Written Testimony of
Professor Daniel Lyons
Boston College Law School

Before the Connecticut Senate Energy and Technology Committee
Hearing on Senate Bill 4, An Act Concerning Data Privacy, Net Neutrality, Cyber Security and Fairness in Data Usage in the New Age of a Digital Workforce

March 9, 2021

Chairmen Needleman and Arconti and Members of the Committee,

Thank you for allowing me to comment today. My name is Daniel Lyons, and I am a professor at Boston College Law School, where I teach and research in the areas of telecommunications, Internet law, and federalism. I am also a Visiting Fellow at the American Enterprise Institute, where I have published over 100 blog posts on tech policy issues, including the net neutrality and privacy issues addressed in Senate Bill No. 4. But I should note that I am testifying on behalf only of myself in today's proceeding.

I wish to make two points about Senate Bill No. 4. First, Connecticut may lack authority to enact the bill's net neutrality provisions. Section 1 conflicts with the Federal Communications Commission's carefully balanced regulatory approach and is arguably preempted under the Supremacy Clause. Moreover, as applied to wireless broadband providers, it is likely preempted in part by the Communications Act. At a minimum, the committee should wait for the Biden Administration to act on the issue, because the bill may inadvertently conflict with the FCC's future plans. Second, even if Connecticut could enact SB No. 4, there are good arguments about why net neutrality and ISP-specific privacy rules are bad policy.

I. SB No. 4 May Be Preempted

A. SB No. 4 Frustrates a Federal Objective

In the 2018 *Restoring Internet Freedom (RIF) Order*,[1] the Federal Communications Commission repealed federal regulations similar to those that Senate Bill No. 4 seeks to impose on broadband Internet service providers. The Commission found that rules prohibiting blocking, throttling, paid prioritization, and the general conduct standard were likely to inhibit consumers and competition. Instead, the agency chose to rely on enhanced transparency and disclosure requirements, against the backdrop of antitrust and consumer protection laws, to promote innovation while protecting against the risk of consumer harm. In *Mozilla v. Federal Communications Commission*, the D.C. Circuit Court of Appeals upheld this rule and found the agency's explanation reasonable.[2]

[1] Restoring Internet Freedom, 33 FCC Rcd. 311 (2018) ("RIF Order").
[2] Mozilla v. Federal Communications Commission, 940 F.3d 1 (2019).

The *RIF Order* expressly preempted "any state or local measures that would effectively impose rules or requirements" that the order repealed or rules that would otherwise be "inconsistent with the federal deregulatory approach" taken in the order.[3] This is consistent with the FCC's long-time approach to state regulation of ISP network traffic management practices. Though the agency has flip-flopped over the years on what the rules should be, it has consistently explained on a bipartisan basis that traffic management rules are primarily a federal function. For example the Obama-era FCC's 2010 *Open Internet Order* explained that the Commission had authority to preempt state regulations that interfere with valid federal objectives and announced it would preempt state laws on a case-by-case basis.[4] The 2015 *Open Internet Order* (upon which SB No. 4 is modeled) was more explicit, explaining it would preempt "state regulations that would conflict with the federal regulatory framework or otherwise frustrate federal broadband policies."[5]

The *Mozilla* court vacated the RIF Order's express preemption provision, finding that the agency failed to ground the clause in a lawful source of statutory authority.[6] But while vacating the *express* preemption provision, the court was careful to preserve the issue of *conflict* preemption, labeling it "wholly premature."[7] Conflict preemption occurs when a state law "frustrate[s] the accomplishment of a federal objective."[8] The agency cannot assert conflict preemption in the abstract; as the *Mozilla* court explained,

> Because a conflict-preemption analysis involves fact-intensive inquiries, it mandates deferral of review until an actual preemption of a specific state regulation occurs. Without the facts of any alleged conflict before us, we cannot begin to make a conflict-preemption assessment in this case, let alone a categorical determination that any and all forms of state regulation of intrastate broadband would inevitably conflict with the 2018 Order.[9]

At first blush, it may seem odd that *Mozilla* can strike down the *RIF Order*'s preemption clause, and yet leave the door open for a future court to nonetheless find a state law is preempted. The resolution of this seeming conundrum lies in the difference between express and conflict preemption. Whereas express preemption turns on congressional intent—whether Congress has granted the agency authority to preempt state law in an area—conflict preemption focuses on the effect of dual sovereigns pursuing different objectives in an area of shared regulatory authority. Where state law frustrates the accomplishment of a federal objective, the state law must yield—preempted not by some express statutory or regulatory command, but by the Supremacy Clause itself.[10]

---

[3] *RIF Order* at 427.
[4] Preserving the Open Internet, 25 FCC Rcd. 17905, 17970 n.374 (2010).
[5] Protecting and Promoting the Open Internet, 30 FCC Rcd. 5601, 5804 (2015).
[6] *Mozilla*, 940 F.3d at 86.
[7] Id.
[8] Geier v. American Honda Motor Co., Inc., 529 U.S. 861, 873 (2000).
[9] *Mozilla*, 940 F.3d at 81-82.
[10] *Geier,* 529 U.S. at 873.

The Supreme Court's decision in *Geier v. American Honda Motor Co*. illustrates how conflict preemption works in an analogous regulatory environment.[11] *Geier* involved an automobile safety standard promulgated by the Department of Transportation pursuant to the National Traffic and Motor Vehicle Safety Act of 1966, which granted the agency broad authority to establish "appropriate Federal motor vehicle safety standards" in the public interest.[12] After experimenting with several different standards over time that varied in onerousness, the agency settled on requirement that automobile manufacturers equip some, but not all, of their vehicles with passive restraints such as airbags.[13] After being injured in an automobile crash, the plaintiff sued the manufacturer, arguing that failure to provide an airbag violated state tort law despite being in compliance with the federal standard.[14] The Act contained an express preemption clause, but the court found this inapposite, as the clause did not address tort claims. Nonetheless, the court found that the tort claim conflicted with the federal standard.

The plaintiff argued that the agency merely set a minimum airbag standard, and states were free to adopt more stringent requirements above that minimum.[15] But the court found otherwise, noting the agency "deliberately provided the manufacturer with a range of choices among different passive restraint devices" designed to "bring about a mix of different devices introduced gradually over time."[16] The agency specifically rejected an all-airbag standard, in part because of concerns about public backlash.[17] The court found the state law claim was preempted because a "rule of state tort law imposing a duty to install airbags in cars such as petitioners' would have presented an obstacle to the variety and mix of devices that the federal regulation sought and to the phase-in that the federal regulation deliberately imposed."[18]

The *RIF Order* reflects a similar exercise of the agency's judgment regarding the appropriate way to regulate the broadband industry. In *Brand X*, the Supreme Court held that the Telecommunications Act's definitions were ambiguous, and therefore the Commission was free to classify broadband Internet access service as either a Title I information service or a Title II telecommunications service.[19] The scope of the agency's Title I power ranges, based upon how the agency interprets ambiguous grants of authority like Section 706 and what rules the agency determines are helpful to execute its clearly defined statutory powers. Similarly, the scope of Title II varies, as the statute gives the agency the power to forbear from applying particular

[11] Id. at 861.
[12] National Traffic and Motor Vehicle Safety Act of 1966, 80 Stat. 718, 15 U.S.C. § 1381 et seq. (repealed by Pub.L. 103-272 § 7(b), July 5, 1994, 108 Stat. 1379).
[13] *Geier,* 529 U.S. at 864.
[14] Id. at 865.
[15] Id. at 874.
[16] Id. at 874-875.
[17] Id. at 879.
[18] Id. at 863.
[19] Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967 (2005).

provisions if the agency determines that "enforcement of the regulation or provision is not necessary" or if forbearance is otherwise "consistent with the public interest."[20]

This flexibility creates a broad menu of potential regulatory options for the agency to choose from, all of which are permissible under the Communications Act as interpreted by *Brand X*. On one end of the spectrum, the agency could opt for a policy of complete nonregulation, disclaiming any interest in broadband whatsoever. On the other end, it could apply the full panoply of Title II obligations to broadband providers, up to and including rate regulation pursuant to tariffs filed with the Commission. Between these poles lie a host of potential regulatory bundles, including minimalist Title I requirements, a more robust common-law regulatory structure constructed using a more intensive Title I process, or a Title II-lite regime that waives most, some, or virtually none of that chapter's traditional common carriage requirements.[21]

The *RIF Order* represents the agency's policy judgment regarding the optimal regulatory bundle from among these options. Contrary to the claim made by some net neutrality advocates, the agency did not foreswear any jurisdiction over broadband access and abandon the field. Rather, it opted to classify broadband as an information service and subject it to specific transparency and disclosure obligations, coupled with enforcement of existing consumer protection and antitrust laws. But it decided against more intensive common carrier-like economic restrictions, which were likely to harm consumers and innovation. Significantly, the *Mozilla* court found this analysis to be a reasonable exercise of the Commission's authority.[22]

My sense is that SB No. 4 "frustrate[s] the accomplishment of a federal objective" by imposing precisely those duties that the Commission explicitly repealed as harmful, and by reducing the flexibility that the Commission recognized as important to future growth. Admittedly, a recent federal court has suggested otherwise, finding that a similar challenge to California's net neutrality rules is unlikely to succeed. No written decision has yet issued, but it appears the court was swayed by the mistaken belief that there is a regulatory vacuum over broadband service, which is an incorrect understanding of the current regulatory framework. Here, as in *Geier*, the agency has adopted a careful regulatory scheme that balances trade-offs between more and less onerous requirements. More onerous state restrictions upset that balance and therefore may be preempted by the Supremacy Clause.

B. The Communications Act Likely Preempts Portions of SB No. 4

A second preemption issue arises with regard to SB No. 4's attempt to regulate wireless broadband. The Communications Act draws the line between federal and state authority in

[20] 47 U.S.C. § 160 (2018).
[21] See, e.g., Daniel A. Lyons, *Net Neutrality and Nondiscrimination Norms in Telecommunications*, 54 ARIZ. L. REV. 1029, 1041 n.64 (2012) (discussing Title II–lite regime).
[22] *Mozilla*, 940 F.3d at 72-73.

different places for different technologies. For mobile services, this boundary is determined by Section 332(c):

> [N]o State or local government shall have any authority to regulate the entry of or the rates charged by any commercial mobile service or any private mobile service, except that this paragraph shall not prohibit a State from regulating the other terms and conditions of commercial mobile services.

Under this statute, states may not regulate rates charged for mobile service—though they are allowed to regulate "other terms and conditions" of commercial mobile services. The Sixth Circuit explored the interplay between these clauses in *Cellco Partnership v. Hatch*, which struck down a Minnesota law preventing wireless providers from changing a customer's rate without getting the customer's affirmative consent. Minnesota argued that this was a consumer protection measure that fell within the safe harbor for "other terms and conditions," but the court ruled that it affected rates and therefore was preempted. Generally, the court explained, the safe harbor applies to "neutral application of state contractual or consumer fraud laws," not industry-specific measures that directly affect rates.

SB No. 4's prohibition on paid prioritization arguably constitutes improper rate regulation. This restriction effectively sets a rate—namely, zero—for priority delivery of congestion-sensitive traffic over the last-mile network. If so, this provision would also face preemption.

C. SB No. 4 May Clash with Biden Administration Policies

Of course, the incoming administration has very different views about net neutrality and has signaled a desire to revisit the *RIF Order*. At present, the Federal Communications Commission is deadlocked and so there is not a majority to overturn the order. But if the Commission repeals the *RIF Order* and adopts net neutrality rules at the federal level, SB No. 4 will be at best superfluous and at worst it could conflict with the Commission's future plans.

As noted above, SB No. 4 adopts the language of the 2015 Open Internet Order prohibiting blocking, throttling, and paid prioritization, as well as the unreasonable interference/disadvantage standard. It is quite possible that a future FCC Order may adopt different language, which could leave this bill in conflict with the Commission's objectives. But even if the FCC uses the same language, there is a risk that federal and state authorities interpreting the same language differently. This is particularly true of vague, relatively open-ended standards such as the command not to "unreasonably interfere with or disadvantage" relationships between consumers and edge providers.

II. Potential Unintended Consequences of Net Neutrality Rules

Moreover, even if Connecticut could enact state net neutrality requirements, it's not clear that it should do so. The committee should consider carefully the unintended consequences of a ban on all paid prioritization. Net neutrality proponents are correct that prioritization can be misused for anticompetitive purposes. But the reality is that there are good and bad reasons why a network

might prioritize some traffic over others. A flat ban on prioritization risks jeopardizing these benefits because of fear the practice will be abused—yet the abuse feared is already largely prohibited by antitrust law.

Net neutrality advocates often argue that without a ban on paid prioritization, internet service providers (ISPs) would divide the network into fast lanes and slow lanes. This rhetoric envisions broadband networks as segmented into various lanes of travel, with packets sorted into channels that move at different maximum speeds at all times. But this is only a metaphor, and distorts how the Internet actually works. All Internet traffic on a network moves at the same speed. The problem is congestion: what happens when users want to transmit more data than the wire can physically manage at a particular moment. In this case, the network must drop some packets and allow others to go through. The dropped packets then must be resent, which delays the delivery of the service.

Of course, congestion is not constant; it is more likely to occur at times of peak use. The solution to chronic congestion is to expand network capacity. But additional capacity is expensive. It is often uneconomic to build a network with zero congestion at peak time because this would create significant excess capacity at off-peak periods—like building an 8-lane highway that sits empty for 23 hours each day. And a zero-congestion network today may nonetheless face congestion in the future, as consumers' appetites for data grow. So some amount of congestion is inevitable.

So how can we address that congestion? One can drop packets randomly, which seems to align with net neutrality's ethos that all traffic should be treated the same. But there's a problem with this model: Different internet content and applications have different susceptibility to congestion. A user loading an email or a webpage is unlikely to notice if some packets are dropped and resent. But streaming video or FaceTime may buffer, which erodes the consumer's experience and makes the product less reliable.

An alternative would be to drop packets intelligently, by deprioritizing traffic that is less sensitive and prioritizing traffic that is more sensitive to congestion. This would improve the experience for streaming video (for example) without measurably degrading the web surfer's experience. But this is precisely the solution that many net neutrality advocates would prohibit. Note, though, that because different applications have different susceptibility to congestion, a ban on prioritization is anything but neutral: it favors apps like email and web-browsing that are not congestion-sensitive, over more bandwidth-intensive services that are. My concern is that requiring the Internet to always function exactly as it does now can have unintended consequences for innovation, as companies seeking to develop the next big application are stymied by an Internet architecture that cannot change to meet their needs.

When pressed, some net neutrality advocates will concede the value of intelligent traffic management. The problem isn't prioritization, they claim, but paid prioritization: the protection against congestion in exchange for a fee. But once one acknowledges the need to prioritize traffic, one then needs a method of prioritization. One solution is a central planning model: An

expert (likely either a government bureaucrat or a broadband company engineer) can develop a master list of all internet-based applications and sort it by priority. This raises difficult questions about the sorting rule. Is it based entirely on how quickly the service erodes, or is the expert choosing, say, telemedicine over cat videos because he or she feels telemedicine is more important? This raises the prospect of government or ISPs picking winners and losers, which is precisely what net neutrality is supposed to prevent. The expert may miscalculate an application's sensitivity. And even if the expert gets the list right, it's hard to maintain in a dynamic environment where new services are being added and existing services are being improved, which makes today's congestion-sensitivity calculations less relevant tomorrow.

Alternatively, we can use the price mechanism, which is the way we generally allocate scarce resources (like bandwidth) in a capitalist society. Hayek taught that prices reveal information that markets can use to sort claims on a decentralized basis. An application developer will only purchase prioritization if its service is congestion-sensitive. When it is willing to do so, and at what price, reveals how susceptible it is compared to other apps. This sorts apps with less error and fewer value judgment than a centrally planned solution.

The concern, of course, is that the price mechanism harms those who cannot afford to pay for prioritization. But these concerns are somewhat overrated. First, apps that are not congestion-sensitive have no need to pay for prioritization. Second, even in a net-neutral world, there are other ways that well-funded companies can — and do — pay to reduce their exposure to congestion, such as using content delivery networks to bypass the public internet.

III. ISP-Specific Privacy Rules are Bad Policy

The bill's privacy provisions are also based on a now-defunct FCC rule. But unlike the net neutrality rule, the FCC's privacy rules never came into effect, as Congress repealed them through the Congressional Review Act procedure, which prohibits the agency from adopting a new rule substantially the same as that which was repealed.

Repeal of that misguided effort was the right decision for two reasons. First, given the competitive dynamics of the Internet ecosystem, it makes very little sense to single out Internet service providers to bear a greater privacy burden than other companies. Second, when leveling the playing field, an opt-out privacy model is preferable to an opt-in model.

First: As many (including me) noted when the FCC passed its rules, it is a mistake to create a new, more stringent privacy regime that applies to ISPs but not Internet-based companies such as Google, Amazon, and Facebook. This creates an unlevel playing field in the market for digital advertising dollars. Supporters justify this disparate burden by highlighting the allegedly "privileged place" that ISPs occupy in the network, by controlling the wires that carry information to and from the consumer's home. But this is misleading. My home broadband provider can only gather, at most, information about my online activity while I am at home. By comparison, Google can capture all my activity while logged into my Google account whether at

home, at work, or on mobile networks, if, like me, you use a phone powered by Google's Android operating system. Furthermore, technological limitations such as encryption and use of virtual private networks significantly limit what information ISPs can gather from the data to which they have access. The notion that an ISP is in a privileged position vis-à-vis edge providers is, at best, questionable.

Putting ISPs at a competitive disadvantage in the digital advertising market is especially problematic because ISPs were late to the digital advertising game. Studies suggest that as much as 2 out of every 3 dollars spent on digital advertising goes to only two companies: Google and Facebook—which is an astounding figure when you consider the broad array of advertising-supported content available online. ISPs have the potential to be disruptive innovators in this market. This means that a regulatory regime that makes it harder for ISPs, but not edge providers, to collect and monetize data not only tilts the playing field, it tilts it in favor of incumbents and against innovation. Ultimately that's bad for consumers and for competition.

It's worth noting that there is an important distinction between the now-defunct FCC privacy rule and SB No. 4. The FCC did not choose between a two-tier privacy regime and a uniform set of rules to govern all companies equally. Rather, the FCC created ISP-specific rules because it lacked jurisdiction over the rest of the Internet ecosystem. Supporters of the FCC rule saw it as a transition measure—they hoped that an opt-in rule for ISPs would prompt lawmakers to create similar opt-in measures for other companies as well. It is also worth noting that the FCC rule never came into effect, as Congress invalidated the rule through the Congressional Review Act process before its effective date.

Second, Even if regulators sought to impose a uniform privacy rule across the Internet ecosystem, it's a mistake to favor an "opt-in" regime over an "opt-out" one. Proponents of the bills discussed above make a mistake that is, unfortunately, all too common in this debate: they consider privacy in a vacuum, without considering the role that consumer data plays as the lifeblood of the Internet ecosystem. It is the monetization of customer data that allows Google, Facebook, and countless other companies offer the "free" services that we all take for granted as the modern internet experience—and may someday bring broadband prices down as ISPs cover more of their fixed costs with advertising rather than subscription dollars.

In both an opt-out and an opt-in regime, consumers have ultimate control over how their data is collected and used. The difference is that an opt-in rule dries up the pool of data available for monetization, by prohibiting companies from accessing data on consumers who are indifferent to the practice. At a minimum, this reduces revenue available for research and innovation and can cause companies to reduce the quality of their products to compensate. At worst, an opt-in regime means those companies might start charging for services that they currently provide for free and higher prices for goods that could otherwise be subsidized through advertising—thus widening the digital divide by stratifying available services between the haves and have-nots.

IV. Conclusion

It’s worth noting that the current light-touch regulatory framework for traffic management is the historical approach under which the Internet as we know it grew and flourished. For most broadband providers, the rules that SB No. 4 seeks to impose were binding only during a brief period from 2015 through 2017. And the federal government has never enforced binding opt-in rules on ISPs. Contrary to claims by some advocates, the federal government has not abandoned the field, leaving a regulatory void that states must rush to fill. The Federal Trade Commission has authority to police anticompetitive behavior and has exercised that authority, including in the privacy arena. Although broadband providers do have some incentives to behave in an anticompetitive fashion, antitrust law protects consumers from the harms that net neutrality advocates fear most, just as it shields consumers from anticompetitive harm everywhere else in American society. It is a mistake to adopt prophylactic state rules because of the specter of a few bad actors that antitrust law already disciplines, particularly given the risk that these new rules may have severe unintended consequences.