Published on *The National Law Review* https://natlawreview.com

The FCC's Net Neutrality Order: Going Beyond Blocking, Throttling, and Fast Lanes

Article By:

Eduardo R. Guzmán

After months of debate and speculation, the Federal Communications Commission (FCC) issued its order last month reclassifying broadband internet access service (BIAS) as a telecommunications service subject to common carriage regulations under Title II of the Communications Act.[1] In so doing the FCC reversed its order of 2017 classifying BIAS as an information service under the Act (and thus not subject to common carriage regulation). It also reinstated rules that prohibit BIAS providers from blocking or throttling access to content, sites, or applications (or categories of content, sites, or applications), prioritizing third-party traffic in exchange for consideration, prioritizing traffic from affiliates, and engaging in broadly defined unreasonable discrimination in the offering of BIAS.

Much has been written about the scope and impact of these rules. Highlighting important differences to the prior open Internet rules, the FCC now defines throttling more expansively to include not only degrading access but also speeding up access to content, sites, or applications (or categories of content, sites, or applications). Adding ambiguity to the matter, the FCC did not rule whether popular and widely used practices such as data caps and zero rating—and newer techniques for mobile networks, such as slicing—violate the new rules. The debate regarding the impact of common carriage regulation on investment continues, as the lengthy and spirited exchanges between the FCC majority and one of the dissenting commissioners show.

Less attention has been given to the order's implications beyond blocking, throttling, and fast lanes. The FCC now has much clearer authority to regulate privacy, data security, and cybersecurity issues impacting BIAS and providers of BIAS. But its less than definite definition of what qualifies as BIAS raises thorny questions as to which Internet-related services are covered by the new rules and the FCC's regulatory reach. And it added an additional wrinkle to an already challenging compliance question by refusing to expressly preempt state laws and regulations dealing with BIAS.

Privacy and Data Security

The FCC now has full authority over privacy and data security issues related to BIAS and the offering of BIAS to customers.[2] The *2024 Open Internet Order* declares that Section 222 of the Communications Act, which protects customer proprietary network information (CPNI), applies to BIAS and BIAS providers. Among other things, that provision requires telecommunications carriers to protect the confidentiality of CPNI and limits when carriers may use CPNI. The FCC clarified that the

detailed CPNI rules implementing Section 222 do *not* apply to BIAS or BIAS providers but warned that it can directly enforce the statutory requirements of Section 222 even in the absence of rules specifically applying to BIAS.

There has been speculation that the FCC will attempt to enact BIAS-specific privacy rules, as it did in 2016 after it first reclassified BIAS as a telecommunications service. That may prove challenging given that Congress in 2017 nullified the 2016 BIAS-specific privacy rules under the Congressional Review Act. The *2024 Open Internet Order* nevertheless hints at a different approach that could moot the discussion over the application of the Congressional Review Act. Not only did the FCC stress that the application and enforcement of Section 222 did not entail running afoul of the Congressional Review Act, but it also emphasized that it has authority under Section 201 to impose and enforce privacy-related obligations beyond CPNI.[3] A better preview of the FCC's likely approach may be the orders it adopted days before issuing the *2024 Open Internet Order* imposing $196 million in fines against the largest national mobile services providers in the United States for sharing consumer location information with third parties without prior customer consent. We reported on that action in a prior post. Underlying those orders was the FCC's finding that customer location information is CPNI when obtained from wireless networks. While the orders did not rely on classifying mobile BIAS services as telecommunications services, they signaled a willingness to interpret CPNI broadly and use Section 201 more aggressively in the privacy space.

Cybersecurity

The *2024 Open Internet Order* makes clear that the reclassification of BIAS opens the door to a more definitive mandate to enforce cybersecurity standards across broadband networks.[4] The FCC emphasized the importance of safeguarding the integrity and security of critical Internet infrastructure. An extension of requirements to participate in network outage reporting systems should be expected, as are requirements for BIAS providers to implement cybersecurity and risk management plans to protect their networks. The *2024 Open Internet Order* also mentioned efforts to address vulnerabilities threatening the security and integrity of the Border Gateway Protocol—and soon afterward the FCC adopted a Notice of Proposed Rulemaking proposing rules to address those vulnerabilities. Telecommunications carriers already were subject to many of these regulations, but now BIAS-only providers will also be covered.

But what is BIAS?

The real challenge coming out of the *2024 Open Internet Order* may be understanding to whom these new obligations will apply. The reclassification of BIAS and the new open Internet rules clearly apply to the mass-market retail broadband Internet access services that ISPs offer to residential customers and small businesses. It also plainly does *not* apply to business data services (e.g., special access), content delivery network (CDN) services, virtual private network (VPN) services, web hosting, data storage, and WiFi hotspots for patrons in commercial establishments. But the FCC's approach creates uncertainty beyond these specifically identified services. For example, the FCC declined to categorically exclude 5G IoT services and inflight entertainment and connectivity services from the definition of BIAS, holding that they would have to be examined case-by-case. It also purported to exclude "non-BIAS data services" (formerly "specialized services") from the definition of BIAS, but then adopted an ambiguous definition of what qualifies as such and cautioned that even the examples it had previously provided would not always be considered non-BIAS data services.[5] In short, determining whether a particular service (even those offered by non-ISPs) could nonetheless fall within the definition of BIAS or be subject to FCC enforcement will require going beyond labels and examining the service's functionality and capacity.

The prospect of expansive FCC authority and federal rules over BIAS and BIAS providers does not mean the end of state-level regulation. The FCC refused to "categorically preempt all state or local regulation affecting BIAS in the absence of any specific determination that such regulation interferes" with the *2024 Open Internet Order*.[6] It also declined to rule that BIAS was "exclusively interstate", which makes it easier for state regulatory authorities to regulate aspects of BIAS and fend off preemption arguments. And it suggested that state regulatory authorities would be able to enforce FCC requirements.[7]

The 2024 Open Internet Order is only the opening salvo of what could be a complex and thorny regulatory process. We will continue to monitor developments and provide our analysis in this space.

---

1. *Safeguarding and Securing the Open Internet*, Declaratory Ruling, Order, Report and Order, and Order on Reconsideration, WC Docket No. 23-320, WC Docket No. 17-108 (May 7, 2024) (*2024 Open Internet Order*).
2. *See 2024 Open Internet Order*.
3. *Id.* ¶ 324 ("[T]he Commission has previously taken enforcement action against providers under section 201 for violation of consumers' privacy rights"); *id.* ¶ 351 ("[T]he Commission's privacy authority under Title II is not limited to CPNI. Sections 222(a) and 201 also impose obligations, which we enforce, on carriers' practices with regard to non-CPNI customer proprietary information and PII.")
4. *Id.* ¶¶ 42-50.
5. *Id.* ¶ 195.
6. *Id.* ¶ 268.
7. *Id.* ¶¶ 268, 271.

National Law Review, Volume XIV, Number 166