely narrow exception to TCPA liability to permit one class of companies to make a limited number of calls per event. Moreover, the relief was subject to conditions that have made it unworkable in practice. In this Notice, the Commission would mandate that a class of companies contact consumers in the event of a breach, and within a certain period of time. However, it takes time for a company to investigate whether a breach has actually occurred and to determine the scope of the impact. If companies have to notify consumers before they have all the facts, it may be over-inclusive, leading to customer confusion. I hope that the Commission will be open to adjusting its proposal as it hears from outside parties with more experience with these situations.

In addition to the major substantive concerns, I was also alarmed to see the Commission acting on issues that should be completely outside the scope of this proceeding and its jurisdiction. For example, the Commission seeks comment on prohibiting carriers from including mandatory arbitration clauses in contracts with their customers. Here again, the Commission assumes that consumers don't understand the choices they are making and is willing to impose needless costs on companies by mandating how they do business.

I am also compelled to remark on a term that is used more than two dozen times throughout this item: harmonize. It seems that this is a new code word for increasing regulation. The Commission proposes expanding CPNI for broadband, and then seeks comment on "harmonizing" the rules for voice. As if we need to pile on new obligations for legacy voice service. Likewise, the Commission seeks to "harmonize" this new proposal with rules applicable to video service. Of course, by the time the

Commission gets around to changing those rules, it will doubtlessly find other necessary "improvements," and that will require further harmonization. Pretty soon, we will end up in a regulatory arms race.

Finally, I must raise a reality check about how ISPs may use the collected information. Unlike governmental entities using the information to potentially threaten and undo the freedom of individuals, the high crime and misdemeanor at issue here is the ultimate desire of some to want to market a commercial product to others. Simply put, they may want to try to sell you something that you would actually enjoy purchasing. It is as if we all forgot how the Internet economy actually works today. There is a trade-off—consumers receive "free" stuff offered by Internet companies while in return the companies receive other things, such as data to place targeted ads, that consumers may or may not want but, at the same time, may be completely comfortable with in the context of the overall package. Heightening the limitations on the use of information, as contemplated by this item, will impact every other pricing component of Internet access and eventually edge providers.

While I would not have been able to support this item in any event as it is based on a flawed legal theory, I had hoped for the sake of institutional credibility that the policy framework would be a sensible one. Unfortunately, that is not the case and I must dissent.