**Before the**
**Federal Communications Commission**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the matter of | ) | |
| Safeguarding and Securing The Open Internet | ) | WC Docket No. 23-320 |

**COMMENTS OF CENTER FOR DEMOCRACY & TECHNOLOGY**

Eric Null
Center for Democracy & Technology
1401 K St NW Ste 200
Washington, D.C. 20005

January 17, 2024

**Table of Contents**

## Statement of Interest

The Center for Democracy & Technology files these comments in response to the Federal Communications Commission's Notice of Proposed Rulemaking on Safeguarding and Securing the Open Internet (2023 Open Internet Notice).[1] CDT is a nonprofit public interest organization dedicated to promoting openness, innovation, freedom, and privacy online – a mission that aligns closely with the 2023 Open Internet Notice.

## Introduction

The internet has been transformational over the past 25 years. Among many things, the internet has changed commerce, how we communicate, how we create and share creative works, how we find new friends and engage with our communities, and how we engage with politics and government. People can do almost anything they want on the internet, from buying clothes to watching TV or videos on sites like YouTube to talking to their friends and family to streaming their own lives or discussing their creations.

The COVID-19 pandemic supercharged the importance of the internet. With stay-at-home orders across the country and people generally being less willing and able to meet in person, people turned to the internet. Classes and meetings went online to Zoom, Google Meet, Microsoft Teams, and other services. Students' homework was assigned, completed, and turned in online. People, who were able to, worked from home, placing substantial burdens on the network. Internet traffic, particularly on home broadband connections, surged 30-40% during the

[1] Notice of Proposed Rulemaking, Safeguarding and Securing the Open Internet, Dkt. No 23-320, FCC 23-83 (Oct. 20, 2023) (hereinafter "2023 Open Internet Notice").

pandemic lockdowns.[2] According to one survey, 93% of people said their children received online educational instruction during the pandemic, and 90% of people said their internet connection was essential or important for them during the pandemic.[3] Despite some people easily transitioning to life on the internet, unfortunately, some lower income people and people who lived in rural areas experienced trouble with their internet connections, whether speed, reliability, or quality.[4]

The pandemic confirmed what many long already knew—the internet is essential to functioning in society. Congress came around to that idea as well. It invested significant sums of money into building out and ensuring broadband affordability. In 2020, in response to the pandemic, passed a $3.2 billion Emergency Broadband Benefit program to help low-income people afford broadband connections by providing a discount of up to $50 per month (or $75 on Tribal lands) on a broadband service.[5] Then, in 2021, Congress injected $65 billion dollars into a variety of broadband initiatives, including $42 billion going to infrastructure build-out itself, and $14 billion going to the Affordable Connectivity Program (ACP), a replacement for the Emergency Broadband Benefit, which allowed a $30 per month discount for low-income people

[2] Stephen Shankland, *Broadband Use Surged More than 30% During Pandemic, Industry Group Says*, CNET (Apr. 7, 2021), https://www.cnet.com/tech/services-and-software/broadband-use-surged-more-than-30-during-pandemic-industry-group-says.
[3] Colleen McClain *et al*., *The Internet and the Pandemic*, Pew Research (Sept. 1, 2021), https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic.
[4] *Id*.; Shara Tibken, *Millions of Americans Can't Get Broadband Because of a Faulty FCC Map. There's a Fix*, CNET (Feb. 19, 2021), https://www.cnet.com/home/internet/features/millions-of-americans-cant-get-broadband-because-of-a-faulty-fcc-map-theres-a-fix.
[5] Emergency Broadband Benefit, FCC, https://www.fcc.gov/broadbandbenefit (last visited January 17, 2024).

to connect to a broadband service.[6] As of August 2023, the ACP had connected more than 20 million American households.[7]

Underpinning this transformation is the fact that the government has, since the early 2000s, adopted a policy that Internet Service Providers (ISPs) or Broadband Internet Access Service providers (BIAS providers) should largely be neutral when providing access to content online.

Between 2005 and 2017, the FCC had some form of open internet policy. The FCC, under chairman Michael Powell, classified cable internet as an information service.[8] Around the same time, it also adopted the Internet Policy Statement.[9] That statement required that ISPs provide access to the internet subject to four rules: (1) consumers are entitled to access the lawful internet content of their choice; (2) consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement; (3) consumers are entitled to connect their choice of legal devices that do not harm the network; and (4) consumers are entitled to competition among network providers, application and services providers, and content providers.[10] When the FCC attempted to enforce the policy statement against Comcast for interfering with legal BitTorrent traffic in 2007, the DC Circuit held that the FCC lacked

[6] Jon Brodkin, *Biden's "Historic" $65 Billion Broadband Plan Approved by Congress*, Ars Technica (Nov, 8, 2021), https://arstechnica.com/tech-policy/2021/11/congress-oks-42-billion-to-deploy-100mbps-broadband-in-unserved-areas; *see also* Affordable Connectivity Program, FCC, https://www.fcc.gov/acp (last visited January 17, 2024).
[7] Fact Sheet, 20 Million+ Households Enrolled in the ACP, FCC, https://docs.fcc.gov/public/attachments/DOC-396000A1.pdf.
[8] Declaratory Ruling and Notice of Proposed Rulemaking ¶ 7, Appropriate Regulatory Treatment for Broadband Access to the Internet over Cable Facilities, Dkt. No. 02-52, FCC 02-77 (Mar. 15, 2002).
[9] Policy Statement, Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, Dkt. No. 02-33, FCC 05-151 (Sept. 23, 2005), https://docs.fcc.gov/public/attachments/FCC-05-151A1.pdf.
[10] *Id*. at ¶ 4.

authority to impose those open internet requirements on Comcast's cable modem (Title I) service.[11]

After that decision, the FCC passed open internet rules in 2010 that prevented BIAS providers from blocking or unreasonably discriminating against lawful internet traffic.[12] The 2010 Open Internet Order also imposed transparency requirements, requiring disclosure of various network practices, performance characteristics, and commercial terms.[13] In the ensuing court challenge, *Verizon v. FCC*, the DC Circuit held that nondiscrimination rules were common carrier requirements, and the FCC lacked authority to place common carrier requirements on companies not classified as telecommunications carriers under the Communications Act.[14]

In 2015, the FCC took the court's advice and reclassified BIAS providers as Title II telecommunications providers and imposed strong open internet rules including no blocking, no throttling, no paid or affiliated prioritization, a general conduct rule, and an enhanced transparency requirement.[15] The FCC's authority to impose the rules came from various parts of Title II as well as Section 706. The DC Circuit in *US Telecom Association v. FCC* upheld the order in its entirety.[16]

A few years later, the FCC, under new leadership and for the first time, decided in its "Restoring Internet Freedom Order" (RIFO) to abdicate its authority over BIAS providers—not only should there be no open internet rules, but that the FCC lacked authority over BIAS providers almost completely. In the court challenge to that decision in *Mozilla v. FCC*, the DC

[11] Comcast v. FCC, 600 F.3d 642, 651-61 (D.C. Cir. 2010).
[12] Report and Order ¶¶ 63, 68, Preserving the Open Internet, Dkt. No. 09-191, FCC 10-201 (Dec. 23, 2010), https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf.
[13] *Id*. ¶¶ 54-56.
[14] Verizon v. FCC, 740 F.3d 623 (D.C. Cir 2014).
[15] Report and Order on Remand, Declaratory Ruling, and Order ¶¶ 110-185, Protecting and Promoting an Open Internet, Dkt. No. 14-28, FCC 15-24 (Mar. 12, 2015) (hereinafter "2015 Open Internet Order").
[16] US Telecom Assoc. v. FCC, 825 F.3d 674 (D.C. Cir. 2016).

Circuit looked upon the FCC's logic with some skepticism, and it remanded three specific issues back to the FCC: public safety, pole attachments, and the Lifeline program.[17] However, the court upheld the order.[18]

In the wake of the FCC's abdication, California stepped up to fill the gap. In 2018, California passed a strong open internet law, reimposing several of the same requirements on BIAS providers.[19] BIAS providers challenged the law in court, but ultimately dropped the challenge when it became clear they were unlikely to prevail after the court decided a series of preliminary motions against them.[20] Thus, thanks to California, open internet rules continue to apply to BIAS providers today. In addition, in 2019 Maine imposed a broadband privacy law that mimicked the FCC's rule from 2016 that Congress repealed (discussed further below).[21]

With the 2023 Open Internet Notice, we are once again presented with the question of whether the FCC should re-adopt most of the rules it adopted initially in 2015 to protect people from harmful behavior by BIAS providers. CDT supports reimposing these rules, and supports reclassifying BIAS providers as Title II telecommunications providers for the purpose of applying these rules and for ensuring that BIAS providers protect user privacy.

---

[17] Mozilla v. FCC, 940 F. 3d 1, 18 (D.C. Cir., 2019).
[18] *Id*.
[19] California Senate Bill 822, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB822, *see also* Cecilia Kang, *California Lawmakers Pass Nation's Toughest Net Neutrality Law*, N.Y. Times (Aug. 31, 2018), https://www.nytimes.com/2018/08/31/technology/california-net-neutrality-bill.html.
[20] Jon Brodkin, *Stung by 3 Court Losses, ISPs Stop Fighting California Net Neutrality Law*, Ars Technica (May 5, 2022), https://arstechnica.com/tech-policy/2022/05/stung-by-3-court-losses-isps-stop-fighting-california-net-neutrality-law.
[21] Peter J. Guffin *et al.*, *Maine's New Internet Privacy Law: What You Need to Know*, Nat'l L. Rev. (June 14, 2019), https://www.natlawreview.com/article/maine-s-new-internet-privacy-law-what-you-need-to-know.

**The FCC should impose strong rules prohibiting blocking, throttling, and paid or affiliated prioritization**

The FCC should re-establish strong rules prohibiting BIAS providers from blocking or throttling content, and engaging in paid or affiliated prioritization.[22] As CDT argued in 2017, "[t]he growth of the internet as a platform for free expression and as a marketplace stem from [its] openness."[23]

Edge providers benefit from an open internet because it promotes edge provider innovation and competition and allows them to operate on a more level playing field in competing for audience.[24] An open internet allows anyone with an idea or a goal to accomplish it without BIAS providers acting as an additional barrier to entry. It also reduces uncertainty for edge providers over whether they can reach, and continue to reach, their audience by preventing ISPs from, at any point, charging additional fees or blocking access to content. Without such protections, edge providers may even have to contract with every ISP on which the edge provider has a customer. Thus, the rules reduce edge provider costs and burdens, thereby increasing competition and providing consumers with more choices.

People also benefit from an open internet because it allows them to access any (lawful) content they prefer to access without having to take into account their ISP's actions. People should be able to access any legal information and services online that they prefer, which is why most people use the internet in the first place. ISPs should not be able to use their gatekeeper

[22] *See* CDT Comments at 6-7, Protecting and Promoting the Open Internet, Dkt. 14-28 (July 17, 2014) (supporting a blocking rule and a nondiscrimination rule) (hereinafter "CDT 2014 Comments"); *see* CDT Comments at 1-2, Restoring Internet Freedom, Dkt. 17-108 (July 19, 2017) (supporting the 2015 Open Internet Order) (hereinafter "CDT 2017 Comments").
[23] CDT 2017 Comments at 1; *see also* CDT 2014 Comments at 3 ("The Internet's … openness is too important to free speech and innovation to leave to chance.").
[24] CDT 2014 Comments at 7 ("[Having a nondiscrimination rule] promotes innovation and speech by ensuring that the Internet remains a relatively level playing field, a platform with low barriers to entry and rough competitive neutrality for all online speakers, competitors, and innovators.").

status to direct, nudge, or otherwise interfere with peoples' desire to access what they want to access and when.[25] Without rules in place to ensure the internet remains open, ISPs would likely begin experimenting with business models that optimized the revenue they could receive by charging both individual subscribers and edge providers.

**The FCC should expand the BIAS provider transparency requirements and continue monitoring the industry for harmful practices**

Transparency is a necessary, but not sufficient, condition of an open internet. The FCC's current approach to ensuring an open internet, primarily through the reduced transparency requirements from the RIFO, provides limited, ineffectual protections. Essentially, the RIFO protects against undisclosed open internet violations. But allowing BIAS providers to engage in blocking, throttling, and paid prioritization simply by disclosing it does not protect an open internet. Much like in privacy, where the Federal Trade Commission has long enforced against companies that do not disclose accurate data practices, a mere disclosure requirement for open internet violations will serve only to normalize the violations rather than stop them.[26] Even after almost thirty years of the Federal Trade Commission actively protecting privacy through their enforcement actions on deceptive practices, people are still confused and concerned about their privacy, and feel powerless to protect themselves.[27]

[25] 2023 Open Internet Notice, ¶ 123.
[26] Section 5 of the FTC Act allows the FTC to enforce against companies that deceive their customers as to their data practices. Rather than prevent those harmful data practices, companies merely disclose them (often in unreadable and unread privacy policies) and now people have become accustomed to privacy violations by simply being online. This phenomenon has led some to claim (incorrectly) that "privacy is dead." Neil Sahota, *Privacy Is Dead and Most People Really Don't Care*, Forbes (Oct. 14, 2020), https://www.forbes.com/sites/neilsahota/2020/10/14/privacy-is-dead-and-most-people-really-dont-care/?sh=11cba5857b73.
[27] Colleen McClain *et al.*, *How Americans View Data Privacy*, Pew Research (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy.

Competition among providers, even with transparency requirements, will not protect the open internet either. At higher broadband speeds, which are increasingly necessary for video calls and streaming entertainment (particularly during the COVID lockdowns),[28] there is little competition among providers.[29] For instance, 28% of people living in urban areas and 70% of people living in rural areas have zero or one option for the 100mbps/20mbps speed tier, meaning competition will not protect those people.[30] Further, 47% of people living in urban areas and 24% of people living in rural areas have access to two providers at that speed tier. But, if the FCC allows ISPs to block, throttle, or prioritize certain content over others, there is no guarantee that one of those two providers would provide access to the open internet—people may, instead, be forced to choose between two types of limited internet access. Even if we assumed that competition provided certainty of access to an open internet, switching comes with significant "switching costs" serving as a deterrent to changing providers, including installation fees, early termination fees, time without a connection to the internet, and the cost of new equipment.[31]

*Transparency of Terms and Network Performance.* Regardless, the FCC should impose transparency requirements on BIAS providers that are sufficient for people to determine whether the service will fit their needs. The 2010 Open Internet Order imposed several of the key transparency requirements, which the RIFO reverted back to, and which provides a baseline for the transparency rule. However, the 2015 Open Internet Order included enhanced transparency requirements that would be important to people who are making a decision on providers. Such

[28] Stan Horaczek, *As More People Work from Home, Internet Speed Requirements Have Become a Critical Issue*, Popular Science (Nov. 8, 2021), https://www.popsci.com/story/technology/work-from-home-broadband-connection-internet-fcc ("Millions of American students and employees lack the necessary connection.").
[29] 2022 Communications Marketplace Report ¶¶ 56-57, Communications Marketplace Report, Dkt. No. 22-203, FCC 22-103 (Dec. 30, 2022).
[30] *Id*. ¶ 58, Fig. II.A.29.
[31] 2015 Open Internet Order, ¶ 81.

requirements should include the disclosure, up-front, of the monthly price, additional fees, and any data caps or allowances.[32] It should also include disclosure of network performance information, such as latency and packet loss.

It is, in general, reasonable to ask network operators to know how well their networks perform and be able to report that information to the public and the FCC. More accurate, public disclosure of network performance would also allow the public to better understand how networks are improving in performance.

The reported information, however, should reflect actual experience with receiving information from the broader internet. Some speed tests are performed "on-net," where the speed tested is from the person's machine to content that is on the ISP's last mile network. That information is not terribly useful to the average user, who is likely to be attempting to find information "off-net," beyond the ISP's own network.[33] Reported information should reflect at least off-net tests, if not both.[34]

The FCC should ensure it has access to information and tools to enable it to monitor the industry and protect against further harmful practices. Transparency requirements, for instance, will allow the FCC to track the industry and ensure that broadband service is widely accessible and affordable. One very helpful requirement could be historical records of disclosures, either at

[32] 2015 Open Internet Order, ¶ 164.
[33] *See* Measurement Lab FAQ, https://www.measurementlab.net/frequently-asked-questions/#why-are-my-m-lab-results-different-from-other-speed-tests (differentiating between "on-net" speed tests that "lets you know about how your Internet connection is performing intra-network within your ISP, but it does not necessarily reflect the full experience of using the Internet," and "off-net" speed tests that "occur between your computer and a server located outside of your ISP's network. This means that traffic crosses inter-network borders and often travels longer distances. Off-net testing frequently produces results that are lower than those produced from on-net testing.") (last visited January 14, 2024).
[34] *See generally* Comments of Measurement Lab at 8, Safeguarding and Securing an Open Internet, Dkt. No. 23-320 (Dec. 14, 2023) (advocating, at the very least, a transparency rule require that ISPs, when disclosing "speed" metrics, include "from which vantage points they measured," which would allow an outside party to know if the measurement is off-net or on-net).

the Commission itself, or at the BIAS provider, at least for a certain amount of time. Longitudinal data would be particularly useful for the public and for the FCC to determine whether there are problematic network practices or network trends. For instance, a network whose latency or packet loss is constantly increasing might be a sign of a neglected system and a reason for a person to avoid that network.

*Zero Rating.* Another practice to monitor, through disclosures and direct monitoring, is zero rating. A provider, particularly a wireless provider, may impose a usage cap, but exempt certain content from the cap. If those exemptions are based on a service's ability or willingness to pay, or because they are affiliated with the BIAS provider, that would harm the open internet because competitors to the ISP's chosen or affiliated services would suffer and would harm people's ability to choose to access the services they prefer. AT&T engaged in this practice when it exempted HBO and DirecTV, two properties it owns, from its data cap.[35] There may be potentially limited circumstances that merit allowing zero rating, particularly as a strategy to encourage broadband adoption, or if the data cap is application-agnostic.[36] Disclosure requirements will provide the FCC with information it needs to help differentiate justified and harmful uses of zero rating.

*Interconnection Disputes.* The FCC should continue to monitor interconnection disputes and take action when they harm people's access to the internet. Interconnection for a long time was shrouded in secrecy, and it was "very hard to evaluate the claims and counterclaims"

[35] Jon Brodkin, *AT&T Exempts HBO Max from Data Cats but Still Limits Your Netflix Use*, Ars Technica (June 2, 2020), https://arstechnica.com/tech-policy/2020/06/att-exempts-hbo-max-from-data-caps-but-still-limits-your-netflix-use.

[36] Erik Stallman & R. Stanley Adams, *Zero Rating: A Framework for Assessing Benefits and Harms*, Center for Democracy & Technology (Jan. 2016), at 22-23, https://cdt.org/wp-content/uploads/2016/01/CDT-Zero-Rating_Benefits-Harms5_1.pdf.

regarding interconnection disputes.[37] But, it became clear that placing a cop on the interconnection beat had significant benefits to the broader public. After the FCC voted on the 2015 Open Internet Order (which indicated the FCC would begin monitoring interconnection disputes), but before it became effective, ISPs started resolving interconnection disputes. For instance, Comcast signed an agreement with Level 3 a few weeks before the 2015 Open Internet Order became effective.[38] Verizon and Cogent signed a similar agreement on a similar timeline.[39] As did AT&T and Level 3.[40]

*5G and Network Slicing.* Last, the FCC should pay attention to network slicing, a practice that is made possible through 5G wireless networks.[41] Network slicing "is the general approach of slicing up a network into customized networks with different properties for different applications."[42] As such, the very purpose of network slicing is to differentiate how the network treats some types of traffic. Without appropriate safeguards, network slicing could undermine an open internet in three ways: (1) it creates a practical way to treat some traffic different than others, thus favoring or disfavoring certain traffic based on its source, destination, or other attribute; (2) the ability to charge a premium rate for network slices capable of performing better means those premium slices will be more attractive the worse the "standard" offering performs;

---

[37] David Sohn, *Getting the Facts on Interconnection*, Center for Democracy & Technology (June 18, 2014), https://cdt.org/insights/getting-the-facts-on-interconnection.
[38] Jon Brodkin, *Comcast Ends an Interconnection Fight Before Net Neutrality Takes Effect*, Ars Technica (May 21, 2015), https://arstechnica.com/information-technology/2015/05/comcast-ends-an-interconnection-fight-before-net-neutrality-takes-effect.
[39] Jon Brodkin, *Verizon and Cogent Settle Differences, Agree to Boost Internet Quality*, Ars Technica (May 1, 2015), https://arstechnica.com/information-technology/2015/05/verizon-and-cogent-settle-differences-agree-to-boost-internet-quality.
[40] Jon Brodkin, *AT&T to Fix Internet Congestion Before It Can Be Hit with Complaint*, Ars Technica (May 11, 2015), https://arstechnica.com/information-technology/2015/05/att-to-fix-internet-congestion-before-it-can-be-hit-with-complaint.
[41] *See generally* Nick Doty & Mallory Knodel, *Slicing the Network: Maintaining Neutrality, Protecting Privacy, and Promoting Competition*, Center for Democracy & Technology (Apr. 2023), https://cdt.org/wp-content/uploads/2023/04/slicing-the-network-v3-accessrem.pdf.
[42] *Id*. at 8.

and (3) operators may end up devoting larger portions of network resources to the premium slices, which could "cannibalize the capacity available for general-purpose internet access."[43]

CDT recently released a report (attached to these comments) that makes, among others, the following recommendations regarding network slicing:

- Monitor the development of network slicing, and ask ISPs to report how they have implemented network slicing;
- Require uses of network slicing to add new types of functionalities, provide greater efficiencies, or bring other benefits, rather than dividing up the internet into tiers and cannibalizing the general internet;
- Access to network slicing needs to be open to all applications and endpoints, without preferential or anti-competitive treatment (and the prohibitions on paid prioritization and self-preferencing are a necessary part of this requirement); and
- Users should be in control of their internet quality and experience, and they should also be in control of whether their services take advantage of network slicing.[44]

**The best way for the FCC to protect people and ensure an open internet is to classify BIAS providers as Title II telecommunications services**

Over a decade of legal challenges to the FCC's authority to impose open internet obligations on BIAS providers has left one unmistakable lesson: under current law, the FCC cannot impose nondiscrimination requirements on services that are not properly classified as telecommunications providers under the Communications Act.[45] The FCC should pursue its prior light-touch approach and apply Title II to the transmission component of BIAS, and forbear from

[43] *Id*. at 19.
[44] *Id*. at 38-40.
[45] *See* Verizon v. FCC, 740 F.3d 623 (D.C. Cir 2014); US Telecom Assoc. v. FCC, 825 F.3d 674 (D.C. Cir. 2016).

several portions of Title II that do not apply or do not make sense to apply to BIAS providers.[46] Title II classification has two other benefits: application of sections 201 and 202, ensuring ongoing protection from harmful BIAS provider practices, and application of section 222, protecting privacy.

To ensure the FCC has continued authority to monitor BIAS providers and take action to protect people, the most important provisions to apply to BIAS providers are sections 201 and 202 of the Communications Act. These two provisions provide significant protections against harmful behavior. Section 201(a) is the general provision that requires providing service upon reasonable request. Section 201(b) requires that charges and practices are just and reasonable. Moreover, section 202(a) makes unjust and unreasonable discrimination in charges and practices illegal. These provisions ensure that the FCC can take action when, as described above, BIAS providers engage in harmful interconnection practices, or zero rating practices that favor BIAS provider's affiliated services, or harmful network slicing practices, or if a BIAS provider were to engage in discrimination based on protected class.[47] Further, the increased transparency proposed under the 2023 Open Internet Notice will allow the FCC to properly ensure BIAS provider practices do not cause harm.

**Title II provides important privacy authority**

Applying Title II to BIAS providers will also provide the FCC important privacy authority. As an initial matter, the FCC should under no circumstances forbear from applying section 222 (and other privacy-related provisions of the Communications Act) to ISPs. The FTC

[46] CDT 2017 Comments at 1 ("For more than a decade, the … FCC has worked to implement a system of light-touch regulation to preserve and protect the openness of the internet and the consumers and businesses that rely on it.").
[47] *See generally* Comments of Lawyers Committee for Civil Rights Under Law at 11-14, Safeguarding and Securing the Open Internet, Dkt. No. 23-320 (Dec. 14, 2023).

Act provides that the agency is "empowered and directed to prevent persons, partnerships, or corporations" from engaging in unfair and deceptive acts, "except … common carriers" subject to the Communications Act.[48] The FTC's lack of authority over common carriers is mandatory, meaning forbearance from privacy-related provisions of the Communications Act would leave ISPs with a weakened or ineffective privacy enforcer.

Title II grants the FCC several sources of authority. First, Section 222(a) states broadly that telecommunications carriers must protect the confidentiality of proprietary information of customers. Then, under section 222(c), customer proprietary network information (CPNI) has specific protections, including that it can only be used to provide the telecommunications service to the customer, unless the other use is approved by the customer. Section 201's prohibition against unjust and unreasonable practices also provides further authority for privacy enforcement.[49]

These sources of authority will be useful for protecting against privacy abuses perpetrated by ISPs. For example, the FCC has taken several important privacy enforcement actions in the past decade, including against YourTel and TerraCom for violating their wired and wireless Lifeline customers' privacy,[50] and against the major wireless carriers for selling location data to data brokers, who then sold it to third parties such as bounty hunters.[51] The FTC released a report in 2021 detailing several privacy issues with ISPS, such as ISPs combining data across product lines, collecting data beyond what is necessary to provide the service, using web data to target

[48] 15 USC § 45(2).
[49] *See* Notice of Apparent Liability for Forfeiture, TerraCom Inc., and YourTel America, Inc., File No. EB-TCD-13-00009175, FCC 14-173 (Oct 24, 2014) (citing Section 201(b) as authority for data security and privacy violations).
[50] *Id*.
[51] Press Release, FCC Proposes over $200 Million in Fines against Four Largest Wireless Carriers for Apparently Failing to Adequately Protect Consumer Location Data, FCC, Feb. 28, 2020, https://docs.fcc.gov/public/attachments/DOC-362754A1.pdf.

ads, grouping consumers using sensitive characteristics, and sharing real-time location data with third parties.[52]

Unfortunately, Congress imposed some limits on the FCC regarding privacy. After the FCC passed privacy rules under Section 222 in October 2016, Congress stepped in by early 2017 and repealed those rules under the Congressional Review Act (CRA). Repeal-by-CRA adds a caveat that the agency may not pass any substantially similar rules to what Congress repealed without further authorization from Congress.[53] However, at the very least, once reclassification occurs, the FCC can continue enforcing Sections 201 and 222 for privacy violations without running afoul of the substantially similar requirement.

The FCC should begin a privacy proceeding under reclassification with haste. Such a proceeding could allow commenters and the FCC to envision what the substance of a new rule could be. For instance, much of privacy discourse has moved on from the "notice-and-consent" model that has so far plagued U.S. law and failed to meaningfully protect people. Instead, data minimization should be the focus. Data minimization places the burden of protecting privacy on the businesses that collect, monetize, and otherwise exploit the data, requiring them to justify

[52] *A Look at What ISPs Know About You, Examining the Privacy Practices of Six Major Internet Service Providers*, Federal Trade Commission (Oct. 21, 2021), at ii-iii, https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf. The RIFO passed authority over broadband privacy back to the FTC, even though some Commissioners at the FTC believe the preferred ISP privacy enforcement agency is the FCC. Remarks of Chair Lina M. Khan Regarding the 6(b) Study on the Privacy Practices of Six Major Internet Service Providers, Federal Trade Commission (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597790/20211021_isp_privacy_6b_statement_of_chair_khan_final.pdf; Remarks of Commissioner Rebecca Kelly Slaughter Regarding the FTC Staff Report – A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers, Federal Trade Commission (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597814/slaughter_isp_report_statement_10-20-21.pdf.

[53] 5 USC § 801(b)(2). The "substantially similar" requirement has never been tested.

collecting the data as necessary for a specific purpose.[54] Given that the prior FCC privacy rules centered around consent, a data minimization approach may avoid the substantially similar requirement from the CRA and provide improved privacy protection for BIAS subscribers.

**Conclusion**

For the foregoing reasons, the FCC should reclassify BIAS providers to Title II telecommunications services, and apply strong open internet rules to them.

[54] *See* American Data Privacy and Protection Act, H.R. 8152, https://www.congress.gov/bill/117th-congress/house-bill/8152/text; Comments of EPIC *et al*. at 15-17, Safeguarding and Securing the Open Internet, Dkt. No 23-320 (Dec. 14, 2023).