How to Strengthen the Open Internet NPRM by Closing Loopholes and Matching the 2015 Open Internet Protections

Professor Barbara van Schewick[1]
Stanford Law School
March 12, 2024

EXECUTIVE SUMMARY

When the FCC announced it would be restoring the net neutrality protections that the FCC eliminated in 2017, the agency said it wanted to restore the 2015 net neutrality protections.

I strongly support this goal, and the Notice of Proposed Rulemaking includes many of the protections included in the 2015 Open Internet Order.

But the Notice of Proposed Rulemaking misses some critical protections in the 2015 Order, creating potential loopholes for Internet Service Providers (ISPs) to exploit.

These include provisions concerning:

- **Throttling:** The proposed rules inadequately address the issue of ISPs manipulating internet traffic by speeding up applications or classes of applications. The 2024 protections need to explicitly prohibit both negative and positive discrimination among apps.
- **Reasonable Network Management:** The NPRM misses a crucial part of the 2015 Order's definition of "reasonable network management," which opens a loophole that ISPs could exploit to circumvent net neutrality principles. Reasonable network management must be as application-agnostic as possible and technically justified.
- **Specialized Services/Non-BIAS Data Services:** ISPs are seeking to bypass Open Internet protections under the guise of "specialized services," particularly with 5G fast lanes. The FCC needs to prevent ISPs from exploiting this label to create fast lanes that are otherwise prohibited.
- **Transparency:** The FCC's 2017 Repeal Order significantly weakened ISP transparency reporting. Restoring the 2015 transparency rules would help people choose the internet service plan that is best for them by restoring ISP reporting requirements on network performance, including during peak times and by geographic area.
- **Interconnection:** The NPRM lacks the 2015 Order's explicit prohibition against ISPs circumventing net neutrality where data enters their networks, often referred to as the point of

[1] M. Elizabeth Magill Professor of Law, Professor (by courtesy) of Electrical Engineering, and Director, Center for Internet and Society, Stanford Law School. Professor van Schewick has not been retained or paid by anyone to participate in this proceeding.

interconnection. ISPs exploited this loophole in the past to degrade internet performance in order to force apps to pay the ISPs, impacting millions of Americans.

- **State Net Neutrality Laws:** The FCC needs to preserve state net neutrality laws as they provide additional protections and enforcement and have not proven burdensome for ISPs. Federal net neutrality protections should set the minimum standard, allowing states to enforce stricter rules.
- **Zero-Rating:** The FCC should set clear rules against ISPs using harmful zero-rating to distort competition or favor certain applications, drawing on California's net neutrality law as a model.

Throttling

The new rules need to clearly prohibit ISPs from speeding up *and* slowing down applications and classes of applications.

The problem: The proposed no-throttling rule clearly prohibits ISPs from slowing down apps or classes of apps.[2] That's important. It prohibits ISPs from distorting competition and interfering with user choice by degrading disfavored apps or kinds of apps. ISPs may not slow down all online telephony apps to keep people paying for the ISPs' expensive calling plans. ISPs may not limit the amount of bandwidth available to online video services, while allowing all other apps and services to use all available bandwidth, either. We should be free to choose how we use our data, not our ISPs.

However, the rule does not explicitly ban ISPs from *speeding up* an application or class of applications. Even if the FCC believes the rule prohibits that, the lack of an explicit ban means AT&T could speed up YouTube while all other video is buffering – or speed up all online gaming while online phone calls break up, and then argue it's allowed. That would force the FCC to relitigate the issue.

Why it matters: As the 2015 Order recognized, speeding up some applications but not others, is just as harmful as slowing down some applications but not others.[3]

An ISP can distort competition and interfere with user choice by slowing down the disfavored apps or by speeding up the favored apps. Putting Google Meet in a fast lane, while leaving Microsoft Teams in the slow lane directly distorts competition among video conferencing apps. Offering a 5G fast lane only to online games, but not to online telephony apps, makes it harder for Signal, WhatsApp, or Vonage to compete with carriers' traditional telephony services.

Thus, not explicitly banning ISPs from speeding up websites, applications or services creates a potential loophole that bypasses the ban on slowing down websites, applications or services.

How to fix the problem: The FCC needs to clarify that its no-throttling rule prohibits positive *and* negative discrimination among apps and classes of apps, subject to reasonable network management.

[2] 2023 Open Internet Notice of Proposed Rulemaking ("2023 Open Internet NPRM"), paras. 154-155.

[3] 2015 Open Internet Order, para. 126.

Reasonable Network Management

The new rules need to ensure that network management is driven by technical needs and, to the extent possible, doesn't discriminate against particular apps or categories of apps.

The problem: The NPRM's rules against blocking and throttling have an exception for reasonable network management, but the NPRM fails to include the requirement that such network management must be as application-agnostic as possible and that practices need to be primarily technically justified.

This allows ISPs to claim that blocking or slowing down individual applications or classes of applications (including ones that compete with their own services) is reasonable network management. That's what Comcast claimed in 2007 when the FCC investigated Comcast's secret blocking of peer-to-peer services.

Why it matters: Failing to include the application-agnostic and technical-justification clauses from the 2015 Open Internet Order threatens to turn the reasonable network management exception into a loophole. It reduces certainty in the market and makes the Open Internet protections harder to enforce by requiring the FCC to re-litigate a decade of net neutrality precedents to decide how to interpret the term.

A well-defined reasonable network management exception is a critical component of a meaningful net neutrality regime.[4]

As the experience of the United States, Canada, and the United Kingdom has shown, ISPs have routinely blocked or discriminated against specific applications or types of applications to manage congestion when they were not prohibited from doing so.[5] These practices harmed Internet users and edge providers and created significant collateral damage. For example, ISPs in the UK routinely managed congestion by singling out specific applications or classes of applications such as online video or peer-to-peer file-sharing, instead of, for instance, managing congestion without targeting specific applications or classes of applications.

These practices prevented many users from using the Internet as they wanted during peak times – e.g. even if a user shut down all applications except for a video, the video would only load at a slow speed. That kind of network management made it harder, if not impossible, for affected applications to reach their users, and also interfered with applications like online gaming that were inadvertently caught up in discriminatory network management practices not targeted at them. By contrast, Internet users in countries that require ISPs to manage their networks as application-agnostic as possible avoided these problems.

Under the application-agnostic standard, ISPs are prohibited from targeting specific apps or classes of apps to manage their network, if they can avoid it. To manage congestion, networks reduce each person's usage, without targeting particular apps or kinds of apps, until the congestion passes.

---

[4] See van Schewick, 2015, Net Neutrality and Quality of Service, pp. 137-140 (discussing the exception for reasonable network management), available at http://www.stanfordlawreview.org/wp-content/uploads/sites/3/2015/01/67_Stan_L_Rev_1_van_Schewick.pdf.

[5] For an in-depth case study and analysis, see Cooper & Brown, 2015, Net Neutrality: Discrimination, Competition, and Innovation in the UK and US, ACM Transactions on Internet Technology, Volume 15, Issue 1, Article No.:2, https://dl.acm.org/doi/10.1145/2700055. See also van Schewick, Net Neutrality and Quality of Service, pp. 96-97.

That ensures that we, not our ISPs, get to decide which apps have priority. ISPs have no idea which apps are most important at any given time; for instance, in times of congestion, one person might be looking up a YouTube video on how to perform CPR, another might be uploading an important work document before a deadline, while a third may be using a video conferencing app for a critical job interview. ISPs are in no position to know which usage is more important.

The application agnostic method has been the standard since the 2008 Comcast Order, in which the FCC ordered Comcast to stop blocking peer-to-peer file sharing apps.[6]

How to fix the problem: To ensure people can continue to use the internet as they want even when the network is busy, the new reasonable network management exception needs to include the 2015 requirement that network management must be "as application-agnostic as possible."[7] This requirement is missing from the NPRM.

In addition, the FCC needs to restore the 2015 requirement that network management be primarily technically justified.[8] ISPs are already arguing that they can invoke business reasons for network management, possibly to justify their arbitrary throttling of video quality on less expensive mobile plans. In other words, not requiring that network management be driven by technical necessity would allow ISPs to use network management as an excuse to engage in behaviors that are otherwise banned or unfair.

Specialized Services/Non-BIAS Data Services

The new Order needs to ensure that ISPs cannot circumvent the Open Internet protections by using the "specialized services" label.

The problem: In a coordinated push, ISPs and their trade associations are urging the FCC to open a dangerous loophole in the order under the guise of "specialized services."[9, 10]

ISPs want to use the specialized services label to offer fast lanes to *any* application, not just to those that can't function without it.[11] That would allow ISPs to get around the ban on fast lanes.

---

[6] 2008 Comcast Order, 23 FCC Rcd. 13,028 (2008), paras. 47-51.

[7] See, e.g., 2015 Open Internet Order, para. 220.

[8] See 2015 Open Internet Rules § 8.2(f): "A network management practice is a practice that has a primarily technical network management justification, but does not include other business practices." See, e.g., Jordan, 2023, Open Internet Comments, pp. 6-7.

[9] Specialized services are services that are delivered over the same last-mile connection as broadband internet access service. Under the framework established by the 2010 and 2015 Open Internet Order, the Open Internet protections generally do not apply to such services, as long as the service does not evade the Open Internet protections, does not provide a functional equivalent to broadband internet access services, and does not negatively affect the capacity for and performance of broadband internet access services. See, e.g., Open Technology Institute at New America, Public Knowledge, van Schewick & Jordan, 2024, Written Ex Parte filed March 11, 2024, pp. 5-6, https://www.fcc.gov/ecfs/search/search-filings/filing/103120890811342.

[10] Most of the following section is adopted almost verbatim from van Schewick, 2024, February 12, 2024 Ex Parte Letter, pp. 4-5, https://www.fcc.gov/ecfs/search/search-filings/filing/102081616713724.

[11] See, e.g., T-Mobile, 2023, Open Internet Comments, pp. 24-37; CTIA February 23, 2024 ex parte letter, p. 10.

The current proposal seems to allow that, turning it into a giant loophole.[12]

Why it matters: A new technology called 5G network slicing makes it easy for ISPs to create fast lanes for select apps or kinds of apps. ISPs want to use that technology to create 5G fast lanes for certain applications such as online video conferencing, online video, and online gaming. They want to decide which apps should get a fast lane and charge the app provider for the fast lane.

T-Mobile is currently testing 5G fast lanes for online video conferencing; it has said it wants to do the same for online gaming. AT&T has tested 5G fast lanes for online gaming.

This is an urgent threat to core net neutrality protections.

Despite the fancy new jargon, 5G network slices are nothing new; they are just another way to give some apps special treatment, and the FCC's net neutrality regime is nuanced enough to handle them.

The FCC's 2015 Open Internet rules rightly prohibited ISPs from charging application providers for a fast lane to the ISP's customers (the so-called "ban on paid prioritization"). This protects competition, innovation, and free speech by ensuring that companies and speakers without deep pockets have an equal chance to compete and be heard.

The 2015 Open Internet rules also ensured that ISPs cannot distort competition by creating fast lanes only for select apps (e.g., only for Google Meet, but not for Zoom) or classes of apps (e.g., only for online gaming, but not for online telephony).

But if ISPs can offer special fast lanes to applications such as online video conferencing, online video, and online gaming using the "specialized services" label, these protections are meaningless.

To create these fast lanes, ISPs want to be free to take away bandwidth from the broadband internet access service they have already sold to their customers and use it for mislabeled "specialized services." That means these mislabeled "specialized services", for which people or application providers would pay extra, would work well even during times of congestion. Since the apps or category of apps in these fast lanes are chosen by the ISP, that means ISPs will be picking winners and losers among applications or categories of applications. Meanwhile, people's ability to access all the apps and services on the Open Internet would suffer, with less bandwidth (and more congestion) to use the applications and services of their choice.

ISPs say they would never do anything that harms their internet access customers, and that requiring them to disclose any negative impact of specialized services is enough.[13]

But disclosure requirements alone will not sufficiently protect Americans.

As the 2012-2015 interconnection disputes showed, ISPs are more than willing to hurt their internet access customers if it increases their profits. The FCC is restoring substantive net neutrality protections

[12] van Schewick, 2024, Open Internet Reply Comments, pp. 20-23, https://www.fcc.gov/ecfs/document/1011865034201/2.

[13] See, e.g., CTIA, 2024, February 23, 2024 Ex Parte Letter, pp. 3-4, 12; T-Mobile, 2024, February 23, 2024 Ex Parte Letter, pp. 2-4.

against blocking and paid fast lanes *exactly because* competition and disclosure alone do not prevent ISPs from violating net neutrality. Additionally, transparency isn't transparent.

Most people have no idea why an application or their connection is slow at times – not knowing if the slow performance is caused by their device, their WiFi connection, the application they are trying to use or their ISP. Figuring that out often requires very sophisticated tools. And even if someone is aware that their connection is now slow because their provider is setting aside a wide swath of bandwidth for these kinds of fast lanes, switching ISPs takes time and energy – and many people are still locked into long-term contracts with their ISP. Switching doesn't help if there's no alternative or all ISPs are engaging in the same practice, as they currently do with video throttling on mobile plans.

How to fix the problem: The 2015 Open Internet Order prohibited ISPs from using specialized services to evade the Open internet protections.[14] This important protection is missing from the NRPM.[15] The FCC needs to restore this critical requirement.[16]

To close the specialized services loophole, the FCC must clarify that offering special treatment to apps such as online gaming, online telephony or online video that can function on the normal internet evades the Open Internet protections.[17, 18] That will prevent ISPs from using specialized services to circumvent net neutrality, while still providing a safety valve for innovation by allowing ISPs to offer specialized services to applications such as remote surgery whose stringent requirements for reliability and delay cannot be met over the Open Internet.

This clarification mirrors the dividing line that BEREC, the EU's top telecom regulator, drew in 2016 to differentiate between permissible specialized services and impermissible specialized services that circumvent net neutrality. That has worked well in practice to prevent circumventions.

To ensure specialized services do not harm people's ability to use their internet connections, the FCC also needs to clarify the 2015 requirement that specialized services may not negatively affect the performance

[14] For a more detailed discussion, see, e.g., van Schewick, 2024, Open Internet Reply Comments, pp. 7-12.

[15] 2023 Open Internet NPRM, paras. 64-65.

[16] See also, e.g., Open Technology Institute at New America, Public Knowledge, van Schewick & Jordan, 2024, Written Ex Parte filed March 11, 2024, pp. 6-8; INCOMPAS, 2024, Open Internet Reply Comments, p. 6.

[17] For the precise language that the FCC should adopt, see Open Technology Institute at New America, Public Knowledge, van Schewick & Jordan, 2024, Written Ex Parte filed March 11, 2024, pp. 6-8 ("The FCC should clarify that providing a different type of service to support an application or class of applications as a non-BIAS data service (or as part of a non-BIAS data service) evades the Open Internet protections unless the particular type of application requires a specific level of quality of service, which is objectively necessary for the specific type of application, that cannot be met over a well-provisioned broadband Internet access service in compliance with the Open Internet protections (including via the type of application-agnostic, user-controlled, and user-paid Quality of Service described [in the filing]"), https://www fcc.gov/ecfs/search/search-filings/filing/103120890811342. See also, e.g., INCOMPAS, 2024, Open Internet Reply Comments, p. 5.

[18] In a limited exception to the clarification of evasion proposed above, fixed and mobile network operators should continue to be allowed to provide special treatment to their facilities-based legacy telephony services (e.g., VoLTE offered by cellular carriers) and linear broadcasting IPTV services. These services should be grandfathered in as legitimate specialized services that do not circumvent the Open Internet rules to account for these operators' reliance interests. For a precise definition of this exception, see ibid., pp. 8-9.

of broadband internet access, including during times of congestion, and that ISPs need to continue to improve the capacity for and performance of broadband internet access over time.[19]

Transparency

The new Order should restore ISP reporting requirements about network performance, both by geography and peak usage time, so that people can make better decisions when choosing an internet plan.[20]

The problem: When the FCC eliminated all substantive net neutrality protections in 2017, it kept a transparency rule, but removed many disclosure requirements.

For example, after 2017, ISPs are no longer required to prominently display the required information on a publicly available website and when people buy internet access.

Under the 2017 transparency rule, submitting the information to the Commission is enough.

Why it matters: Many of the disclosure requirements that the FCC eliminated in 2017 are critical for consumers trying to find the internet service plan that best meets their need.

For example, after 2017, ISPs are no longer required to disclose the amount of packet loss, and they have stopped doing so.

That's a problem. Packet loss is critical for many real-time applications such as online video conferencing. For example, applications like Zoom and Microsoft Teams recommend a packet loss of 2% or less. Thus, the 2017 disclosure rule makes it impossible for consumers that need to use online video conferencing for work, school, or other purposes to determine which of the potential internet service plans allows them to do so.

After 2017, ISPs are no longer required to separately disclose the performance of their plans during peak times, when everyone is online, which creates congestion.

That's a problem because performance on a network can vary wildly throughout the day. Speeds during peak times will often be the most relevant for consumers, but after 2017, consumers are no longer able to compare ISPs using this metric.

Similarly, after 2017 ISPs are no longer required to disclose the actual quality of internet plans by geographic areas. Especially on mobile networks, network performance often varies considerably, depending on the amount of spectrum, and the quality of that spectrum, in each area. To find the internet service plan that is right for them, consumers need to know the actual quality of the networks in their area.

[19] For the precise language that the FCC should adopt, see Open Technology Institute at New America, Public Knowledge, van Schewick & Jordan, 2024, Written Ex Parte filed March 11, 2024, pp. 9-11. See also van Schewick, 2024, Open Internet Reply Comments, pp. 23-28.

[20] The information in this section is based on Jordan, 2023, Open Internet Comments, pp. 7-20. For a detailed analysis, including a discussion of relevant data, see ibid.

How to fix the problem: The FCC should restore the 2015 transparency rule, along with the transparency requirements defined in the 2015 Order and the FCC's 2016 Advisory Guidance. This will help consumers make educated decisions when trying to find an internet service plan that best fits their needs.

Interconnection

The new Order should clarify that last-mile ISPs can't use practices related to interconnection to evade the FCC's network neutrality protections.

The problem: The 2015 Open Internet Order explicitly prohibited ISPs from circumventing the FCC's net neutrality protections at the point where data enters their networks.[21] The NPRM is missing this critical requirement.[22]

As a result, ISPs have an opening to circumvent the FCC's net neutrality protections at the point of interconnection. Thus, instead of blocking a website as it is transported over the ISP's network, the ISP can just block or slow it down as it enters the ISP's network. So Comcast could effectively slow down all competing online video applications at the edge of its network to give itself a competitive advantage.

Why it matters: Allowing ISPs to circumvent net neutrality protections at the point of interconnection would create a known loophole that ISPs have exploited in the past, in ways that caused harms to tens of millions of Americans. The FCC's 2010 Open Internet rules did not apply to the point of interconnection. From at least 2013 to 2015, major ISPs serving more than 75 percent of American broadband customers deliberately let connections into their networks congest to extract fees from the Internet companies delivering data to the ISPs' Internet service customers – data these customers had requested.

As a result, customers of these ISPs experienced significant performance problems in the afternoon and evening: Internet applications, websites and services entering the ISPs' networks through these congested connections became effectively unusable, even though customers had paid their ISPs for good connections to the Internet. Employees couldn't connect to their company's network. Schools couldn't upload their payload data. Skype calls dropped. And online video stuttered.

These problems only ended when affected companies decided to pay (as Netflix did in early 2014) or, for those that refused to pay, when the FCC's 2015 Open Internet Order went into effect. In response to these problems, the FCC decided to include oversight over interconnection in the 2015 Open Internet Order.

The 2015 Order explicitly made clear that interconnection practices could not be used to evade net neutrality protections.[23] This was further emphasized in Chairman Wheeler's signing statement, where he said, "Today's Order also asserts jurisdiction over interconnection. The core principle is the Internet must remain open. We will protect this on the last mile and at the point of interconnection."

Interconnection negotiations between the largest ISPs and their interconnection partners (e.g., apps, CDNs, or transit providers) happen behind closed doors and under NDA, where the public and the FCC are blind. Without an explicit statement that interconnection practices can't circumvent net neutrality,

[21] 2015 Open Internet Order, para. 206.

[22] 2023 Open Internet NPRM, para. 187.

[23] 2015 Open Internet Order, para. 206.

ISPs can credibly threaten in negotiations to use measures that effectively throttle applications, CDNs, or transit networks. And the threatened party would not have a clear avenue to counter that the threat is a violation of the FCC's order.

Since the 2017 repeal, parties looking to connect to the nation's largest ISPs are facing actual congestion or threats of congestion (e.g. throttling) if they do not pay access fees to the ISP.[24]

How to fix the problem: The FCC's 2015 Open Internet Order prohibited ISPs from using interconnection practices to circumvent the FCC's net neutrality protections. It did so by saying that the FCC would review ISPs' interconnection practices case-by-case under Sections 201 and 202 of the Communications Act, which prohibit ISPs from engaging in unjust and unreasonable practices and unjust and unreasonable discrimination. The 2023 NPRM rightly includes this important safeguard.

However, the text of the 2015 Order clarified that the FCC would use this case-by-case review to ensure that last-mile ISPs cannot use practices related to interconnection to evade or circumvent the FCC's network neutrality protections.[25] This requirement is missing from the FCC's 2023 proposal.[26]

There's simply no reason to allow large ISPs to continue making or even expand the demands and threats they have been making since the 2017 repeal. The 2024 Order, like the 2015 Order, should explicitly state that interconnection agreements can't be used to evade the Open Internet protections.

State Net Neutrality Laws

We prevented the worst consequences of the repeal of federal net neutrality protections by fighting for state net neutrality laws and orders. These kept pressure on ISPs and provided enforcement mechanisms for individuals in states covered by these laws and orders. The laws survived repeated court challenges. We need to preserve them.

Federal net neutrality protections should be the floor, not the ceiling, for net neutrality protections.[27]

[24] See, e.g., Lumen, 2024, Open Internet Comments, pp. 2, 6-7, 11-13; Lumen, 2024, March 5, 2024 Ex Parte Letter, pp. 2-3; Declaration of Dave Schaeffer in Support of Opposition to Preliminary Injunction Motions (2020), ACA et al. v. Becerra (District Court for the Eastern District of California), paras. 79-80, https://www.fcc.gov/ecfs/document/102261063431042/4.

[25] 2015 Open Internet Order, para. 206.

[26] 2023 Open Internet NPRM, para. 187.

[27] See, e.g., ACLU, 2023, Open Internet Comments, pp. 12-15; EFF, 2023, Open Internet Comments, pp. 22-23; Public Knowledge, 2023, Open Internet Comments, pp. 96-103; Writers Guild of America, 2023, Open Internet Comments, pp. 7-8.

ISPs can comply with net neutrality laws state-by-state,[28] and ISPs have not provided any evidence that state net neutrality laws have been burdensome to comply with. [29] Complying with both state and federal law is the bedrock of our federalist system.[30]

Existing state net neutrality laws in California, Colorado, Maine, Oregon, Vermont, and Washington State simply provide additional layers of protection: each codifies a subset of the FCC's 2015 Open Internet protections. As a result, they reinforce and support, not contradict, the FCC's proposed Open Internet protections.

Federal and state enforcement coexist to protect people's rights in many areas of law.[31] Allowing states to continue to enforce their own net neutrality laws improves protections by allowing the FCC *and* the states to enforce net neutrality, and letting states handle minor cases the FCC might not have time for.

States may also be able to react faster to new technical developments and provide a laboratory to experiment with specific approaches.[32]

Zero-rating

The FCC should prohibit ISPs from using harmful forms of zero-rating to distort competition, advantage themselves, or favor companies and speakers with deep pockets.

The problem: Zero-rating is the practice of not counting certain websites and services against a consumer's monthly data cap. Zero-rated apps don't use people's data, while all other apps do. Harmful zero-rating schemes almost invariably favor the ISP's own services or those of giant platforms like Facebook or YouTube.

The FCC proposes to evaluate zero-rating case-by-case under the general conduct rule, like in 2015. That leaves ISPs free to engage in the most egregious forms of zero-rating and forces future FCCs to spend precious time and judicial resources litigating obvious violations of net neutrality.

Why it matters: Most people are worried about hitting their data cap, so they will prefer websites and apps that do not eat up their data over those that do. Thus, harmful zero-rating is just another tool that lets ISPs give some websites an advantage over others and pick winners and losers online.

---

[28] See, e.g. Declaration of Scott Jordan, former FCC Chief Technologist, Attachment # 6 to Opp'n. to Prelim. Inj., *Am. Cable Ass'n., et al v Becerra*, No. 2:18-CV-02684 (E.D. Cal. Sept. 6, 2020), ECF No. 57.

[29] To the contrary, the California Attorney General affirmatively noted in his comments that there have not been operational issues in that state. California Attorney General, 2023, Open Internet Comments, p. 4.

[30] As the Supreme Court recently said in *National Pork Producers Council v. Ross*, 598 U.S. 356, 364 (2023), "Companies that choose to sell products in various States must normally comply with the laws of those various States."

[31] As the Supreme Court said in *Kansas v Garcia*, 140 S. Ct. 791, 806 (2020), "in the vast majority of cases where federal and state laws overlap, allowing the States to prosecute is entirely consistent with federal interests."

[32] As the Supreme Court observed, "We have long recognized the role of states as laboratories for devising solutions to difficult legal problems." *Oregon v. Ice*, 555 U.S. 160, 171 (2009).

The 2015 Open Internet Order gave the FCC the power to look into such schemes, but did not prohibit any outright. Taking advantage of the lack of a clear prohibition, AT&T and Verizon zero-rated their own online video services. AT&T Wireless customers on a 3GB plan were able to watch as much video from DirectTV or HBO Max as they liked, but watch only 9 minutes of video a day from providers AT&T didn't own. That's not a meaningful choice, and makes it harder for other voices to compete and be heard.

Other apps that wanted to be zero-rated had to pay AT&T and Verizon to be included. Such "sponsored data" plans create the same harms as requiring apps to pay for a fast lane. They benefit incumbents with deep pockets, while squeezing out startups, small businesses, and non-profits.

A 2017 report from the FCC (later discarded by Chairman Pai) found that these plans violated net neutrality. Building on these insights, California's net neutrality law explicitly prohibited ISPs from zero-rating select apps and requiring apps to pay to be zero-rated. Faced with this clear prohibition, AT&T and Verizon ended their anticompetitive zero-rating schemes in California the moment the law became enforceable – without waiting for enforcement actions.

That's good for internet users and competing online video providers. People should be free to choose which videos they want to watch – whether that's Netflix, Twitch or their local church's Sunday service, without the company they pay to get online trying to influence their choices.

Curtailing harmful zero-rating schemes not only expands users' choices, it leads to better data plans. When harmful zero-rating plans were prohibited in other countries, consumer data caps rose dramatically and the monthly price for unlimited data plans fell.

California's net neutrality law wisely allows non-discriminatory zero-rating programs that treat all data the same, regardless of what people use the data for (so-called "application-agnostic" zero-rating). Your ISP can still exempt data usage from your cap at certain times of day or as a promotion; it just can't force you to use that data on a specific site. ISPs in other countries have innovated with offers such as unmetered data from midnight to 6 a.m., unmetered data on the weekend, or letting users choose hours per month where their data usage is uncounted.

How to fix the problem: The FCC should adopt the same rules for zero-rating as California's net neutrality law.[33] That would ban the most harmful forms of zero-rating, prohibiting ISPs from zero-rating their own apps or select popular apps and from charging apps to be zero-rated, while leaving room for ISPs to offer consumer-friendly zero-rating plans.

[33] SB 822, §§ 3101(a)(5), (6) & (7) & 3101(b), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB822.

Barbara van Schewick is a leading expert on net neutrality, a professor of Law and, by courtesy, Electrical Engineering at Stanford University, and the director of the Stanford Law School Center for Internet and Society. She is the author of Internet Architecture and Innovation (MIT Press 2010). Parts of this text draw on her earlier writing on net neutrality.

Barbara van Schewick's salary, research support, and travel are funded through the general budget of Stanford Law School and are independent of the budget and funding of the Center for Internet and Society. She has received no direct or indirect corporate funding, and the Center does not accept corporate funding for its network neutrality-related work.*

**Unless covered by event organizers.*