EDITOR'S NOTE

Welcome to the second Issue of Volume 74 of the *Federal Communications Law Journal*, the nation's premier communications law journal and the official journal of the Federal Communications Bar Association (FCBA). In this Issue of the *Journal,* we present a combination of practitioner Articles and student Notes. This Issue provides analysis and insight on policy issues facing the communications field today, including proposals to regulate ISPs, data privacy, and how section 230 reform might be achieved, in addition to many others.

We are excited to feature two practitioner Articles in this Issue, including an Article from University of Michigan Law School Lecturer Daniel T. Deacon and an Article co-written by Christopher Terry and Caitlin Ring Carson. In the first Article, Deacon commemorates the twenty-fifth anniversary for the Telecommunications Act of 1996 with an analysis of various proposals for internet service provider (ISP) regulation. Deacon highlights the inadequacies of several recently-proposed frameworks for regulating ISPs, including the Save the Internet Act and state-level regulations. He advocates that Congress adopt a framework that mirrors commercial mobile radio services (CMRS) legislation passed in the advent of cellular voice service technology. Deacon asserts that this solution shows the most promise because it would resolve ISPs' classification under Article II of the Communications Act of 1934 and in turn give the FCC flexibility to focus on policy, rather than definitional, questions about ISPs.

In the second Article, Terry and Ring address the lack of diversity in gender and race in broadcast media ownership and the need for FCC to take appropriate regulatory action. Unlike the 1990 Supreme Court's decision in *Adarand Contractors, Inc. v. Pena*, which held that any regulations regarding preferential treatment based on race be subject to strict scrutiny review, the authors assert that such regulations should be subject to the less-stringent rational basis review. The authors argue that had the Supreme Court focused on broadcast media ownership in *FCC v. Prometheus Radio* (2021), it would have similarly reached the conclusion that rational basis review was the appropriate standard of review for regulatory decisions.

This Issue also features three student Notes written by FCLJ members. The first Note, written by Tyler Dillon, takes stock of current proposals for section 230 reform. Dillon acknowledges the importance of preserving the competitive and free market enabled by section 230 as it stands today and thus proposes a solution that would restrict section 230 immunity be limited to high-revenue companies that operate popularly-used social media platforms.

In the second Note, author Michael DeJesus examines whether the expansion of state-level consumer data privacy regulations survive inquiry under the dormant commerce clause. DeJesus focuses his analysis on the California Consumer Privacy Act and the Constitutional implications should other states adopt comparable consumer data privacy frameworks.

The third Note, James Elustondo identifies a significant circuit split on section 2510(17)(B) of the Stored Communications Act and argues that the Fourth Circuit's broad interpretation of the law in *Hately v. Watts* should

be adopted. Elustondo cautions that a narrow reading, as advanced by the Eigth Circuit, would leave consumers little recourse for hacked emails. Elustondo argues that multiple canons of construction and policy considerations support a broad interpretation of the law.

The Editorial Board would like to thank the FCBA and The George Washington University Law School for their support of the *Journal*. Furthermore, the Board would like to thank all the authors and editors who contributed to this Issue.

The *Journal* is committed to providing its readership with scholarly analysis and thought leadership on topics relevant to communications and information technology law and related policy issues. The *Journal* thus welcomes any submissions for publication, which may be directed to fcljarticles@law.gwu.edu for consideration. Any further questions or comments may be directed to fclj@law.gwu.edu. This Issue and our archives are available at http://www.fclj.org.

Merrill Weber
Editor-in-Chief

FEDERAL COMMUNICATIONS LAW JOURNAL

THE TECH JOURNAL

VOLUME 74

Published by THE GEORGE WASHINGTON UNIVERSITY LAW SCHOOL
and THE FEDERAL COMMUNICATIONS BAR ASSOCIATION

Federal Communications Law Journal

The *Federal Communications Law Journal* is published jointly by the Federal Communications Bar Association and The George Washington University Law School. The *Journal* publishes three issues per year and features articles, student notes, essays, and book reviews on issues in telecommunications, the First Amendment, broadcasting, telephony, computers, Internet, intellectual property, mass media, privacy, communications and information policymaking, and other related fields.

As the official journal of the Federal Communications Bar Association, the *Journal* is distributed to over 2,000 subscribers, including Association members as well as legal practitioners, industry experts, government officials and academics. The *Journal* is also distributed by Westlaw, Lexis, William S. Hein, and Bloomberg Law and is available on the Internet at www.fclj.org.

The *Journal* is managed by a student Editorial Board, in cooperation with the Editorial Advisory Board of the FCBA and two Faculty Advisors.

Federal Communications Bar Association

The Federal Communications Bar Association (FCBA) is a volunteer organization of attorneys, engineers, consultants, economists, government officials and law students involved in the study, development, interpretation and practice of communications and information technology law and policy. From broadband deployment to broadcast content, from emerging wireless technologies to emergency communications, from spectrum allocations to satellite broadcasting, the FCBA has something to offer nearly everyone involved in the communications industry. That's why the FCBA, more than two thousand members strong, has been the leading organization for communications lawyers and other professionals since 1936.

Through its many professional, social, and educational activities, the FCBA offers its members unique opportunities to interact with their peers and decision-makers in the communications and information technology field, and to keep abreast of significant developments relating to legal, engineering, and policy issues. Through its work with other specialized associations, the FCBA also affords its members opportunities to associate with a broad and diverse cross-section of other professionals in related fields. Although the majority of FCBA members practice in the metropolitan Washington, DC area, the FCBA has 11 active regional chapters, including: Atlanta, Carolina, Florida, Midwest, New England, New York, Northern California, Southern California, Pacific Northwest, Rocky Mountain, and Texas. The FCBA has members from across the U.S., its territories, and several other countries.

The George Washington University Law School

Established in 1865, The George Washington University Law School (GW Law) is the oldest law school in Washington, DC. The Law School is accredited by the American Bar Association and is a charter member of the Association of American Law Schools. GW Law has one of the largest curricula of any law school in the nation with more than 275 elective courses covering every aspect of legal study.

GW Law's home institution, The George Washington University is a private institution founded in 1821 by charter of Congress. The Law School is located on the University's campus in the downtown neighborhood familiarly known as Foggy Bottom.

The *Federal Communications Law Journal* is published by The George Washington University Law School and the Federal Communications Bar Association three times per year. Offices are located at 2028 G Street NW, Suite LL-020, Washington, DC 20052. The *Journal* can be reached at fclj@law.gwu.edu, and any submissions for publication consideration may be directed to fcljarticles@law.gwu.edu. Address all correspondence with the FCBA to the Federal Communications Bar Association, 1020 19th Street NW, Suite 325, Washington, DC 20036-6101.

Subscriptions: Subscriptions are $30 per year (domestic), $40 per year (Canada and Mexico), and $50 per year (international). Subscriptions are to be paid in US dollars, and are only accepted on a per-volume basis, starting with the first issue. All subscriptions will be automatically renewed unless the subscriber provides timely notice of cancellation. Address changes must be made at least one month before publication date, and please provide the old address or an old mailing label. Please direct all requests for address changes or other subscription-related questions to the journal via email at fclj@law.gwu.edu.

Single and Back Issues: Each issue of the current volume can be purchased for $15 (domestic, Canada and Mexico) or $20 (international), paid in U.S. dollars. Please send all requests for single or back issues to fclj@law.gwu.edu.

Manuscripts: The *Journal* invites the submission of unsolicited articles, comments, essays, and book reviews mailed to the office or emailed to fcljarticles@law.gwu.edu. Manuscripts cannot be returned unless a self-addressed, postage-paid envelope is submitted with the manuscript.

Production: The citations in the *Journal* conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia L. Rev. Ass'n et al. eds., 21st ed., 2021). Variations exist for purposes of clarity and at the editors' discretion. The *Journal* is printed by Joe Christensen, Inc.

Citation: Please cite this issue as 74 FED. COMM. L.J. ___ (2022).

FEDERAL COMMUNICATIONS
LAW JOURNAL
THE TECH JOURNAL
GW LAW VOLUME 74 ISSUE 2 fcba THE TECH BAR
FEBRUARY 2022

ARTICLES

Written to commemorate the twenty-fifth anniversary of the Telecommunications Act of 1996, this Essay looks forward at possible settlements regarding the nagging question of whether and how best to regulate Internet service providers. Rather than start from the standpoint that this or that policy, such as net neutrality, is good or bad, I ask more broadly who should regulate ISPs and under what general framework. I assess and critique various frameworks, including reliance on markets and antitrust; state-level regulation under a federal Title I regime; various frameworks set forward in Republican-sponsored bills; and the Save the Internet Act. I argue that all of these frameworks suffer from numerous drawbacks, such as the lack of the ability to set clear rules (as with antitrust) or insufficient flexibility (as I argue besets both Republican and Democratic-sponsored bills, in differing ways). I suggest that the legislative proposal with the most promise would be roughly based on the legislation enacted to govern the regulation of CMRS in the early 1990s. This would bring ISPs within the general Title II framework while perhaps taking certain things—such as ex ante price regulation and many forms of state-level regulation—off the table. It would also preserve the FCC's flexible role going forward, and re-channel the FCC's inquiry toward the policy-focused forbearance factors and away from endless scholastic debate about whether ISPs really "are" telecommunications carriers.

For the last several decades, the FCC has been in a stalemate with media activist organizations about the lack of diversity in broadcast media ownership. Women own less than 10% of broadcast television and AM/FM radio stations, and racial minorities own less than 6%. We argue that this inequity is due to the Commission's misperception that policies that put stations in the hands of historically underrepresented groups must pass strict scrutiny. In 1990, the Supreme Court ruled in *Adarand Contractors, Inc. v. Pena* that any laws or regulations that showed preferential treatment to people based solely on their

race would subsequently need to withstand strict scrutiny. This prompted the FCC to avoid embedding race (or gender) based preferences into media ownership regulations, despite repeated instructions from the Third Circuit Court of appeals to address the racial and gender imbalance in broadcast ownership. In *FCC v. Prometheus Radio* (2021), the Supreme Court had an opportunity to address the question of whether strict scrutiny was an appropriate level of review for broadcast regulatory decisions. Rather than tackling the issue of ownership head-on, the Court concentrated its decision on how much discretion administrative agencies have regarding changes to their initiatives. Had the Court focused exclusively on the ownership question, we believe it would have come to the same conclusion that we do here: a rational basis of review should be used for regulatory decisions. We believe this shift is needed to break the nearly two decades-long legal, policy, and regulatory deadlock over media ownership policy.

NOTES

Leash the Big Dogs, Let the Small Dogs Roam Free: Preserve Section 230 for Smaller Platforms

There are numerous proposals to reform section 230, the provision of the US code that immunizes interactive computer services from most civil and criminal liability for content created by third parties, and which is partly responsible for the dominance of the United States in the global Internet economy. While these reforms vary in terms of the variables that would trigger removing section 230 immunity, almost all of them seek to restrict the power that large online platforms would have on public discourse. This article argues that in order to preserve the competitive and free market purposes of section 230 and the consequential economic benefits, while still accomplishing the primary purposes of section 230 reformers, any changes that restrict immunity should be limited to companies with over $500 million in annual revenue that operate social media platforms with over fifty million monthly active users.

Stitching a Privacy Patchwork Together—for Now: The Constitutionality of State Privacy Regulations Under the Dormant Commerce Clause

With the recent turn towards skepticism of Big Tech, policymakers have rushed to implement regulations safeguarding consumer data privacy. Because of a failure to pass comprehensive federal policy, the majority of regulation in this area has occurred on the state level. In this paper, I consider whether expansive state-level consumer data privacy survives an inquiry under the dormant commerce clause. I primarily examine the CCPA as amended by the CPRA because these are the most expansive U.S. consumer data privacy statues at the state-level, but I also consider implications more broadly for other state regulatory frameworks.

A substantial circuit split has formed as to whether section 2510(17)(B) of the Stored Communications Act should be read broadly or narrowly, with the protection of opened or previously read emails in inboxes under the law hanging in the balance. This Note argues that courts around the country should adopt the Fourth Circuit's broad interpretation of the relevant statutory language in *Hately v. Watts*. The decision offers compelling arguments regarding the law's legislative history, the plain meaning of the relevant language, the absurdity doctrine, the superfluity doctrine, and the developments in technology since the law was passed in 1986. This paper will also offer independent policy considerations in favor of the broad interpretation of the statutory language, including judicial efficiency, litigation costs, making Americans feel more secure in their personal data, and providing additional opportunities for victims to hold wrongdoers accountable under the law's private right of action. Lastly, this Note will offer some possible solutions for the current circuit split separate and apart from advocacy for the widespread adoption of the Fourth Circuit's interpretation.

Institutional Considerations for the Regulation of Internet Service Providers

Daniel T. Deacon*

TABLE OF CONTENTS

* Lecturer, University of Michigan Law School. Many thanks to Tejas Narechania and Erik Stallman for their helpful comments and to participants at the symposium at which this paper was presented. I am also grateful for feedback on an earlier version of this project that was presented at the University of Michigan Law School Governance Group Workshop.

I. INTRODUCTION

Since the dawn of the commercial Internet, how to treat Internet service providers has bedeviled the Federal Communications Commission (FCC). The reasons are easily enough known. The Communications Act—last subject to major overhaul in 1996, when broadband Internet was still in its adolescence—does not speak clearly to how (or even whether) the FCC should regulate ISPs. The FCC has thus been left to grapple with how archaic sounding terms, concocted when the Bell operating companies still dominated the landscape, apply in modern times: adjunct-to-basic, "enhanced" services, ancillary authority, etcetera. At the same time, broadband Internet has become central to American life. More and more traditional communications services are being operated over IP-based platforms. And there is a growing unease with the power that large, agglomerative entities—ISPs, but also platforms like Google and Facebook—wield over the consumer.[1]

The situation has recently reached a potential head. When the Obama-era FCC finally classified ISPs as Title II common carriers,[2] many immediately perceived that the classification might not outlast a changeover in party control of the White House. And indeed, with the pivot to a Republican-controlled Commission following the election of Donald Trump, the FCC swiftly moved to remove ISPs from Title II and place them back into the Title I "light touch" regulatory framework.[3] Fast forward through another election cycle, and it looks likely that a Democratic-controlled FCC will again reverse course, with news outlets suggesting that the Commission will again move ISPs back into the Title II box.[4] And although the FCC's flip-flopping has been good for lawyers in the industry, few think it's good for the industry itself or for society at large.

Against this backdrop, there are widespread calls to finally settle the issue. But there seems to be little consensus on how to do so.[5] The main Democratic piece of legislation, the Save the Internet Act, passed the House in April 2019, but soon died in the Senate.[6] Republican-sponsored bills have attracted little bipartisan support. And various options for working within the legislative status quo strike many as unappealing.

---

1. *See, e.g.*, STIGLER COMMITTEE ON DIGITAL PLATFORMS, FINAL REPORT 6 (2019) (detailing various "concerns about [the] unchecked power" of digital platforms).

2. Protecting & Promoting the Open Internet, *Report and Order on Remand, Declaratory Ruling, and Order*, 30 FCC Rcd 5601 (2015) [hereinafter *Title II Order*].

3. Restoring Internet Freedom, *Declaratory Ruling, Report and Order, and Order*, 33 FCC Rcd 311 (2018) [hereinafter *Restoring Internet Freedom Order*].

4. *See, e.g.*, Jon Reid, *Net Neutrality Tops To-Do List for FCC Democrats in Biden Era*, BLOOMBERG L. (Nov. 18, 2020, 6:01 AM), https://news.bloomberglaw.com/tech-and-telecom-law/net-neutrality-tops-to-do-list-for-fcc-democrats-in-biden-era [https://perma.cc/H4KT-G68W].

5. *See, e.g.*, Makena Kelly, *Democrats Are Gearing Up to Fight for Net Neutrality*, VERGE (Mar. 9, 2021, 4:24 PM), https://www.theverge.com/2021/3/9/22321995/net-neutrality-ed-markey-save-the-internet-open-ajit-pai-rosenworcel.

6. *Id.*

This short essay surveys the current landscape and discusses various potential ways out of the current morass. In doing so, I bring a primarily institutional focus. That is, rather than starting from the standpoint questioning whether this or that policy, such as net neutrality, is good or bad, I ask more broadly who should regulate ISPs and under what general framework. I assess and critique various frameworks, including reliance on markets and antitrust; state-level regulation under a federal Title I regime; various frameworks set forward in Republican-sponsored bills; and the Save the Internet Act. I argue that all of these frameworks suffer from numerous drawbacks, such as the lack of the ability to set clear rules (as with antitrust) or insufficient flexibility (as I argue besets both Republican- and Democratic-sponsored bills, in differing ways). I suggest that the legislative proposal with the most promise would be roughly based on the legislation enacted to govern the regulation of commercial cellular service in the early 1990s. This would bring ISPs within the general Title II framework while perhaps taking certain things—such as ex ante price regulation and certain forms of state-level regulation—off the table. It would also preserve the FCC's flexible role going forward, and re-channel the FCC's inquiry toward the policy-focused forbearance factors and away from endless scholastic debate about whether ISPs really "are" telecommunications carriers.

Part II briefly describes how we got here, cataloguing the history of the FCC's efforts to regulate ISPs, most recently in the context of the controversy over net neutrality. Part III then turns to considering potential institutional settlements that could prove more enduring than that currently prevailing. After discussing two alternatives that could be implemented largely within the legal status quo—reliance on antitrust and state-level regulation—I turn to the main competing Republican and Democratic legislative proposals. Those proposals, I will argue, suffer from a similar defect—namely, failing to provide the FCC with sufficient flexibility to adapt to changing circumstances and treating today's regulatory controversies as if they will continue to define the field going forward. Part III ends by discussing a legislative option, modeled on what Congress did in 1993 regarding cellular voice service, which has greater promise.

II. THE CURRENT MORASS

The history of how the FCC has come to its current posture regarding ISPs has been well told in the numerous court decisions and regulatory orders dealing with the issue. This part will provide a brief recap of that history. The Communications Act is divided into different Titles, which include: Title II (dealing with "common carriers");[7] Title III ("radio communications");[8] and Title VI ("cable communications").[9] Communications services that do not fit neatly within any Title but are still subject to the FCC's general jurisdiction

7. Communications Act of 1934 tit. II, 47 U.S.C. §§ 201-21.
8. *Id.* tit. III, 47 U.S.C. §§ 301-29.
9. Cable Communications Policy Act of 1984, 47 U.S.C. §§ 521-73.

over "all interstate and foreign communication by wire or radio"[10] fall under Title I. The FCC has some, but limited, authority over Title I services.

A large part of the controversy over ISPs has concerned whether ISPs should be subject to Title II of the Act—because they are properly considered common carriers—or whether they can be treated only under Title I. ISPs provide "last mile" connectivity to their customers. When a customer of an ISP wishes to visit a website, for example, the ISP takes the customer's request and routes it to a separate backbone network. The backbone network then delivers the customer's query to the website's ISP, which transmits it to the website's servers. The website processes the request and sends the requested information (a web page) back to the customer using the same chain of networks.[11] The whole process takes (hopefully) just a few seconds.

Whether in performing these functions the ISP acts as a "common carrier" subject to Title II of the Communications Act has enormous consequences. The Act defines common carriers, rather circularly, as "any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio."[12] The Act imposes a range of duties on such carriers, including obligations to charge "just and reasonable" rates,[13] to file detailed rate tariffs,[14] and to refrain from "unjust or unreasonable discrimination."[15] Those requirements automatically attach to common carriers, except the Commission may "forbear" from applying them to particular providers, or category of providers, if certain conditions are met.[16]

The roots of the FCC's current treatment of ISPs extend back to a series of decisions the FCC made in the 1970s and 1980s concerning services that used computers to provide "data processing" over telephone lines.[17] In its *Computer II* order, the FCC decided that these data processing services would be treated as what it termed "enhanced services."[18] Such enhanced services, the FCC made clear, would not be subject to common-carrier regulation under Title II.[19] The FCC contrasted enhanced services, which provided users the ability to manipulate information, with so-called "basic services," including data transmission services with no data processing capability (such as

---

10. 47 U.S.C. § 152(a).

11. *See generally* United States Telecom Ass'n v. FCC, 825 F.3d 674, 690 (D.C. Cir. 2016) (providing similar example).

12. 47 U.S.C. § 153(11); *see also* Christopher S. Yoo, *Is There a Role for Common Carriage in an Internet-Based World?*, 51 HOUS. L. REV. 545, 552 (2013) (noting that "[t]he circular nature of this definition inevitably leads those seeking to determine what a common carrier is to look to other sources").

13. 47 U.S.C. § 201(b).

14. *Id.* § 203.

15. *Id.* § 202(a).

16. *Id.* § 160(a).

17. *See, e.g.*, James B. Speta, *Deregulating Telecommunications in Internet Time*, 61 WASH. & LEE L. REV. 1063, 1083-84 (2004).

18. Second Computer Inquiry, *Order*, 77 F.C.C. 2d 384, para. 92 (1980).

19. For a comprehensive history of the Computer Inquiries orders, see Robert Cannon, *The Legacy of the Federal Communications Commission's Computer Inquiries*, 55 FED. COMM. L.J. 167 (2003); *see also* Speta, *supra* note 17, at 1083; JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: TELECOMMUNICATIONS LAW AND POLICY IN THE INTERNET AGE 190 (2d ed. 2013).

traditional telephony), which continued to be regulated under principles of common carriage.[20]

The Telecommunications Act of 1996 largely codified the distinction between enhanced and basic services, albeit using different nomenclature. Corresponding to the old "basic services" category was a new term, "telecommunications service," which Congress defined as "the offering of telecommunications for a fee directly to the public."[21] "Telecommunications" was further defined as "the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received."[22] In contrast with telecommunications service, Congress introduced the term "information service," which corresponded to the old regulatory category of enhanced service and was defined as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications."[23]

Crucially, Congress also preserved the differing regulatory treatment of basic and advanced services, now recast as telecommunications and information services. Specifically, 47 U.S.C. § 153(51) defines "telecommunications carrier" as a "provider of telecommunications services."[24] It goes on to state that "[a] telecommunications carrier shall be treated as a common carrier under this chapter only to the extent that it is engaged in providing telecommunications services."[25] The 1996 Act thus exempts non-telecommunications carriers—i.e., entities that do not provide "telecommunications service"—from regulation under Title II of the Communications Act. And because the FCC has long defined telecommunications service and information service as mutually exclusive categories such that a single service cannot simultaneously be both,[26] whether a given service is classified as one or the other has significant regulatory consequences.

The controversy regarding how to classify ISPs really kicked off when cable providers began to offer high-speed (broadband) Internet service using their own facilities.[27] These companies, like earlier non-facilities-based ISPs, offered their customers a suite of functionalities, including e-mail and other

---

20. *See* Cannon, *supra* note 19, at 183-88; Susan P. Crawford, *Transporting Communications*, 89 B.U. L. REV. 871, 892-94 (2009); *see generally* Amend. of Section 64.702 of the Comm'n's Rules and Reguls. (Second Computer Inquiry), *Final Decision*, 77 F.C.C. 2d 384 (1980).

21. 47 U.S.C. § 153(53).

22. *Id.* § 153(50).

23. *Id.* § 153(24).

24. *Id.* § 153(51).

25. *Id.*

26. *See, e.g.*, Fed.-State Joint Bd. on Universal Serv., *Report to Congress*, 13 FCC Rcd 11501, 11507-08, para. 13 (1998) [hereinafter *Universal Service Report*] ("We conclude, as the Commission did in the Universal Service Order, that the categories of 'telecommunications service' and 'information service' in the 1996 Act are mutually exclusive.").

27. On the regulatory treatment of ISPs prior to the rise of broadband Internet, see Daniel T. Deacon, *Common Carrier Essentialism and the Emerging Common Law of Internet Regulation*, 67 ADMIN. L. REV. 134, 141 (2015).

add-ons, that had traditionally been considered unregulated information services. But they also offered last-mile transmission of the type that had been the domain of highly regulated local telephone companies Were these companies offering telecommunications services, information services, or a bundle that included both?

After first declining to answer that question,[28] the FCC ruled that broadband Internet offered over cable facilities was an integrated information service not subject to Title II.[29] It did so based on the FCC's determination that such ISPs offer customers certain functionalities—such as Domain Name System (DNS)[30]—properly classified as "information services" and that are functionally inseparable from the pure "telecommunications" aspects of the ISPs' overall service offering.[31] The Supreme Court upheld the FCC's classification decision in *National Cable & Telecommunications Ass'n v. Brand X Internet Services*, applying the *Chevron* framework to hold that the Communications Act was ambiguous regarding the proper classification of broadband Internet service and that the FCC had reasonably construed the Act to exclude ISPs from Title II.[32] Following *Brand X*, the FCC extended the approach that it had taken regarding broadband over cable to broadband over DSL and to other types of broadband service.

The result of the FCC's decisions was to ensconce a largely anti-regulatory approach to broadband ISPs. As long as ISPs were treated as offering a Title I service, they could not be subject to core provisions of Title II, such as tariffing obligations. But whether ISPs should remain completely unregulated was subject to doubts. Many such doubts were expressed in the context of the controversy regarding so-called "net neutrality" rules.[33] Proponents of net neutrality seek to regulate the relationship between Internet service providers (such as Comcast or Verizon) and Internet content providers (such as Netflix, Facebook, or Google), often called "edge providers."[34] More specifically, net neutrality proponents would generally place two requirements on Internet access providers: "(1) a ban on 'blocking' or 'degrading' lawful content over an Internet access platform and (2) a ban on, or at least close regulation of, contractual deals between broadband networks and Internet content providers for favored treatment over that platform."[35] They fear that, absent these requirements, broadband Internet access

---

28. *See id.* at 141-42.

29. *See* Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, *Declaratory Ruling and Notice of Proposed Rulemaking*, 17 FCC Rcd 4798, 4819, para. 33 (2002) [hereinafter *Cable Broadband Order*].

30. As the Commission explained, "A DNS is an Internet service that enables the translation of domain names into IP addresses," *Cable Broadband Order*, *supra* note 29 at para. 17 n.74, and it can also be used to perform a variety of other functions that, the Commission concluded, constituted information services. *See id.* para. 37.

31. *Id.* para. 39.

32. Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 1002 (2005).

33. *See generally* Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. ON TELECOMM. & HIGH TECHNOLOGY L. 141 (2003) (coining the term "network neutrality").

34. Verizon v. FCC, 740 F.3d 623, 629 (D.C. Cir. 2014).

35. *See* NUECHTERLEIN & WEISER, *supra* note 19, at 198.

providers will favor certain edge providers—most prominently, perhaps, those affiliated with the access provider itself—and disfavor others, to the long-term detriment of Internet innovation and consumer welfare.[36]

Matters regarding net neutrality reached a head when the FCC, responding to complaints, condemned Comcast for allegedly interfering with its customers' use of certain peer-to-peer applications, including BitTorrent in particular.[37] As authority for doing so, the FCC pointed to its "ancillary authority" to regulate Title I providers, which allows the Commission to place rules on Title I providers that are "reasonably ancillary to the effective performance of the Commission's various responsibilities" under the other, substantive Titles of the Act.[38] On appeal, the D.C. Circuit disagreed with the FCC's conclusion that its ancillary authority allowed it to regulate ISPs' network practices.[39] In the court's view, the FCC had not pointed to a specific "statutory delegation of regulatory authority" to which the regulations in question were reasonably ancillary.[40] Perhaps most important was the D.C. Circuit's seemingly parsimonious attitude toward the FCC's ancillary authority as a general matter. Long gone, it appeared, were the days when the FCC could regulate entire new emerging technologies under Title I, as it had done when cable television networks first appeared.

After having been sent back to the drawing board, the FCC cast about for other options for regulating ISPs' network practices. The Commission first considered reclassifying broadband Internet access as (at least in part) a Title II telecommunications service.[41] But the FCC pulled back from that option and, in 2010, once again relied on grounds outside of Title II to impose net neutrality rules on ISPs—namely, section 706 of the Telecommunications Act of 1996.[42] As most relevant here, section 706(a) directs the Commission to:

---

36. *See, e.g.*, BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION 270-73 (2010); Wu, *supra* note 33, at 145-46; Barbara van Schewick, *Towards an Economic Framework for Network Neutrality Regulation*, 5 J. ON TELECOMM. & HIGH TECHNOLOGY L. 329, 378-80 (2007).

37. *See* Deacon, *supra* note 27, at 146.

38. United States v. Sw. Cable Co., 392 U.S. 157, 178 (1968); *see also, e.g.*, John Blevins, *Jurisdiction as Competition Promotion: A Unified Theory of the FCC's Ancillary Jurisdiction*, 36 FLA. ST. U. L. REV. 585, 595-96 (2009).

39. Comcast Corp. v. FCC, 600 F.3d 642, 644 (D.C. Cir. 2010).

40. *Id.* at 658.

41. *See* Framework for Broadband Internet Access, *Notice of Inquiry*, 25 FCC Rcd 7866 (2010).

42. *See* Preserving the Open Internet, *Report and Order*, 25 FCC Rcd. 17905, 17906 (2010) [hereinafter *Open Internet Order*] (Section 706 is codified at 47 U.S.C. § 1302).

> [E]ncourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans . . . by utilizing, in a manner consistent with the public interest, convenience, and necessity, price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market, or other regulating methods that remove barriers to infrastructure investment.[43]

The FCC decided that net neutrality rules such as those described above were "other regulating methods that remove barriers to infrastructure investment."[44] In support of that determination, the FCC pointed to the "virtuous cycle of innovation," under which "new uses of the [broadband] network—including new content, applications, services, and devices—lead to increased end-user demand for broadband, which drives network improvements, which in turn lead to further innovative network uses."[45] Net neutrality rules, the FCC reasoned, were critical to fostering new innovations by upstart content providers without having to deal with potentially anticompetitive deals between ISPs and incumbent content providers. They therefore helped the Internet ecosystem as a whole, including by (down the line, at least) stimulating infrastructure investment by ISPs.

This time, the FCC won a partial victory at the D.C. Circuit, but the court went on to strike down the bulk of the Commission's net neutrality regulations. First siding with the FCC against ISP challengers, the court determined that section 706 provided the FCC with substantive regulatory authority and deferred to the FCC's "virtuous cycle" theory.[46] But the D.C. Circuit went on to vacate the no-blocking and nondiscrimination rules that made up the core of the *Open Internet Order*.[47] It did so based on the statutory prohibition, mentioned above, on treating "information services" providers—including broadband Internet service providers—as "common carrier[s]."[48] In essence, the court found that the *Open Internet Order*'s nondiscrimination rule—which prevented access providers from distinguishing among edge providers in providing service—constituted a classic "compelled carriage obligation" that the FCC is statutorily prohibited from placing on non-telecommunications carriers.[49] As for the no-blocking rule, the court held that it too ran afoul of the common-carrier prohibition by denying access providers' discretion over what traffic to carry and on what terms.[50]

---

43. *Id.* § 1302(a). Section 706(b) similarly requires the FCC to conduct a yearly inquiry "concerning the availability of advanced telecommunications capability to all Americans," and, if it finds such availability lacking, to "take immediate action to accelerate deployment of such capability by removing barriers to infrastructure investment and by promoting competition in the telecommunications market."

44. *Id.*

45. *Open Internet Order*, at 17,972 para. 123.

46. Verizon v. FCC, 740 F.3d 623, 634, 641-45 (D.C. Cir. 2014).

47. *Id.* at 659.

48. *Id.* at 650 (quoting 47 U.S.C. § 153(51)).

49. *Id.* at 650, 655-56.

50. *Id.* at 657-59.

Having again been sent back to the drawing board, the FCC once more considered its options. At first, the FCC appeared reluctant to go the full Title II route by finally reclassifying ISPs as telecommunications carriers. Instead, the FCC proposed a system where, exercising authority under section 706, it would police potential abuses directed against consumers by ISPs on a case-by-case basis under a more flexible standard.[51] This would, the FCC believed, remedy the legal defects in its prior approach while still allowing the FCC to root out the worst of abuses by ISPs. At the same time, the FCC was at first believed likely to treat traffic exchanged between ISPs and edge providers under Title II, creating a so-called "hybrid" approach to regulating Internet traffic.[52]

The FCC's proposal met widespread opposition from net neutrality activists and consumer groups, who argued that bright-line rules against discrimination and blocking were necessary, and, in light of *Verizon*, that the only way to ensure such rules would survive judicial review was to reject the hybrid approach and go "full Title II."[53] Following President Obama's release of a YouTube video endorsing a full Title II approach, the Commission did just that, declaring that ISPs offered telecommunications services.[54] As to DNS (and caching), the FCC found that those services fell within the Act's "telecommunications management exception," which treats as a telecommunications service "any use [of an information service] for the management, control, or operation of a telecommunications system or the management of a telecommunications service."[55] Having found that ISPs offered telecommunications services, the Commission then went on to "forbear" from applying many of the obligations found in Title II, rendering them inapplicable to ISPs.[56] These obligations included, most importantly, Title II's tariffing regime. The FCC did not forbear from Title II's ban on "unjust or unreasonable discrimination,"[57] which it used to root the 2010 *Open Internet Order*'s no-discrimination and no-blocking rules.[58] On appeal, the D.C. Circuit handed the FCC a total victory, applying *Brand X*'s finding

---

51. *See* Protecting & Promoting the Open Internet, *Notice of Proposed Rulemaking*, 29 FCC Rcd 5561, 5602-04 paras. 116-21 (2014).

52. *See* Amy Schatz, *FCC Eying Net Neutrality Plan That Will Make No One Happy*, VOX (Oct. 31, 2014), https://www.vox.com/2014/10/31/11632498/fcc-eying-net-neutrality-plan-that-will-make-no-one-happy [https://perma.cc/8EY3-2RFU].

53. *See id.*

54. *See Title II Order*, *supra* note 2, at 5610 para. 29.

55. *Id.* at 5765-71 paras. 365-372.

56. *Id.* at 5838-64 paras. 493-536. Section 10 of the Communications Act allows the Commission to "forbear" from applying provisions of the Communications Act "to a telecommunications carrier or telecommunications service, or class of telecommunications carriers or telecommunications services, in any or some of its or their geographic markets," provided that the Commission makes certain public-interest determinations. 47 U.S.C. § 160(a).

57. 47 U.S.C. § 202 (2018).

58. *Title II Order*, *supra* note 2, at 5724-25 paras. 283-84. In the alternative, the Commission argued that those rules could be reapplied under section 706, now unfettered by the prohibition against treating ISPs as common carriers. Telecommunications Act of 1996 § 706, 47 U.S.C. § 1302 (2018). *Title II Order*, *supra* note 2, at 5721-24 paras. 275-82.

that the Act was ambiguous and thus concluding that the FCC had discretion to move ISPs back and forth between Title I and Title II.[59]

From the perspective of Title II supporters, victory was short lived. Following Donald Trump's election, the FCC (now with a Republican majority) signaled that it was going to reconsider the classification of ISPs as common carriers. And, in 2018, the FCC formally re-re-classified ISPs, sending them back to Title I.[60] DNS, the Commission declared, was not properly subject to the telecommunications management exception, with the FCC returning to the view of the *Broadband Internet Order* that ISPs offered a service with inseparable information-service components.[61] Having returned ISPs to Title I, the FCC also disclaimed the Commission's prior view that section 706 granted it independent regulatory authority, leaving the FCC's power over ISPs limited to whatever (if anything) it might be able to do under its ancillary authority.[62] The D.C. Circuit recently upheld the *Restoring Internet Freedom Order* in large part, again finding under *Brand X* that the FCC had wide discretion to make the call on classification and that section 706 was also ambiguous.[63] The court did send a few issues back to the FCC for further explanation—including the question of how the FCC intended to provide universal service support to ISPs now that they were no longer telecommunications carriers.[64] But the court refused to vacate the FCC's reclassification, and ISPs thus currently remain outside the Title II framework.[65]

But, perhaps, not for long. With the Biden administration in town, the Commission is widely expected, once it reaches full strength, to put Title II back on the table.[66] And once the Commission does, finally, re-re-re-classify ISPs[67] as telecommunications carriers, you can expect litigation to follow—this time, maybe, all the way to the Supreme Court.

***

To recap, here is the status as of this writing:

- ISPs are Title I "information service providers."
- Under the D.C. Circuit's prevailing view, ISPs could be shunted back to Title II. The FCC would then be free to apply (or not apply, using forbearance) the various provisions of Title II to ISPs.

---

59. Provided, of course, that doing so was reasonable and not arbitrary and capricious. *See* United States Telecom Ass'n v. FCC, 825 F.3d 674 (D.C. Cir. 2016). The court also upheld the Commission's reclassification of mobile broadband ISPs as Title II common carriers, which raised separate legal questions which needn't detain us here.

60. *Restoring Internet Freedom Order*, *supra* note 3, at 227.

61. *Id.* at 415.

62. *Id.* at 378.

63. Mozilla Corp. v. FCC, 940 F.3d 1, 18, 46, 84 (D.C. Cir. 2019).

64. *Id.* at 68-70.

65. *Id.* at 86.

66. *See* Reid, *supra* note 4.

67. Or "re-re-re-re-classifies" them, depending on how you parse the pre-*Cable Modem Order* state of affairs.

- Section 706 does not give the FCC independent regulatory authority over ISPs. Rather, it is merely hortatory, declaring that the FCC should use whatever authority it might otherwise have to stimulate broadband infrastructure investment.
- Again, under the D.C. Circuit's view, section 706 is ambiguous regarding whether it grants the FCC independent regulatory authority. Thus, a future FCC could find that it does.
- If a future FCC did decide to reinvigorate section 706, it could regulate under that section to the extent that doing so was (a) consistent with the "virtuous cycle" theory, and (b) did not run afoul of the Act's ban on treating information service providers as common carriers.
- If a future FCC reinvigorated section 706 *and* reclassified ISPs as Title II common carriers, it could regulate under section 706 provided doing so was consistent with the virtuous cycle theory. Having reclassified ISPs, it would not have to worry about whether its methods of regulation ran afoul of the Act's ban on treating information service providers as common carriers.
- Even today, the FCC could regulate ISPs using whatever ancillary authority it might have over them. However, following *Comcast*, its ability to do so is likely limited.

III. ESCAPE ROUTES

Few find the above situation tenable. At academic conferences around the country, participants cry out: "Congress must act! Bring an end to the madness!" And yet, there is little consensus on what Congress, or anyone else, might do. I have been an occasional skeptic of calls for Congress to fix things, believing that the most likely outcome of congressional action would be to replicate existing controversies just in different statutory garb. But following the latest FCC flip-flop—and the prospect of another coming soon—it seems best to survey the land to see if we might in fact do better. Recently, a bipartisan congressional working group has convened to explore if there is a reasonable path forward. This article seeks to contribute to those efforts.

A few words at the outset. I am more concerned, for present purposes, with coming to a sensible institutional framework than I am with defending particular approaches to specific regulatory controversies, net neutrality included.[68] That said, a sense of the policy stakes necessarily informs those higher-order institutional questions, and I will argue, for example, that placing sole reliance on background law such as antitrust is likely insufficient because it takes certain regulatory tools off the table that are at least plausibly necessary in certain contexts. I also proceed with some sense in mind of the politically possible. Of course, this involves some amount of guesswork. But certain political realities seem clear enough. For example, it is difficult to see

68. For an institutional take on the net neutrality dispute in particular, *see* Jonathan E. Nuechterlein, *Antitrust Oversight of an Antitrust Dispute: An Institutional Perspective on the Net Neutrality Debate*, 7 J. TELECOMM. & HIGH TECH. L. 19 (2009).

a congressional majority coalesce around a regime requiring ISPs to file tariffed end-user rates for all services. Similarly, one might doubt whether "doing nothing" will be a stable political approach, especially given the dissatisfaction with the status quo as described in Part II. That said, given the realities of American politics, "doing nothing" has often shown a tendency to prevail over the seeming odds.

A. The Market (and Antitrust)

One option would be to essentially lock in the status quo as inherited from the Trump era, with the FCC more or less falling out of the picture. This option would treat ISPs similarly to most other sectors of the economy, including, importantly, other potential Internet "gatekeepers" such as Google. It would mean relying primarily on the market to discipline potential bad behavior by ISPs, with background antitrust and consumer protection laws serving as a backstop.

There are certainly things to be said for this option, and it has been ably defended in the literature.[69] Specialized regulation, in one view, has been reserved for sectors of the economy that are monopolistic and is particularly appropriate for those that exhibit natural monopoly tendencies.[70] Applied to non-monopoly markets, the tools of the specialized regulator—tariffs, especially, but also strict non-discrimination obligations, structural separation requirements, and the like—are seen as cumbersome to administer and potentially at odds with consumer welfare.[71] And the market for broadband Internet access is not strictly monopolistic. Most consumers in the United States have access to at least two providers of broadband Internet access, and many have access to more.[72] Perhaps as importantly, a number of new technologies—such as fixed or mobile wireless and fixed satellite service—may expand that number in coming years.[73]

While stressing that competition will discipline ISP behavior in most cases, proponents of a market-based approach also stress that background antitrust law already has the tools to address potential abuses. Advocates for an antitrust approach see net neutrality in particular as a matter of regulating vertical contractual relationships.[74] And they point out that antitrust law views

---

69. *See, e.g.*, Thomas W. Hazlett & Joshua D. Wright, *The Law and Economics of Network Neutrality*, 45 IND. L. REV. 767 (2012).

70. *See* Howard A. Shelanski, *Adjusting Regulation to Competition: Toward A New Model for U.S. Telecommunications Policy*, 24 YALE J. ON REGUL. 55, 58-59 (2007).

71. *See id.* at 64-66.

72. *See* 2020 Comm. Marketplace Rpt., *In the Matter of Comm. Marketplace Rep.*, 18 FCC Rcd. 188, para. 126 (2020) [hereinafter *2020 Communications Marketplace Report*].

73. *See, e.g.*, Inquiry Concerning Deployment of Advanced Telecomms. Capability to All Ams. in A Reasonable & Timely Fashion, *Fourteenth Broadband Deployment Report*, No. FCC21-18, 2021 WL 268168, at para. 11 (OHMSV Jan. 19, 2021) (expressing "optimis[m] that increased deployment of 5G may allow mobile services to serve as an alternative to fixed services"); *see generally* Christopher S. Yoo, *Technological Determinism and Its Discontents*, 127 HARV. L. REV. 914 (2014) (reviewing SUSAN CRAWFORD, CAPTIVE AUDIENCE: THE TELECOM INDUSTRY AND MONOPOLY POWER IN THE NEW GILDED AGE (2013)).

74. *See* Hazlet & Wright, *supra* note 69 at 795-796.

vertical contracts as likely to be pro-consumer or at least benign.[75] When challenged as anti-competitive, antitrust deploys a rule-of-reason approach that looks to the specifics of the particular contractual relationship in question and, deploying modern analytical tools, decides whether the specific contract in question harms competition. Antitrust advocates argue that this approach allows for a more fine-grained determination that recognizes that the effects on competition from vertical contracts are often nuanced.[76]

That all said, in my view, there would be significant flaws with locking in a market-plus-antitrust framework under current conditions. As an initial matter, the current levels of competition in the market for Internet access should not be overstated. According to the FCC's own data and using its broadband benchmark of 25/3 Mbps service, most consumers in the United States still can only choose between two providers.[77] Nearly one-quarter of Americans have either zero options or only one.[78] And less than half have access to multiple providers of 50/5 Mbps service,[79] which may increasingly be necessary in today's online environment. Even where there is competition, high switching costs prevent consumers from defecting in response to (from their point of view) subtle changes in ISP behavior.[80] And due to consumer misperceptions, ignorance, or inability to uncover the facts, the idea that consumer choices will discipline ISP behavior may be more dream than reality.

I want to focus here, though, on two broader institutional features of the antitrust framework that may limit its effectiveness when it comes to communications markets: first, antitrust prefers standards over rules, and second, there are a limited set of values relevant to the antitrust enterprise.
First, antitrust operates ex post, condemning past anticompetitive acts on their facts, and although antitrust could embrace a more rules-focused regime, the trend has been toward standards.[81] This isn't a bad thing, necessarily. In many contexts, selecting a standard as opposed to an ex ante rule is the right choice.[82] But there are, of course, benefits to rules that may be particularly salient when it comes to broadband markets. Barbara van Schewick has developed several critiques of the reliance on standards in the context of net neutrality in particular.[83] These include (1) lack of certainty for market players, (2) the costs imposed by regulation through individual adjudication,

---

75. *Id.* at 798.
76. *See* Hazlett & Wright, *supra* note 69, at 797; Nuechterlein, *supra* note 68.
77. *See 2020 Communications Marketplace Report*, *supra* note 72, at para. 126.
78. *Id.*
79. *Id.*
80. *See Title II Order*, *supra* note 2, at para. 81.
81. *See* Daniel A. Crane, *Rules Versus Standards in Antitrust Adjudication*, 64 WASH. & LEE L. REV. 49, 50-51 (2007).
82. For some classic explorations, *see* Colin S. Diver, *The Optimal Precision of Administrative Rules*, 93 YALE L.J. 65 (1983); Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557 (1992).
83. *See* Barbara van Schewick, *Network Neutrality and Quality of Service: What A Nondiscrimination Rule Should Look Like*, 67 STAN. L. REV. 1, 70-74 (2015).

and, relatedly, (3) the potential for regulation through ex post adjudication to bias the system against less-well-financed players.[84]

The point, however, is not to bury standards in favor of rules. The point is that turning over broadband markets to antitrust law involves the decision to (largely) impose a standards-reliant framework across the board. By contrast, under the modified Title II-plus-forbearance approach (discussed below),[85] the FCC would always have the ability, under its forbearance authority, to disclaim regulatory authority over particular issues, and, in effect, send them back to antitrust. That is, Title II does not involve *renouncing* the usefulness of antitrust, including its "rule-of-reason"-focused approach, but only creates the *option* to proceed by different means, where appropriate. As I have argued elsewhere, the FCC should more squarely refocus its forbearance decisions to render more fine-grained determinations regarding the appropriateness of antitrust or specialized regulation regarding a particular issue as opposed to a more crude, across-the-board conclusion regarding the entire industry.[86]

The second potential limitation of reliance on the market and antitrust is more deeply embedded. The "market-plus-antitrust" framework—at least in its current form—is concerned with consumer welfare, usually (though not always exclusively) measured through effects on price and output.[87] But as historically practiced, communications regulation has served a broader set of goals. Based on a recognition that communications networks play a role in orienting society itself, communications regulators have focused more squarely on ensuring, for example, that the market respects the principle of equality.[88] Related to, or as an aspect of, that commitment, communications law has striven to provide access to technologies necessary for persons to be able to participate in society as equals, regardless of race, sex, physical location, disability, or other characteristic. And the FCC has long served as the repository of such authority.

The "market-plus-antitrust" framework serves access in its own way, of course. By driving down prices to competitive levels and increasing output, that framework ensures that more people willing to pay the market price for a good or service will be able to do so. But the access-oriented applications of antitrust don't extend to situations where it would simply be uneconomic for market participants to provide a certain good. Nor do they provide the ability to subsidize access by persons who are unable to pay the competitive price or to ensure that persons who are vision- or hearing-impaired can meaningfully engage on communications platforms. And antitrust could not plausibly be reformed to serve such goals. In the United States' system, at least, courts simply do not sit to dole out government subsidies but rather are limited to resolving concrete disputes among individuals.

---

84. *Id.* at 70-74.

85. *See infra* Part III.E.

86. *See* Daniel T. Deacon, *Justice Scalia on Updating Old Statutes (with Particular Attention to the Communications Act)*, 16 COLO. TECHNOLOGY L.J. 103, 116-19 (2017).

87. *See, e.g.*, Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 716 (2017).

88. *See* Olivier Sylvain, *Network Equality*, 67 HASTINGS L.J. 443, 445 (2016).

The FCC's current approach, working from within the Title I framework, has been to interpret its statutory authority to provide it with the ability to subsidize broadband facilities under its universal service programs without deeming the underlying services as telecommunications.[89] Without dwelling on the legal arcana, suffice it to say that the FCC's approach was somewhat thrown into doubt when the D.C. Circuit in *Mozilla Corp. v. FCC* expressed skepticism that the FCC could subsidize broadband through its Lifeline program and remanded that issue to the FCC for further explanation.[90] Although the FCC has since responded, drawing attention more carefully to the Tenth Circuit's ratification of a similar legal theory in prior litigation,[91] the legal theory itself may be time limited. That is because it depends, on reasons we need not discuss, upon the entity receiving funds offering both broadband services and Title II voice services. But in the future, many such companies may shift to offering *only* what the FCC currently deems unregulated Title I services, raising questions about the long-term viability of the FCC's legal strategy.[92]

One response to the above would be to argue that, yes, funding broadband deployment and the like are worthwhile goals not easily pursued through court-centered systems like antitrust, and the FCC should be statutorily authorized to perform such goals and provided with additional funds to do so. Other matters, however, can and should be returned to the market. Such a response, however, misses the rationale for *why* there is near universal agreement on matters like the necessity of access to broadband. And that's because, I submit, the public has a special relationship to things like communications markets that, in the words of Sabeel Rahman, provide "infrastructural goods," which he defines as those that "form the vital foundation or backbone of our political economy."[93]

In recognition of the special role of communications platforms, communications regulation has historically treated those platforms as subject to public superintendence and control, treating such superintendence as a worthwhile goal in itself. As then-Commerce Secretary Herbert Hoover put it in defending what would become the Federal Radio Act of 1927, which extended administrative control over the spectrum, the bill "recognizes that the interest of the public as a whole supersedes the desire of any individual. This is a new and highly desirable feature in the radio law."[94] And that public interest has been attendant to a range of values other than ensuring bare access to technology. Through a variety of tools ranging from market entry and exit requirements, merger review, licensing, and others, communications

89. *See generally Restoring Internet Freedom Order*, *supra* note 3, at para. 193; Connect Am. Fund et al., *Report and Order and Further Notice of Proposed Rulemaking*, 26 FCC Rcd. 17663 (2011).

90. Mozilla Corp. v. FCC, 940 F.3d 1, 68-70 (D.C. Cir. 2019).

91. *See In re FCC 11-161*, 753 F.3d 1015, 1044-49 (10th Cir. 2014).

92. *See* Deacon, *supra* note 86, at 118.

93. K. Sabeel Rahman, *The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept*, 39 CARDOZO L. REV. 1621, 1625 (2018).

94. *To Regulate Radio Communications: Hearings Before the H. Comm. on the Merchant Marine and Fisheries on H.R. 5589*, 69th Cong., 11 (1926) (statement of Herbert Hoover, Sec'y, U.S. Dep't of Commerce).

regulation has pursued a variety of social goals such as equality, diversity, "free speech" (as more broadly defined than in the First Amendment context), and privacy, none of which are easily captured by the "market-plus-antitrust" framework.

B. State-Level Regulation Under a Title I Regime

Another institutional option, also rooted in the status quo, is to rely on the states. California, for example, passed a statute in 2018 containing a suite of net neutrality and related obligations.[95] Other states have also passed various laws concerning ISPs.[96]

The balance of federal-state power in the area of communications regulation is too large of a topic to explore in this short essay. Suffice it to say that as a policy matter, I seriously doubt there are many who view *exclusive* state-level regulation of ISP practices as a first-best solution.[97] Indeed, the interest in state net neutrality laws came about largely because it was widely perceived that, following the election of Donald Trump, the FCC would swing back to Title I, as it did.

Under the legal status quo, I also believe there are also serious legal difficulties with relying on the states. To be sure, the *Mozilla* court, with Judge Williams dissenting on this point, held that the *Restoring Internet Freedom Order* could not expressly preempt state regulation in the area.[98] The court held, essentially, that to expressly preempt the states, the FCC had to point to a statutory source of authority allowing it such power.[99] And having moved ISPs to Title I, the FCC could not rely on anything in Title II to do so.[100] Thus, somewhat counterintuitively, the act of deregulating ISPs meant that the FCC could no longer prevent the states from regulating them.

Although this aspect of *Mozilla* was taken as a victory for net neutrality proponents hoping to fashion laws at the state level, the victory was a shaky one. That is because *Mozilla* also explained that the Commission was free to argue, as it had not done in its order, that specific state laws were preempted by ordinary obstacle preemption principles, as opposed to expressly preempting state statutes as a blanket matter.[101] And obstacle preemption can

---

95. California Internet Consumer Protection and Net Neutrality Act of 2018, CAL. CIV. CODE §§ 3100-3104 (West 2021).

96. *See, e.g.*, Or. Rev. Stat. Ann. § 276A.418(3) (West 2021) (effective January 1, 2019); Wash. Rev. Code Ann. § 19.385.020(1)-(3) (West 2021) (effective June 7, 2018).

97. Of course, there still may be a role for states in an overall regulatory system. For a thoughtful defense of state authority, *see* Tejas Narechania & Erik Stallman, *Internet Federalism*, 34 HARV. J.L. & TECHNOLOGY 547, 548-620 (2021). Others suggest that states should have *no* role in the regulation of broadband networks. *See, e.g.*, Daniel Lyons, *State Net Neutrality*, 80 U. PITT L. REV. 905, 951 (2019) (arguing that "[b]roadband networks are inherently interstate" and "beyond the traditional realm of state telecommunications regulation").

98. Mozilla Corp. v. FCC, 940 F.3d 1, 74-86 (D.C. Cir. 2019); *see also id.* at 95-107 (Williams, J., dissenting).

99. *Id.* at 74-76.

100. *Id.* at 76-86.

101. *Id.* at 85.

flow from agency decisions to deregulate just as they can flow from decisions to affirmatively regulate.[102]

There is now a split concerning the preemptive effect of the *Restoring Internet Freedom Order*. In a challenge to California's net neutrality law, the state defeated a motion for a preliminary injunction, with the judge concluding that the Order likely did not preempt California's statute.[103] That decision is now on appeal. More recently, a federal district court in New York preliminarily enjoined that state's statute requiring broadband providers to offer low-income households basic broadband service at a capped rate.[104] The essence of that court's ruling was that the FCC's decision to move ISPs out of the Title II framework preempted states from imposing "common carrier" rules similar to those contained in Title II.[105] The New York district court's judgment is also on appeal as of this writing.

Although each state law will present unique considerations depending on its particulars, I believe that, at a minimum, state laws placing obligations on ISPs that the FCC has specifically foresworn conflict with federal policy objectives and thus call for obstacle preemption. That is because the driving force behind the FCC's decision to move ISPs back to Title I was its judgment that such obligations were inappropriate as a policy matter. As the FCC explained, in its view, "[t]he record evidence, including [the Commission's] cost-benefit analysis, demonstrates that the costs of [common-carrier] rules to innovation and investment outweigh any benefits they may have."[106] Reimposing those obligations on ISPs at the state level thus presents a plain case of conflict between state and federal prerogatives.

Proponents of state-level net neutrality laws respond with a similar argument as carried the day in *Mozilla*.[107] They say that by moving ISPs out of Title II, the FCC took the position that the FCC had no jurisdiction over them and, thus, there can be no federal interest in maintaining federal policy in an area over which the FCC doesn't even have power.[108] This argument misconceives the nature of the FCC's authority. Under *Brand X*, the FCC does have jurisdiction over ISPs.[109] But it has the choice, using *Chevron*, to exercise that jurisdiction by treating ISPs as telecom carriers or not. That is fundamentally a policy choice. And placing ISPs within Title I does not strip

---

102. Ark. Elec. Coop. Corp. v. Ark. Pub. Serv. Comm'n, 461 U.S. 375, 384 (1983) ("[A] federal decision to forgo regulation in a given area may imply an authoritative federal determination that the area is best left *un*regulated, and in that event would have as much pre-emptive force as a decision *to* regulate.").

103. *See* Tony Romm, *Net Neutrality Law to Take Effect in California After Judge Deals Blow to Telecom Industry*, WASH. POST (Feb. 23, 2021), https://www.washingtonpost.com/technology/2021/02/23/net-neutrality-law-take-effect-california-after-judge-deals-blow-telecom-industry/ [https://perma.cc/43YS-XM3J].

104. N.Y. State Telecomms. Ass'n v. James, No. 221CV2389DRHAKT, 2021 WL 2401338, at *1 (E.D.N.Y. June 11, 2021).

105. *Id.* at *13.

106. *Restoring Internet Freedom Order*, *supra* note 3, at para. 4.

107. *See, e.g.*, Karl Bode, *Why Feds Can't Block California's Net Neutrality Bill*, VERGE (Oct. 2, 2018), https://www.theverge.com/2018/10/2/17927430/california-net-neutrality-law-preemption-state-lawsuit [https://perma.cc/2NDF-8D52].

108. *See, e.g.*, *James*, 2021 WL 2401338, at *7 (describing state's argument).

109. *See* NCTA v. Brand X Internet Servs., 545 U.S. 967, 1002-03 (2005).

the FCC of jurisdiction. ISPs remain engaged in the provision of interstate communications by wire. It is just that Title II of the Act does not apply to them. True, that means that, as a practical matter, the FCC can do very little to regulate ISPs. But that was the FCC's choice, based on its determination that regulation was largely inappropriate, and that choice embodies the relevant federal policy for obstacle preemption purposes.[110]

Mozilla does not change this bottom line. There, the court was searching for a particular provision that allowed the FCC to announce, as a general rule, that states were preempted from acting.[111] It found none.[112] But under *Brand X*, the FCC has authority to announce, as a rule, that ISPs are not telecom carriers.[113] Obstacle preemption then asks what the consequences of *that* determination are.[114] No further source of statutory authority is required. And on that question, courts are likely to find that those consequences include the preemption of any state law that the FCC specifically chose not to apply under Title II, including net neutrality protections. Thus, as long as the Title I framework stands at the federal level, I believe many state net neutrality laws are on shaky legal ground.

C. Republican-Sponsored Bills

At the federal level, some of the earliest attempts to legislate out of the morass described by Part II came from the Republican side of the aisle.[115] Although the bills vary somewhat in their particulars, they follow the same basic outline: codify ISPs' classification as information service providers under Title I; subject ISPs to certain basic net neutrality obligations (no blocking, no paid prioritization); and restrict the FCC's ability to implement the new obligations, for example, by prohibiting the FCC from engaging in rulemaking.[116]

The various Republican bills suffer from some serious flaws. For one, certain issues that could be handled under a Title II framework—such as broadband funding and privacy—are not addressed at all. Of course, these could be handled by different legislation, but there's no guarantee they will be, and Title II already contains the panoply of options that have traditionally attached to communications markets.

More generally, the Republican bills give a false sense that they are putting to bed today's controversies through imposing "clear" obligations on ISPs while at the same time kneecapping the FCC's ability to adapt the

---

110. *See James*, 2021 WL 2401338, at *7 (the federal district court in New York accepted a very similar argument).

111. Mozilla Corp. v. FCC, 940 F.3d 1, 75-76 (D.C. Cir. 2019)

112. *Id.* at 74.

113. *See Brand X*, 545 U.S. at 996-97.

114. *See Ray v. Atl. Richfield Co.*, 435 U.S. 151, 178 (1978) (explaining that "where failure of … federal officials affirmatively to exercise their full authority takes on the character of a ruling that no such regulation is appropriate or approved pursuant to the policy of the statute, States are not permitted to use their police power to enact such a regulation").

115. *See* H.R. 1101, 116th Cong. (2019); H.R. 1096, 116th Cong. (2019); H.R. 1006, 116th Cong. (2019).

116. *Id.*

regulatory regime to new circumstances. For example, in dealing with paid prioritization, one bill provides that ISPs "may not throttle lawful traffic by selectively slowing, speeding, degrading, or enhancing internet traffic based on source, destination, or content, subject to reasonable network management."[117] The bill's sponsors see this provision as enshrining what net neutrality proponents have always wanted, but even from today's vantage point its application to emerging controversies is unclear. Take "zero rating," which describes the practice of allowing users to use certain apps free from otherwise applicable data caps or fees.[118] Those who wish to regulate zero rating argue that it may have the same harmful effects on innovation that classic paid prioritization arrangements have.[119] Those on the other side argue that zero rating may be beneficial to consumers, allowing ISPs to have lower prices and expand access.[120] What's important for present purposes is not who's right, it is that the bills in question don't resolve the issue. And that is to say nothing of controversies over network practices that haven't even emerged yet.

The same bill would require the FCC to "enforce the [bill's] obligations . . . through adjudication of complaints alleging violations of such subsection," and provides that it "may not expand the internet openness obligations for provision of broadband internet access service beyond the obligations established in such subsection, whether by rulemaking or otherwise."[121] This restriction to adjudication contains ambiguities of its own. Is the FCC barred from rulemaking entirely, or only rulemaking that "expands . . . obligations"? And what does it mean to "expand" an obligation? Does this strip the FCC of *Chevron* deference when it proceeds by rulemaking? When it proceeds by adjudication? Does it get *Chevron* deference when it "restricts" and not "expands" an obligation?

Those ambiguities aside, the seeming purpose of the provision would be to push the FCC toward adjudication and away from rulemaking. But why? Proponents of the bill would likely say that proceeding by individual adjudication provides a more flexible regulatory regime that can better adapt to changed circumstances, and there is something to that. But adjudication also has its drawbacks. It can be hard to definitively settle issues through adjudications, and a case-by-case approach provides less certainty to regulated entities and to the public.[122] Rulemaking procedures also enhance political accountability and, by soliciting public input, can produce higher quality policy.[123] Those agencies that have pursued mostly adjudication have been subject to severe criticism.[124] The FTC, for example, has been pushed

117. H.R. 1101, 116th Cong. § 1 (2019).

118. Ellen P. Goodman, *Zero-Rating Broadband Data: Equality and Free Speech at the Network's Other Edge*, 15 COLO. TECHNOLOGY L.J. 63, 64 (2016).

119. *See id.* at 73-77.

120. *See id.* at 77-80.

121. H.R. 1101, 116th Cong. § 14(b)(1) (2019).

122. *See* 1 KRISTIN E. HICKMAN & RICHARD J. PIERCE, JR., ADMINISTRATIVE LAW TREATISE 520-24 (6th ed. 2019).

123. *See id.* at 518-20.

124. *See, e.g.*, Justin (Gus) Hurwitz, *Data Security and the FTC's Uncommon Law*, 101 IOWA L. REV. 955, 1001 (2016).

toward a system of regulation by adjudication by statutory provisions that made it more onerous for the FTC to engage in rulemaking.[125] The result has been that the FTC has formulated, through adjudication and (often) consent decrees, a body of common-law-like obligations in areas such as privacy.[126] Commentators, including academics, have criticized this system for violating fundamental norms such as the right to fair notice.[127] And yet, the Republican bills would seemingly require the FCC to proceed similarly, subject only to a hazy backstop prohibiting it from "expanding" on the obligations contained in the bills.

At the very least, it would seem appropriate to give the FCC the option of proceeding by rulemaking (if that is indeed what the bill prohibits). One does not need to do a full dress rehearsal of the administrative law class on *Chenery II* to understand that whether to proceed through rulemaking or adjudication is often a highly contextual question on which the agency likely has better information.[128] To artificially restrict the agency to one or the other—and especially to adjudication—should require special justification, which has not been supplied here. To the contrary, arguments have been made (canvased in the antitrust section above) that clear ex ante rules may be particularly appropriate when it comes to ISP practices.

D. The Save the Internet Act

The main Democratic legislative proposal in the area, passed by the House in April 2019, is the Save the Internet Act.[129] The Save the Internet Act is a very strange piece of legislation. Section 2(a)(1) of the Act provides that "[t]he Declaratory Ruling, Report and Order, and Order in the matter of restoring internet freedom that was adopted by the [FCC] on December 14, 2017 shall have no force or effect."[130] That provision nullifies the Trump-era FCC's Restoring Internet Freedom Order. So far, nothing totally out of the ordinary. Section 2(a)(2) then states that the Trump-era order "may not be reissued in substantially the same form" and further that the [FCC] may not issue a "new rule" that is "substantially the same" as the Trump-era rule.[131] This language appears borrowed from the Congressional Review Act. Section 2(b)(1) "restore[s] as in effect on January 19, 2017" the Obama-era FCC order classifying ISPs as telecom carriers and the regulations promulgated along with that order.[132]

Those provisions were, at the time the bill was originally introduced, basically it. What was left unclear was the extent to which the bill actually enshrined the Obama-era order in the U.S. Code, such that a future FCC could

---

125. *See id.*

126. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 676 (2014).

127. *See generally* Hurwitz, *supra* note 124, at 1001.

128. *See* HICKMAN & PIERCE, *supra* note 122, at 524-41.

129. Save the Internet Act of 2019, H.R. 1644, 116th Cong.

130. *Id.* § 2(a)(1).

131. *Id.* § 2(a)(2).

132. *Id.* § 2(b)(1).

not depart from it, or whether it simply reinstated the order subject to future revision. My personal understanding was that it "restored" the Obama-era order, but would allow—consistent with normal principles of administrative law—a future FCC to depart from it, at least to the extent that the resulting legal regime was not "substantially the same" as the Trump-era one. But uncertainty remained.

The apparent response to that uncertainty, added by later amendment, is the current bill's section 2(c)(2). That provision defines what it means to "restore" the Obama-era FCC's order and states that "restore" means "to permanently reinstate the rules and legal interpretations set forth in [the Obama-era order], including any decision (as in effect on such date) to apply or forbear from applying a provision of the Communications Act of 1934 . . . or a regulation of the [FCC]."[133]

That provision presumably sticks the FCC with the Obama-era rules, full stop. Once you drill down, though, the bill remains a minefield. For one, everyone who has read a few FCC orders—including, very much so, the Title II Order—knows that they contain sprawling discussions of various issues, often resembling a judicial opinion more than a code of law. The regulations that are to be codified in the Code of Federal Regulations (CFR) are appended to the order. The Save the Internet Act does not just return the CFR to its pre-Trump state of being, however. It protects, on a permanent basis, "the rules and legal interpretations set forth" in the order itself.[134] But which parts of the underlying order this effectively codifies and which it doesn't is not self-evident.

In addition, section 2(c)(2) specifically states that it is permanently restoring the Obama-era order's "decisions" regarding which statutory provisions and regulations to forbear from applying to ISPs. For example, the Obama-era FCC decided to forbear from section 203 of the Communications Act—dealing with tariffing requirements.[135] Presumably, then, the Save the Internet Act would bar the FCC from reapplying section 203 to ISPs. But the Obama-era order also reserved the FCC's authority to act more aggressively going forward, including by imposing forms of rate regulation under its sections 201 and 202 authority, which the FCC did not forbear from.[136] If a future FCC did decide to get more aggressive, how far could it push such rate regulation before running afoul of the Save the Internet Act's apparent intent not to allow forms of rate regulation resembling section 203 tariffing? Again, it's not clear.

It's similarly unclear how the Act would apply to future deregulatory actions. The seeming intent of the bill is to set the Obama-era rules as a floor. But given the rigidity this reading would impose, it is possible that a future FCC could try to cheat, and a sympathetic court could potentially allow the FCC to do so. For example, say a future FCC promulgates a new rule, formally codified some other place in the CFR, exempting a subset of Internet

133. *Id.* § 2(c)(2).
134. *Id.*
135. *Id.*
136. *Id.*

service providers—fixed wireless ISPs,[137] for example—from the Obama-era net-neutrality rules "notwithstanding" those rules, which continue to appear in the CFR just as before. Would that violate the bill's command that the Obama-era rules be "permanent"? A good argument could be made that it would, but that conclusion wouldn't necessarily be a slam dunk, particularly if there was solid evidence that the rules were wreaking havoc on some category of providers.

As should be reasonably clear from this discussion, I believe there are serious issues with the Save the Internet Act. First, the above questions would invite a litigation bonanza, as future FCCs attempt to navigate the vagaries of the Act. That would be good, of course, for telecom lawyers and those of us writing at the intersection of administrative law and communications regulation, but probably not so much for society at large. That is especially true when what is especially needed now, in light of the current state of things, is some kind of stable framework within which to work. The Save the Internet Act does not provide such a framework—indeed, it may invite even more confusion and uncertainty than what it is designed to replace.

Second, the Save the Internet Act suffers from a similar infirmity as Republican legislative proposals—namely, treating today's regulatory issues as etched in stone and hampering the FCC from making flexible adjustments going forward. That is especially ironic given that the Obama-era FCC order—the one that the Save the Internet Act would enshrine as code—was itself ambivalent about some issues, deferring consideration of some and building in flexibility for future FCCs to depart from the specifics on others. And there are good reasons for that. Communications markets are constantly evolving, and the FCC has a long and sometimes troubled history with adapting regulation to new conditions. The Save the Internet Act would (to some unknown but likely substantial degree) freeze the FCC in its tracks, treating as inviolable an FCC order when the authors of that order recognized its own fallibility.

E. The CMRS Model (Tweaked)

The final option I'll survey is the one I believe has the most promise. This I'll call this the CMRS option because it is based on, with some tweaks, the model that Congress enacted for commercial mobile radio services—most importantly, cellular voice service. The emergence of CMRS raised similar issues as the emergence of the commercial Internet. A new technology developed with exciting applications. The FCC tentatively waded into the waters, distributing licenses for CMRS services and regulating around the edges using a hodgepodge of authorities.[138] But the application of the Communications Act to CMRS was unclear. Broadcast radio, the closest historical kin to CMRS, had not traditionally been regulated as a common

137. Fixed wireless ISPs offer customers, largely in rural areas, Internet access service over the air. Some of them have argued that strict anti-prioritization rules prevent them from effectively managing traffic over their networks, which raise unique engineering issues.

138. *See generally* NUECHTERLEIN & WEISER, *supra* note 19, at 133-41.

carrier service under Title II. And the CMRS market was far from perfect. Most early CMRS markets had a duopoly structure.[139] One player in each market was typically the legacy landline voice monopolist, with an incentive not to allow burgeoning competition in the CMRS market to affect their legacy profits.[140] This dynamic led to disputes regarding the terms on which CMRS providers were entitled to interconnect their networks with the local landline provider and other CMRS providers.[141]

Congress's solution, passed in 1993, was what became 47 U.S.C. § 332(c). Section 332(c) does a number of things. First, it expressly classifies CMRS as a Title II common carrier service. Second, it provides that the FCC may "specify by regulation" that certain provisions of Title II do not apply to CMRS.[142] Third, it states that the FCC may not nullify, using this "specification" authority, certain provisions of the Communications Act, including those prohibiting unjust or unreasonable charges and discrimination.[143] Fourth, it provides that the FCC may nullify provisions as applied to CMRS only if three conditions are met.[144] Fifth, it expressly preempts the states from regulating CMRS providers in certain ways, particularly with regard to charges.[145]

The section 332(c) framework has worked tolerably well in the cellular service marketplace. The FCC has used it, as Congress intended, to adapt provisions of the Communications Act, like those provisions governing interconnection, to the CMRS market, while forbearing from the application of many other provisions, such as entry and exit licensing requirements and ex ante rate regulation, that make less sense.[146] Perhaps more controversially, the FCC has allowed CMRS providers to engage in individualized pricing practices that would typically have been anathema to a common carrier regime.[147]

The CMRS model could be straightforwardly applied to ISPs. At a minimum, Congress would declare that ISPs are common carriers, re-affirm that the FCC has broad authority not to apply provisions of the Act to them using its forbearance power, and specify any requirements (perhaps a basic "no blocking" obligation) that the FCC must apply to ISPs.

---

139. *Id.* at 133-34.

140. *Id.*

141. *Id.* at 143.

142. 47 U.S.C. § 332(c)(1)(A). This became the model for the Act's general grant of forbearance authority to the Commission, enacted in 1996. Telecommunications Act of 1996, Pub. L. No. 104-104, § 401, 110 Stat. 56, 128-30.

143. 47 U.S.C. § 332(c)(1)(A).

144. 47 U.S.C. § 332(c)(1)(A)(i)-(iii) ("(i) enforcement of such provision is not necessary in order to ensure that the charges, practices, classifications, or regulations for or in connection with that service are just and reasonable and are not unjustly or unreasonably discriminatory; (ii)enforcement of such provision is not necessary for the protection of consumers; and (iii) specifying such provision is consistent with the public interest.").

145. *Id.* § 332(c)(3).

146. *See generally* Implementation of Sections 3(n) & 332 of the Commc'ns Act, *Second Report and Order*, 9 FCC Rcd 1411 (1994).

147. *See* Orloff v. FCC, 352 F.3d 415, 420-21 (D.C. Cir. 2003) (blessing the FCC's policy).

So far, this looks a lot like a statutory codification of the Obama-era FCC's order and, for that reason, it is likely to be a political nonstarter. Indeed, the Obama-era FCC pointed to the CMRS experience when crafting its Title II-plus forbearance framework.[148] Partly due to that political reality, the CMRS model would likely need to be tweaked somewhat in order to garner support. In particular, Congress could specify that certain provisions of the Communications Act *could not* be applied to ISPs. That is, the legislation would set both a regulatory floor and a ceiling. What the FCC should be prohibited from doing could be left to political negotiation, but one obvious candidate is ex ante (and perhaps ex post) price regulation of consumer rates. When the Obama-era FCC re-classified ISPs as Title II carriers, it simultaneously forbore from those provisions of the Act, like tariffing requirements, that are designed to facilitate ex ante price controls. ISPs and the dissenting Commissioners complained, however, that a future FCC could always "unforbear" and apply such requirements, and they pointed out that the FCC retained the power, under its general authority to investigate "unjust rates," to engage in ex post price regulation.[149] These latent powers have been seen as an existential threat to ISPs and provided a basis for ISP arguments that, although they did not object to net neutrality regulation per se, they do object to Title II.[150]

Statutorily prohibiting the FCC from regulating consumer rates—perhaps with carve outs for services designed to serve lower-income individuals and others who have historically benefited from universal service—would undercut these arguments and could be paired with other reforms that would address ISP pricing practices. For one, the FCC could eliminate, or, at least narrow, the FTC Act's "common carrier exemption," which places "common carriers subject to the Acts to regulate commerce" outside of the FTC's jurisdiction.[151] Doing so would be especially necessary if the FCC was completely disabled from investigating ISP pricing practices, in order to make sure that those practices did not fall into a regulatory void. Second, the FCC could be directed to ensure that existing funding mechanisms, such as the FCC's Lifeline program, be used to support subsidizing broadband access for lower-income individuals. Third, Congress and the FCC could continue to work toward facilitating broadband "public options" in the form of municipally provided services, though this is not without its own political controversies.

To quell ISP concerns about state regulation, the imagined legislation could also contain a broad express preemption provision. Title II already

148. *See Title II Order*, *supra* note 2, at 5791, paras. 409-10.

149. *See id.* at 5922 (statement of Commissioner Ajit Pai) (citing arguments by ISPs).

150. *See* AT&T Blog Team, *Net Neutrality and Modern Memory*, AT&T PUB. POL'Y (June 6, 2014), https://www.attpublicpolicy.com/fcc/net-neutrality-and-modern-memory/ (reiterating AT&T's stance that it is not opposed to some forms of net neutrality regulation) [https://perma.cc/4ARV-AGEP]; Paul Mancini, *The FCC: Having its Forbearance Cake and Eating it Too*, AT&T PUB. POL'Y (June 16, 2010), https://www.attpublicpolicy.com/broadband/the-fcc-having-its-forbearance-cake-and-eating-it-too/ (linking the FCC's power to "unforbear" to AT&T's opposition to Title II) [https://perma.cc/LR6D-P9ED].

151. 15 U.S.C. § 45(a)(2).

expressly prohibits states from imposing requirements that are the same as those the FCC has forborne from, and that could be expanded to preempt states from regulating other issues that are thought best left to uniform federal regulation. At the same time, state authority could be preserved for matters, such as deceptive or fraudulent advertising or local franchising, that the states have traditionally had an active role in.

What are the benefits of this framework? First, by finally putting the Title II issue to bed, this approach would allow the FCC to focus on the right issues. Whether broadband ISPs should be regulated in this or that way does not depend, in my view, on whether they "offer" a telecommunications service as the Act defines it, or on such technical sub-issues as whether DNS or caching fall within the telecommunications management exception. Accepting the applicability of Title II while modulating regulation through the exercise of forbearance, by contrast, allows the FCC to focus on the right questions. The forbearance factors themselves are quite broad and allow the FCC a fair amount of discretion. But they point toward what should be the central inquiry: Does FCC regulation provide a valuable addition to background forms of regulation, such as antitrust? And answering this question properly focuses the FCC on whether regulatory interventions are justified, or whether other institutions, such as the courts or FTC, are better able to police the issue.

Second, by setting a regulatory floor and ceiling, the approach would inject some amount of regulatory certainty into the area while still allowing the FCC broad discretion to operate within the bounds opened to it. For example, the FCC would be free to adapt the Act's prohibition on "unjust and unreasonable discrimination" to new practices and in light of evolving market conditions. Other provisions of the Act governing things like privacy and subsidies, less salient in the fight over net neutrality, could be similarly adapted to the realities of the broadband market. The approach thus largely avoids the lock-in problems that are invited by several of the other alternatives discussed above.

Third, the framework installs a permanent public regulator as steward in the area. Of course, whether this is viewed as good or bad depends on one's perspective. But because of the importance of broadband Internet to society and democracy, there is a good case for embracing the public stewardship model that has been a traditional hallmark of communications regulation and public utility regulation more broadly. Doing so allows us to maintain a certain degree of democratic or quasi-democratic control over infrastructure that undergirds the modern world.

The primary drawbacks of the CMRS model follow from its strengths. ISPs will argue that any model that involves investing the FCC with authority as vague as the prohibition against "unjust" or "unreasonable" discrimination will lead to regulatory uncertainty and depress investment in broadband networks, thus undermining the FCC's goals regarding broadband deployment. That concern can be partially militated against, as discussed above, through legislation that provides a regulatory ceiling as well as a floor, taking at least certain things off the table, such as ex ante price regulation of consumer rates, that have been viewed as especially threatening to ISP profits.

Moreover, the prohibition against unjust and unreasonable discrimination has a long history and much precedent attached to it. And although the FCC has the ability, under *Chevron*, to depart from that precedent to some degree, its presence should operate to reduce the uncertainty associated with a Title II framework. Indeed, in the years that ISPs were classified under Title II, the evidence of grave uncertainty, at least as reflected in investment numbers, was difficult to detect.

IV. CONCLUSION

This essay has explored various institutional settlements concerning the regulation of Internet service providers, finding the current options to be mostly unsatisfactory. In their place, I have advocated for a surely-not-perfect-but-maybe-better alternative modeled on, with some changes, Congress's solution to CMRS.

Rethinking *Adarand* After *Prometheus*: A Rational (Basis) Solution to FCC Minority Ownership Policy

Christopher Terry*
Caitlin Ring Carlson†

TABLE OF CONTENTS

* Christopher Terry is an assistant professor of Media Law at the University of Minnesota's Hubbard School of Journalism and Mass Communication. He received his Ph.D. from UW-Madison in 2012 after spending 15 years as producer in broadcast radio. His research includes policy, regulatory and legal analysis of media ownership, media content and political advertising. Terry's research has earned top paper awards from the Communication and Law Division of the National Communication Association (NCA), the Law and Policy Division of the International Communication Association (ICA), has received financial support from both the Industry Research Forum of AEJMC and the Center for Information Policy Research. He is regularly interviewed by the media about FCC and FTC regulations.

† Caitlin Ring Carlson is an Associate Professor in the Department of Communication and Media at Seattle University. Her research focuses on media law and policy from a feminist perspective. Her first book, *Hate Speech*, was published by MIT Press in 2021. Her work has appeared in leading academic journals such as *Communication Law and Policy*, the *Journal of Media Law and Ethics,* and the *Journal of Mass Media Ethics.* Carlson's research has also been featured in mainstream media publications, including the *Wall Street Journal*, *Wired*, and *Venture Beat*. Professor Carlson teaches courses in Communication Law, Social Media, and Media Studies. She has a Ph.D. in Communication from the University of Colorado, Boulder.

I. INTRODUCTION

Although charged with serving in the public's interest, the Federal Communications Commission (FCC) has struggled to put forth a coherent media ownership policy that promotes ownership by women or minorities.[1] The agency's efforts have been plagued by a range of procedural issues and a lack of empirical evidence which became a central issue in decisions in which the Third Circuit Court of Appeals remanded media ownership decisions to the FCC four times between 2004 and 2019.[2] When the Supreme Court examined media ownership in early 2021, the Court largely avoided much of the history of media ownership policy, and in a unanimous but narrow opinion, ruled that the FCC had not acted outside a zone of reasonableness because of a lack of empirical evidence on minority ownership. Despite the ruling, the question of how to deal with an actual lack of diversity among broadcast owners and the impact that has on the public remains unanswered and is problematic.

The FCC's implementation of the ownership limits contained in the Telecommunications Act and the repeated failure of the agency to develop a functional minority ownership policy has resulted in trivial control and ownership of media properties by women and minorities. According to the 2017 data released by the FCC in 2020, women own less than 10% of all television and AM/FM radio stations and racial minorities own less than 6%.[3] Empirical evidence suggests that smaller media organizations in the control of minority owners are more likely to create content that directly targets minorities, however the agency continues to allow for greater convergence, minimizing opportunities for women and people of color.[4] By allowing the media ownership environment to degrade to this point, the FCC has limited the political participation of these groups, one of which—women—represents more than half of the U.S. population.

Throughout this process, the FCC had failed, even at the most basic of levels, to meaningfully address the lack of empirical evidence on minority

---

1. *See, e.g.*, 47 U.S.C. §§ 302(a), 307(d), 309(a), 316(a) (1934). In both the 1927 Radio Act and the 1934 Communications Act, Congress indicated that the public interest supersedes a station's interest. Both laws say that federal regulation is to be guided by "public interest, convenience, and necessity." Despite the market-driven model of current U.S. media, these laws indicate that public interest must be considered. As half of the public, this means women's interests must be considered.

2. *See* Prometheus Radio Project v. FCC, 373 F.3d 372 (3d Cir. 2004) [hereinafter Prometheus I]; Prometheus Radio Project v. FCC, 652 F.3d 431, 483 (3d Cir. 2011) [hereinafter Prometheus II]; Prometheus Radio Project v. FCC, 824 F.3d 33 (3d Cir. 2016) [hereinafter Prometheus III]; FCC v. Prometheus Radio Project, 939 F.3d 567 (3d Cir. 2019) [hereinafter Prometheus IV].

3. INDUS. ANALYSIS DIV., FCC, FOURTH REPORT ON OWNERSHIP OF BROADCAST STATIONS 6 (2017) [hereinafter FOURTH REPORT ON OWNERSHIP]. *See* FCC, FCC FORM 323: INSTRUCTIONS FOR OWNERSHIP REPORT FOR COMMERCIAL BROADCAST STATIONS (2017) [hereinafter 2017 323 REPORT].

4. Christopher Terry & Caitlin Ring Carlson, *Hatching Some Empirical Evidence: Minority Ownership Policy and the FCC's Incubator Program*, 24 COMM. L. & POL'Y 403, 407 (2019).

ownership policy.[5] Prior to the 1996 Telecommunications Act, however, the FCC had been responsive to the "nexus" principle that minority voices should have access to the airwaves.[6] Prompted, at least in part, by the changes brought about by the Civil Rights movement, in 1965, the FCC said that its two objectives when awarding its highly coveted broadcast television and radio licenses were to provide the best possible service to the public and to promote diversity in control of the mass media.[7] Under this framework, race, and, later, gender could be considered in comparative hearings, and preferential treatment was given to diverse applicants. In order to promote the public interest, the FCC developed policies designed, at least nominally, to expand minority ownership.[8]

Over the ensuing decades, media organizations repeatedly challenged these rules as part of a larger agenda that promoted the consolidation of ownership of broadcast stations. In response, the U.S. Supreme Court established in 1990 in *Metro Broadcasting v. FCC* that racial preferences for awarding broadcast licenses must withstand intermediate scrutiny.[9]

However, just five years later, the Supreme Court held in *Adarand Constructors, Inc. v. Pena* that the presumption of a disadvantage based on race alone as a justification for preferred treatment was discriminatory and violated the Due Process Clause of the Fifth Amendment.[10] Thus, any laws or regulations that showed preferred treatment to people based solely on their race would subsequently need to withstand strict scrutiny.[11]

Arguing that any initiative it developed could not meet the requirements of strict scrutiny, the FCC has avoided embedding preferences based on race (or gender) into regulations of media ownership since the *Adarand* decision. During the running legal battle with Prometheus Radio Project and the citizen petitioners, the agency even argued that the *Adarand* decision makes the entire process of assessing minority ownership, much less developing a policy to enhance it, functionally impossible.[12] As a result, the number of women and people of color who own broadcast media outlets remains abysmally small according to data released by the FCC.[13] Over the last two decades, the FCC was unable (and largely unwilling) to meet the Third Circuit's remands to better address the efficacy of their minority ownership policies, in large

---

5. *Id.*

6. David Honig, *How the FCC Suppressed Minority Broadcast Ownership, and How the FCC Can Undo the Damage It Caused*, 12 S.J. POL'Y & JUST. 44 (2018).

7. 1965 FCC Pol'y Statement on Comparative Broad. Hearings, *Public Notice*, 1 F.C.C. 2d 393, 394 (1965).

8. Honig, *supra* note 6, at 51.

9. Metro Broad., Inc. v. FCC, 497 U.S. 547, 606 (1990).

10. Adarand Constructors, Inc. v. Pena, 515 U.S. 200 (1995).

11. *Id.* at 227.

12. The FCC adopted the Small Business Administration's revenue-based definition of eligible entities and defended it as a legally supportable means of promoting minority and female ownership because the requirements were content neutral. 2014 Quadrennial Regul. Rev.– Rev. of the Comm'n's Broad. Ownership Rules and Other Rules Adopted Pursuant to Section 202 of the Telecomms. Act of 1996, *Second Report and Order*, 31 FCC Rcd 9864 (2016) [hereinafter *2016 Second Report and Order*].

13. 2017 323 REPORT, *supra* note 3.

part because the agency's approach to the problem has arguably been based on flawed reasoning. Rather than being paralyzed by the strict scrutiny requirement put forth by *Adarand*,[14] the FCC should be arguing that broadcast regulations have traditionally been subject only to a rational basis review, a position the Supreme Court upheld in *FCC v. Pacifica Foundation* in 1978.[15] There is significant historical precedent for treating licensed broadcasters differently in regulatory terms. In *NBC v. United States*, the Supreme Court said the FCC was more than a traffic officer, and that it had an obligation to determine the nature of the traffic on the airwaves.[16] Likewise, in *Red Lion v. FCC*, the Court unanimously declared that the FCC did not infringe on the First Amendment rights of broadcasters by keeping the airwaves open through regulation, and that the rights of the listeners were paramount.[17]

Not only does increasing ownership diversity (and the likelihood for a corresponding increase in content) benefit would-be station owners, this type of regulation does not infringe on broadcasters First Amendment rights.[18] Moreover, broadcast regulations designed to put more stations in the hands of women and people of color also directly serves the interests of listeners and viewers, which has been the traditional standard used to judge the outcomes of the FCC's broadcast policy. The law has required that the FCC act in the public's interest for nearly ninety years. However, the agency has failed to do so legally, functionally, and empirically, even using its own metrics meet this goal.[19]

This article will explore the role of minority ownership policy within the larger context of media ownership regulation, focusing on the implications of the *Adarand* decision. *Adarand* has become the FCC's most useful scapegoat for the agency's failed attempts to resolve the four remands from the Third Circuit Court of Appeals; *Adarand* also could have played an important role in the Supreme Court's decision, had the Court chosen to address the issue of minority ownership head-on rather than focusing their decision on issues surrounding administrative agencies' discretion regarding their actions and initiatives.[20] The article then argues that the historical application of rational basis review of broadcast regulations should be employed as an option to break the nearly two decade long legal, policy, and regulatory deadlock over media ownership policy. In anticipation of the FCC's future ownership review proceedings, the article concludes with a simple proposal to increase racial and gender diversity among media owners.

---

14. *Adarand Constructors*, 515 U.S. at 227.

15. FCC v. Pacifica Found., 438 U.S. 726, 748 (1978) (stating that "of all forms of communications, it is broadcasting that has received the most limited First Amendment protection.").

16. Nat'l Broad. Co. v. United States, 319 U.S. 190, 215-16 (1943).

17. *Red Lion Broad. v. FCC*, 395 U.S. at 375, 390 (1969) (holding that the "fairness doctrine" as applied to the RTNDA "enhance[d] rather than abridg[ed]" First Amendment liberties).

18. *Id.* at 390.

19. 47 U.S.C. §§ 302a(a), 309(a), 316(a).

20. FCC v. Prometheus Radio Project, 141 S. Ct. 1150, 1152 (2021).

II. THE FCC, MEDIA OWNERSHIP, AND THE ISSUE OF MINORITY OWNERSHIP

Some scholars have argued that the media ownership policy dispute goes back to the 1920s,[21] and others have argued that the implementation of the 1996 Telecommunications Act was the defining moment for media ownership policy.[22] In reality, however, the inception point for modern media ownership theory was the six-year long FCC proceeding between 1969 and 1975, which resulted in the agency's ban on Newspaper-Broadcast Cross Ownership.[23] During the lengthy review, the FCC developed a rule that restricted the ability of a single entity to own and operate broadcast stations and a daily newspaper in the same market.[24]

Since the agency's passage of the newspaper-broadcast cross ownership ban in 1975,[25] the FCC has relied on a regulatory premise that conceptually ties the ownership of stations to the level of content diversity available to citizens at the market level.[26] While the conceptual premise that ownership and content are directly related has become the "touchstone premise" of FCC regulation of broadcaster ownership for more than fifty years,[27] the body of empirical evidence supporting this regulatory premise has been inconsistent at best.[28] At the base level, the debate over media ownership represents a policy conflict between increasing the economic efficiency of media companies and the traditional societal goals associated with citizen access to diverse information.[29] Despite the lack of support for the conceptual relationship this approach is based on, the FCC has repeatedly attempted to implement media ownership policy through numerical ownership limits (as

---

21. *See* ROBERT W. MCCHESNEY, TELECOMMUNICATIONS, MASS MEDIA, AND DEMOCRACY: THE BATTLE FOR THE CONTROL OF U.S. BROADCASTING, 1928-1935 13 (1993).

22. *See* Bruce E. Drushel, *The Telecommunications Act of 1996 and Radio Market Structure*, 11 J. Media Econ. 3 (1998).

23. *See* Christopher Terry, *Localism as a Solution to Market Failure: Helping the FCC Comply with the Telecommunications Act*, 71 FED. COMM. L.J. 327, 334-35 (2019).

24. Multiple Ownership of Standard, FM, & TV Broad. Stations, *Second Report and Order*, 50 F.C.C. 2d 1046, 1084 (1975).

25. *Id.*

26. The FCC has employed a range of methodologies ranging from voice counts to Congressional mandated ownership limits, but defends the use of quantitative limits as a proxy protection for diversity. *See* Sinclair Broad. Grp., Inc. v. FCC, 284 F.3d 148, 154 (D.C. Cir. 2002).

27. 2002 Biennial Regul. Rev., Rev. of the Comm'n's Broad. Ownership Rules and Other Rules Adopted Pursuant to Section 202 of the Telecomms. Act of 1996, *Report and Order and Notice of Proposed Rulemaking*, 18 FCC Rcd 13620, para. 6 (2003) [hereinafter *2002 Biennial Review*].

28. Adam Candeub, *Media Ownership Regulation, the First Amendment, and Democracy's Future*, 41 U.C. DAVIS L. REV. 1547, 1603 (2008).

29. *See* MCCHESNEY, *supra* note 21, at 16.

the policy implementation) as a proxy for assessing the diversity of media content (the agency's stated policy goal).[30]

While relying heavily on a regulatory philosophy which promotes economic competition and a corresponding policy implementation that favors quantitative assessments of diversity using proxy measurements, the FCC continues to recognize that access to a wide range of "diverse and antagonistic" viewpoints is essential.[31] While there is little debate that substantial viewpoint diversity exists in the modern media environment, the problem for regulators requires developing policy that results in public access to viewpoint diversity at the same time that it allows for an assessment of competition.[32] In the context of minority ownership's policy objectives, the access to viewpoints from underrepresented groups includes not just racial or ethnic minorities, but also women.[33]

In defense of the FCC's efforts, as well as its failures, media ownership policy is a complex issue that incorporates a range of economic, regulatory and social objectives, many of which are in direct conflict with one another. But the agency has done itself no favors in a continuing effort to simultaneously regulate media based on three policy objectives: competition, localism, and diversity. Favoring competition through the implementation of structural limits on numerical broadcast station ownership,[34] the FCC launched a localism and broadcasting initiative which involved a formal notice and comment proceeding on broadcasting and localism.[35] Additionally, in a vain effort to ensure diversity which the FCC repeatedly claims to be

30. *See, e.g.,* 2014 Quadrennial Regul. Rev. – Rev. of the Comm'n's Broad. Ownership Rules and Other Rules Adopted Pursuant to Section 202 of the Telecomms. Act of 1996, *Order on Reconsideration and Notice of Proposed Rulemaking*, 32 FCC Rcd 9802, para. 15 (2017) [hereinafter *2017 Ownership NPRM*] (These changes eliminated the newspaper/ broadcast cross-ownership rule, the radio / television cross-ownership rule, and the eight-voices test). *2016 Second Report and Order*, *supra* note 12, at para. 7 (This report contained no data regarding the diversity of broadcast media content.).

31. *2016 Second Report and Order*, *supra* note 12, at para. 207.

32. *See* Terry, *supra* note 23, at 329-30.

33. Phillip Napoli proposes that providing diversity is worthless without exposure. Content, especially informational content is a necessity, but consumption of the content is also required. Philip M. Napoli, *Deconstructing the Diversity Principle*, 49 J. COMM. 7, 9 (1999).

34. Rev. of the Comm'n's Reguls. Governing TV Broad., *Further Notice of Proposed Rulemaking*, 10 FCC Rcd 3524, para. 60 (1995) ("The principal means by which the Commission has fostered diversity of viewpoints is through the imposition of ownership restrictions…. [D]iversity of ownership as a means to achieving viewpoint diversity has been found to serve a legitimate government interest, and has, in the past, been upheld under rational-basis review."). *See also* Rev. of the Comm'n's Broad. Ownership Rules and Other Rules Adopted Pursuant to Section 202 of the Telecomms. Act of 1996, *Notice of Proposed Rule Making*, 17 FCC Rcd 18503, paras. 36-55 (2002) [hereinafter *2002 Ownership Rules*].

35. The FCC's localism task force was created in 2003, but it has taken only limited actions in the eight years since its inception, and it has taken no formal action since April of 2008. *See* FCC, BROADCASTING AND LOCALISM, https://transition.fcc.gov/localism/Localism_Fact_Sheet.pdf [https://perma.cc/ZSN8-6P3A].

important,[36] the Commission has struggled to follow a consistent regulatory path when developing and reviewing its media ownership rules.[37]

Within the larger structure of media ownership policy is a related issue: the ownership of broadcast stations by women and minorities. Minority ownership has proven to be a problematic aspect of the FCC's broadcast licensing efforts for some time.[38] The FCC granted licenses exclusively to non-minority applicants for radio stations until 1949 and for television stations until 1973.[39] This process continued beyond these origination dates as the agency tended to favor applicants with existing broadcast industry experience in cases where there were competitive and comparative hearings for licenses.[40] Consequently, as late as 1971, minorities owned only ten of the nearly 7,500 radio stations in the U.S.[41]

The FCC established a Minority Ownership Task Force with the intent of researching options to increase not only minority ownership, but minority employment in the broadcasting industry as well, arguing, "representation of minority viewpoints in programming serves not only the needs and interests of the minority community but also enriches and educates the non-minority audience."[42] In 1978, the task force released a report that concluded that the best option to increase minority representation was to increase the number of minority owners, arguing that both minority populations and the general public were being deprived the access of minority viewpoints.[43]

In a critical case, *TV 9, Inc. v. FCC*, the idea that a nexus between minority ownership and increased viewpoint diversity was established and quickly became the conceptual basis for minority ownership policy, which the FCC expanded on in the Newspaper Broadcast-Cross Ownership proceeding.[44] In the *TV 9* case, the FCC had chosen not to award a minority, but corporate, candidate merit in a comparative hearing for a license.[45] The D.C. Circuit Court overturned the FCC, arguing "[m]inority ownership is likely to increase diversity of content, especially of opinion and viewpoint, merit should be awarded."[46]

---

36. *2002 Biennial Review*, *supra* note 27, at paras. 18-53.

37. Christopher R. Terry, *Minority Ownership: An Undeniable Failure of FCC Media Ownership Policy,* WIDENER J.L., ECON. & RACE, 2013, at 18, 32 (2011).

38. *See* Caitlin Ring Carlson, *Half the Spectrum: A Title IX Approach to Broadcast Ownership Regulation*, 23 COMM. L. & POL'Y 221, 227-28 (2018).

39. W. LaNelle Owens, *Inequities on the Air: The FCC Media Ownership Rules - Encouraging Economic Efficiency and Disregarding the Needs of Minorities*, 47 HOW. L.J. 1037, 1055 (2004).

40. *Id.* at 1045.

41. *Id.* at 1044.

42. Neal Devins, Metro Broadcasting, Inc. v. FCC*: Requiem for a Heavyweight*, 69 TEX. L. REV. 125, 144 n.132 (1990) (quoting Statement of Policy on Minority Ownership of Broadcasting Facilities, *Public Notice*, 68 F.C.C. 2d 979, 981 (1978)).

43. *See id.* at 134, 151.

44. TV 9, Inc. v. FCC, 495 F.2d 929, 938 (D.C. Cir. 1973); Multiple Ownership of Standard, FM, and TV Broad. Stations, *Second Report and Order*, 50 F.C.C. 2d 1046, 1074 (1975).

45. *TV 9*, 495 F.2d at 938.

46. *Id.*

In 1978, following *TV 9*, the FCC adopted two new policies designed to expand minority representation on the airwaves. The first was a tax certificate program to help new entrants.[47] Likewise, the second policy, a distressed station sale program, was adopted to help direct station licenses towards minority applicants by giving broadcast licensees the opportunity to sell a station to a minority-owned entity at a reduced price of 75% of fair market value.[48]

The FCC's 1978 minority ownership enhancement policies were challenged and were initially upheld in *Metro Broadcasting Inc. v FCC*.[49] Metro Broadcasting was involved in a comparative bidding proceeding for the rights to construct and operate a new UHF television station in Orlando, Florida.[50] The FCC awarded the license and construction permit to a competitor, Rainbow Broadcasting. The FCC had given a substantial enhancement to Rainbow because its ownership was 90% Hispanic, while Metro had only one minority partner.[51] The FCC ruled that the minority enhancement awarded to Rainbow outweighed the local residence and civic participation advantage that Metro had demonstrated in the proceeding.[52]

In a related case, *Shurberg Broad. of Hartford, Inc. v. FCC*, Shurberg Broadcasting challenged the FCC's distress sale policy after filing a construction permit to build a station in Hartford, Connecticut.[53] At the time, the permit was mutually exclusive with a station already on the air, which the owner, Faith Center, was trying to sell under the distress sale policy.[54] The FCC approved the transfer of the station under the distress sale policy in 1980, but the applicant faced financing problems that caused the transfer to be abandoned.[55] In June of 1984, the FCC approved a second transfer of the station's license under the distress sale policy to minority applicant Astroline Communications.[56] Shurberg then petitioned the FCC to hold a comparative license hearing to examine the mutually exclusive applications.[57] The FCC denied the hearing request, rejected Shurberg's challenge as without merit, and awarded the license to Astroline.[58]

At the Circuit level, both the *Metro* and *Shurberg* challenges were focused on an argument that the FCC's 1978 policies violated the Equal Protection Clause.[59] On review, the D.C. Circuit upheld the FCC's decision

---

47. Owens, *supra* note 39, at 1045-46.
48. *Id.*
49. *Metro Broad., Inc. v. FCC*, 497 U.S. 547 (1990).
50. *Id.* at 558.
51. *Id.* at 559.
52. *Id.*
53. *Id.* at 562-63.
54. *Id.*
55. *Id.*
56. *Id.* at 562 (citing App'n of Faith Ctr., Inc., *Memorandum Opinion and Order*, 99 F.C.C. 2d 1164, 1171 (1984)).
57. *Id*. at 562.
58. *Id. See also* App'n of Faith Ctr., Inc., *Memorandum Opinion and Order*, 99 F.C.C. 2d 1164, 1171 (1984).
59. *See* Shurberg Broad. of Hartford, Inc. v. FCC, 876 F.2d 902 (D.C. Cir. 1989); Winter Park Comm., Inc. v. FCC, 873 F.2d 347 (D.C. Cir. 1989).

regarding Metro Broadcasting but overturned the agency's sale to Astroline, ruling in favor of Shurberg.[60] In the *Shurberg* decision, the circuit court ruled that the distress sale policy was not, "narrowly tailored to remedy past discrimination or to promote programming diversity."[61] The cases were consolidated for review in front of the Supreme Court.[62]

In reviewing the dispute in *Metro*, the Supreme Court examined a number of empirical studies that supported the conceptual "nexus" between minority ownership and viewpoint diversity.[63] Of the research examined, the conclusions contained in a Congressional Research Service study, "Minority Broadcast Station Ownership and Broadcast Programming: Is There a Nexus?" proved important.[64] The research concluded, based on FCC survey data, that increasing minority ownership in a market led to an increase in diversity of the available programming content.[65]

In the *Metro v. FCC* decision, the Supreme Court held that both of the FCC's minority enhancement policies could withstand "intermediate" scrutiny of the Fifth Amendment's Equal Protection Clause.[66] The decision proposed five significant reasons for reducing the level of protection from strict to intermediate scrutiny in this area.[67] First, the minority ownership policies at issue in *Metro* served an important government objective, as all audiences, not just those made up of minorities are served by an increase in the diversity of viewpoints minority owners were likely to provide.[68] On a second, related point, the Court added that the policies were directly related to the long standing goal of content diversity.[69] Justice Brennan argued that the robust exchange of ideas that minorities were able to engage in as a result of the minority enhancement policies resulted in positive influence for news production while promoting diversity in the hiring practices of existing media outlets.[70] Justice Brennan also said that the FCC's previous policies to promote minority access, including community ascertainment, had failed to provide adequate minority content to listeners.[71] Therefore, the policies under review in *Metro* served an important governmental objective, but were also substantially related to the government's interest.

Importantly, Justice Brennan also noted the "overriding significance" of the fact that the FCC's enhancement and distress sale policies had been specifically mandated and approved by Congress.[72] In light of these factors,

---

60. *Metro Broad.*, 497 U.S. at 562; *Shurberg Broad. of Hartford*, 876 F.2d at 907-08.
61. *Metro Broad.*, 497 U.S. at 563.
62. *Id.* at 552.
63. *Id.* at 569-70.
64. *Id.* at 578-79; *see also* Allen S. Hammond, IV, *Measuring the Nexus: The Relationship Between Minority Ownership and Broadcast Diversity After Metro Broadcasting*, 51 FED. COMM. L.J. 627 (1999).
65. Hammond, *supra* note 64.
66. *Metro Broad.*, 497 U.S. at 566.
67. *Id.*
68. *Id.* at 567.
69. *Id.* at 567-68.
70. *Id.* at 569-70.
71. *Id.* at 586-87.
72. *Id.* at 563.

the Court ruled that the substantial government interest in promoting diversity outweighed any equal protection violations, adding that the petitioners were free to bid on any other stations that became available.[73] In practical terms, the majority employed an intermediate standard of review in *Metro* relying on a "substantial" rather than "compelling" interest.

III. *ADARAND*, STRICT SCRUTINY AND MINORITY OWNERSHIP

Despite the decision in *Metro*, in 1995, the protections for the FCC's licensing enhancement and distress sale programs were overturned in a non-broadcast case, *Adarand Constructors Inc. v. Pena*.[74] In *Adarand*, the four dissenters in the *Metro* Court and the newly appointed Justice Clarence Thomas, who had ruled against a gender-based enhancement in *Lamprecht v. FCC* while on the D.C. Circuit,[75] struck down a federal program granting preferences to minorities bidding on public works projects.[76] In *Adarand*, the majority found that the Court should have applied a strict scrutiny test to the policies at issue in *Metro*.[77]

A dispute over preference given to a minority business as part of a Small Business Administration (SBA) minority preference program for contractors was at the center of the dispute in the case.[78] Adarand Constructors challenged the preference policy after failing to win a government bidding process for a contract to construct highway rail guards in Colorado.[79] Adarand was otherwise qualified complete the work and had even submitted the lowest bid on the project.[80] The Court held that Adarand had standing to bring its suit, and that all programs for federal, state, and local entities should be reviewed under a strict scrutiny standard, thus resolving the difference between the federal and state reviews upheld in *Metro* and *City of Richmond v. J.A. Croson Co.*[81]

As part of this newer, more tailored approach to judicial review of government preference programs, the majority decision proposed that strict

---

73. *Id.* at 596.

74. Adarand Constructors, Inc. v. Pena, 515 U.S. 200, 227 (1995).

75. Lamprecht v. FCC, 958 F.2d 382 (D.C. Cir. 1992).

76. *Adarand Constructors*, 515 U.S. at 227.

77. *Id.* ("[W]e hold today that all racial classifications, imposed by whatever federal, state, or local government actor, must be analyzed by a reviewing court under strict scrutiny. In other words, such classifications are constitutional only if they are narrowly tailored measures that further compelling governmental interests. To the extent that Metro Broadcasting is inconsistent with that holding, it is overruled").

78. *Id.*

79. *Id.*

80. *Id.*

81. Justice O'Connor's opinion in *Croson* also applied strict scrutiny to a quota based system, and in overturning the City's provision requiring 30% of city building contracts went to Minority Business Entity subcontractors, explained that rules designed as a remedy for past discrimination did not reach a compelling government interest. "The dream of a Nation of equal citizens in a society where race is irrelevant to personal opportunity and achievement would be lost in a mosaic of shifting preferences based on inherently unmeasurable claims of past wrongs." *City of Richmond v. J.A. Croson Co.*, 488 U.S. 469, 505 (1989).

scrutiny was not "strict in theory and fatal in fact,"[82] and applied three principles to a review: First, race-based criterion should always be treated with skepticism.[83] Second, equal protection should be consistently applied and not depend on race for the group benefitting or being burdened by the program.[84] Finally, an analysis of equal protection demanded "congruence" under both the Fifth and Fourteenth Amendments.[85]

As a result of *Adarand*, all minority preferences, including programs designed to correct "benign discrimination," required narrow tailoring to meet a compelling governmental interest.[86] The decision explicitly overturned the holding in *Metro* that the FCC's "benign" minority ownership policies need only meet intermediate scrutiny.[87] Arguably, the Court's majority no longer supported diversity as sufficient to justify race-based classifications in public contracting.[88] Functionally, after *Adarand*, a preferential government program requires empirical statistical evidence to (1) demonstrate previous discrimination, and, (2) show that the program under review meets a narrow tailoring test which assesses if the policy will correct that discrimination.[89]

After *Adarand*, the mandate imposing stringent justifications for preferential programs led the FCC to discontinue the distress sale policy: first, by refusing to extend the policy to women, and then by refusing to extend a preferential policy during spectrum auctions.[90] But *Adarand* would bring even more complications to the FCC's policymaking process and regulatory objectives following the passage of the 1996 Telecommunications Act, which lingered in the background until the Third Circuit Court of Appeals decision in *Prometheus Radio Project v. FCC (Prometheus I)* in 2004.

IV. *LAMPRECHT*, INTERMEDIATE SCRUTINY, AND WOMEN'S OWNERSHIP

Initially, minority and female ownership were viewed as separate issues. However, in the *Mid-Florida Television Corp.* case (1978), the Second Circuit Court of Appeals held that merit for female broadcast ownership and participation is warranted upon essentially the same basis as the merit given for black participation and ownership.[91] The court said that the need for diversity and sensitivity reflected in the structure of a broadcast station is "not so pressing with respect to women as it is to black people because women

82. *Adarand Constructors*, 515 U.S at 237.
83. *Id.*
84. *Id.*
85. *Id.*
86. *Id.*
87. *Id.*
88. *Id.*
89. *Id.*
90. While awaiting a decision from the Supreme Court in the *Shurberg* and *Metro* cases, the Commission closed down a rulemaking proceeding that could have expanded the Distress Sale policy to new categories of participants, including women. *See* Distress Sale Pol'y of Broad. Licensees, *Order*, 5 FCC Rcd 397, para. 2 (1990).
91. App'ns of Mid-Fla. TV Corp., *Decision*, 69 F.C.C. 2d 607, 652 (1978), *set aside on other grounds,* 87 F.C.C. 2d 203 (1981).

have not been excluded from mainstream society as have black people."[92] At a subsequent comparative hearing the board said it was "obliged to consider minority (and presumably, female) ownership and participation as qualitative attributes of and management."[93] Thus, female preference grew out of a presumption.[94]

Like with minority preferences, the FCC's efforts to demonstrate favorable treatment for women in the distribution of broadcast licenses was also challenged. The first of these challenges was brought by a male applicant who was denied a license in favor of a woman, despite having substantial industry experience. [95] The D.C. Circuit Court found that the FCC's rationale for the claim that gender preferences in comparative hearings and the subsequent ownership of media by women fostered a diversity of viewpoints was unconfirmed.[96] The court held that the premise had not been critically examined in this case and also ran counter to the constitutional principle that race, sex, and national origin are not valid factors on which to base government policy.[97] Judge Patricia Wald, who was the only woman on the court and the only dissenting judge in the case, wrote that ownership diversity was the only way the FCC could influence diverse content as it was prohibited from mandating the broadcast of particular moral, social, or political viewpoints.[98] Moreover, "[w]omen having ownership interest and policy making roles in the media are likely to enhance the probability that varying perspectives and viewpoints of women will be fairly represented by the broadcast media."[99]

The D.C. Circuit Court took up the relationship between viewpoint diversity and promoting women (and minority) ownership again in *Lamprecht v. FCC*.[100] Here, the court held that the FCC "cited nothing that might support its predictive judgment that women owners will broadcast women's or minority or any other underrepresented type of programming at any different rate than men will";[101] the court was right. Very little research existed to examine whether and how women's broadcast ownership led to diverse programming. Once again, the court relied on the 1988 study, "Minority Broadcast Station Ownership and Broadcast Programming: Is there a Nexus?"[102] The court wrote that because the study did not establish a statistically meaningful link between women's broadcast ownership and "women's programming," the FCC could not prove that the regulation was substantially related to achieving their important objective of viewpoint

92. *Id.*
93. Lorna Veraldi & Stuart A. Shorenstein, *Gender Preferences*, 45 FED. COMM. L.J. 219, 223 (1993).
94. *See id.*
95. Steele v. FCC, 770 F.2d 1192, 1192 (D.C. Cir. 1985).
96. *Id.* at 1199.
97. *Id.*
98. *Id.* at 1202 (Wald, J., dissenting).
99. *Id.* at 1209.
100. Lamprecht v. FCC, 958 F.2d 382, 399 (D.C. Cir. 1992).
101. *Id.*
102. *Id.* at 396.

diversity.[103] This time, the FCC's gender preference did not meet the requirements of intermediate scrutiny and was struck down.[104] Perhaps most notably, the D.C. Circuit reaffirmed that the standard of review for gender-based preferences was intermediate scrutiny while strict scrutiny continued to be used for race-based preferences.[105]

V. THE THIRD CIRCUIT AND PROMETHEUS RADIO PROJECT

The FCC launched the first of the mandated biennial reviews for media ownership rules under section 202(h) on March 12, 1998.[106] At the time, the agency was adjudicating many proposed mergers and license transfers made possible by ownership rules contained in the Telecom Act. Anticipating that the biennial review process would result in additional changes to those rules, the FCC had already granted a series of conditional waivers to various owners.[107] By continuing to grant waivers, even conditionally, the FCC openly encouraged further ownership consolidation to occur at a rate faster than the agency could empirically assess the results of its freshly approved mergers.[108]

At the conclusion of the first biennial review in August of 1999, the FCC chose to use the required 2000 Biennial Review to build a framework to "form the basis for further action."[109] Mergers were occurring at a rapid pace,

---

103. *Id.* at 398.

104. *Id.* at 396.

105. *Id.* at 390.

106. The FCC already began the process of reviewing two ownership rules. The first, the television duopoly rule prevented a party from owning, operating, or controlling two or more broadcast television stations with overlapping "Grade B" signal contours, essentially preventing the ownership of more than one television station in a market. Additionally, the FCC launched a review of the "one-to-a-market" rule, which prohibited the common ownership of a television and a radio station in the same market. 1998 Biennial Regul. Rev.– Rev. of the Comm'n's Broad. Ownership Rules and Other Rules Adopted Pursuant to Section 202 of the Telecomms. Act of 1996, *Notice of Inquiry*, 13 FCC Rcd 11276, paras. 1, 9 (1998) [hereinafter *1998 Notice of Inquiry*].

107. App'n of Concrete River Assocs., *Memorandum Opinion and Order*, 12 FCC Rcd 6614, paras. 108-10 (1997), assigning a license to QueenB Radio and granting QueenB's request for waiver, "Because the present case also proposes a commonly owned television station, we must next determine whether to waive our one-to-a-market rule. In considering the current request for a permanent waiver we will follow the policy established in recent one-to-a-market waiver cases where the radio component to a proposed combination exceeds those permitted prior to the adoption of the Telecommunications Act of 1996. . . . In such cases, the [FCC] declined to grant permanent waivers of the one-to-a-market rule, and instead granted temporary waivers conditioned on the outcome of related issues raised in the television ownership rulemaking proceeding. . . . Similarly, we conclude that a permanent, unconditional waiver would not be appropriate here. QueenB has, however, demonstrated sufficient grounds for us to grant a temporary waiver conditioned on the outcome of the rulemaking proceeding."

108. *Id.*

109. 2000 Biennial Regul. Rev., *Report*, 15 FCC Rcd 1207, para. 13 (2001) [hereinafter *2000 Biennial Review*. While the review was of existing regulations agency wide, media ownership rules were reviewed by the Media Bureau staff during the 2000 proceeding. *See* Biennial Reg. Rev. 2000 Staff Rpt., *Public Notice*, 15 FCC Rcd 21142, para. 43 (2000) [hereinafter *2000 Staff Report*].

and the FCC argued that it needed more time to understand the effects the rules were having.[110]

At the launch of the biennial review in 2000, the FCC proposed building a working framework for future reviews under section 202 (h), most notably for the review scheduled to begin in 2002.[111] As a result of the agency-wide review commenced in 2000, the FCC proposed retaining, but modifying, three of its media ownership rules while eliminating a fourth.[112] The FCC then launched rulemaking inquiries to amend the dual network rule,[113] the definition of local radio markets,[114] and the newspaper-broadcast cross-ownership rule.[115] The agency also proposed to eliminate its restriction on multiple ownership of experimental broadcast stations.[116] Ultimately, each of these individual proceedings would become elements of the next required review under section 202(h), the 2002 Biennial Review.

The FCC's lengthy legal struggles on media ownership policy began with the judicial review of the its media ownership decision released in June of 2003.[117] In *Prometheus Radio Project v. FCC*, the FCC suffered the first in a long of a series of setbacks that have continued to limit its ability to alter media ownership policy.[118] Groups of both "citizen petitioners"[119] and "deregulatory petitioners"[120] challenged the FCC's 2003 Order on media ownership in multiple federal circuit courts, and the Judicial Panel on Multidistrict Litigation consolidated the petitions.[121] Unlike *Sinclair*

110. *Id.* at para. 127.
111. *Id.* at paras. 14-17.
112. *Id.* at para. 30.
113. *Id.* at para. 127.
114. *Id.* at paras. 118-19.
115. *Id.* at paras. 122-24.
116. *Id.* at para. 128.
117. *Prometheus I*, 373 F.3d 372, 381 (3d Cir. 2004).
118. *Id.* at 381-82.
119. In the *Prometheus* ruling, the court assigned the various petitioners to two groups. The first was referred to as the "Citizen Petitioners." "Prometheus Radio Project, Media Alliance, National Council of the Churches of Christ in the United States, Fairness and Accuracy in Reporting, Center for Digital Democracy, Consumer Union and Consumer Federation of America, Minority Media and Telecommunications Council (representing numerous trade, consumer, professional, and civic organizations concerned with telecommunications policy as it relates to racial minorities and women), and Office of Communication of the United Church of Christ ("UCC") (intervenor). The Network Affiliated Stations Alliance, representing the CBS Television Network Affiliates Association, the NBC Television Affiliates, and the ABC Television Affiliates, and Capitol Broadcasting Company, Inc. (intervenor) also raised anti-deregulatory challenges to the national television ownership rule." *Prometheus I*, 373 F.3d at 381 n.1.
120. *See id.* at 381-82 n.2 (stating that the "Deregulatory Petitioners," included: "Clear Channel Communications, Inc.; Emmis Communications Corporation; Fox Entertainment Group, Inc.; Fox Television Stations, Inc.; Media General Inc.; National Association of Broadcasters; National Broadcasting Company, Inc.; Paxson Communications Corporation; Sinclair Broadcast Group; Telemundo Communications Group, Inc.; Tribune Company; Viacom Inc.; Belo Corporation (intervenor); Gannett Corporation (intervenor); Morris Communications Company (intervenor); Millcreek Broadcasting LLC (intervenor); Nassau Broadcasting Holdings (intervenor); Nassau Broadcasting II, LLC (intervenor); Newspaper Association of America (intervenor); and Univision Communications, Inc. (intervenor)".) *Id.*
121. *Id.* at 382.

Broadcasting Group, Inc. v. FCC and *Fox TV Stations, Inc. v. FCC*, two earlier cases that dealt with ownership reviews undertaken by the agency which were reviewed by the D.C. Circuit Court of Appeals,[122] the multidistrict panel sent the case to the Third Circuit Court of Appeals, consolidating the challenges under lead plaintiff in that circuit, Prometheus Radio Project.[123] After a preliminary hearing, the Third Circuit stayed implementation of the FCC's 2003 rules pending review.[124]

The Third Circuit remanded most of the FCC's 2003 Order.[125] Among the primary reasons for remand was the FCC's arbitrary and capricious decision-making process and the lack of supporting evidence for its decisions in the record.

> [W]e have identified several provisions in which the [FCC] falls short of its obligation to justify its decisions to retain, repeal, or modify its media ownership regulations with reasoned analysis. The [FCC]'s derivation of new Cross-Media Limits, and its modification of the numerical limits on both television and radio station ownership in local markets, all have the same essential flaw: an unjustified assumption that media outlets of the same type make an equal contribution to diversity and competition in local markets. We thus remand for the [FCC] to justify or modify its approach to setting numerical limits.[126]

The Third Circuit was extremely skeptical of the FCC's new approach to regulating media ownership using the Diversity Index.[127] The court's opinion suggested that the FCC's assumption of equal market shares was inconsistent with the intended approach of the agency's new metric.[128] This inconsistency generated a set of unrealistic assumptions about the relative contributions of media outlets to viewpoint diversity within local markets. Local news production, which the FCC functionally applied as a quantitative assessment of its localism objective, factored heavily into the majority decision, which stated the record lacked basic evidence to support the agency's premise of independent news websites producing local news.[129]

After the Third Circuit issued the remand in 2004, the FCC took minimal action on media ownership policy beyond adjudicating merger

---

122. Sinclair Broad. Grp., Inc. v. FCC, 284 F.3d 148 (D.C. Cir. 2002); Fox TV Stations, Inc. v. FCC, 280 F.3d 1027, 1033, 1048 (D.C. Cir. 2002).

123. *Prometheus I*, 373 F.3d at 382.

124. *Id.* at 389.

125. *Id.* at 435*; See also 2002 Biennial Review*, *supra* note 27, at para. 327 (describing the cross-ownership rulemaking by the FCC — with foregoing explanation — with which the Third Circuit found fault).

126. *Prometheus I*, 373 F.3d at 435.

127. *See id.* at 411.

128. *Id.* at 420.

129. *Id.* at 406.

actions that were permitted by existing ownership limits.[130] A new FCC chairman, Kevin Martin, took charge in March 2005,[131] and the agency launched into the first now quadrennial review scheduled for 2006 under the amended section 202(h) of the Telecommunications Act.[132] At the launch of the review process, the FCC suggested it had designed the assessment to resolve any procedural issues from the *Prometheus I* remand.[133]

The late release of data developed during the 2002 Biennial Review surfaced in a hearing in front of Congress, and the FCC was now unable to put the genie back in the bottle concerning the consolidation of the radio industry which had occurred between 1998-2005; the FCC acted to conclude its 2006 Quadrennial Review in late 2007, and it proposed modest rule alterations.[134] The FCC proposed revising only one ownership rule, a partial repeal of the 1975 prohibition on newspaper-broadcast cross-ownership, but only in the top 20 media markets.[135] Although minority ownership represented an insignificant aspect of the FCC's stated diversity assessments since the implementation of the Telecommunications Act,[136] the FCC also released a new minority ownership policy developed in a parallel proceeding to the 2006 Quadrennial Review in response to the remand on the issue in *Prometheus I*.[137]

In the December 2007 proposal, the FCC adopted Small Business Administration financial standards based on gross sales revenue for a radio or television company creating a class of license applicants called "Eligible

130. *See* App'ns of AT&T Wireless Servs., Inc. & Cingular Wireless Corp., *Memorandum Opinion and Order*, 19 FCC Rcd 21522 (2004); *see, e.g.*, App'ns for Consent to the Assignment of Licenses Pursuant to Section 310(d) of the Comm. Act from NextWave Personal Comm., Inc., *Memorandum Opinion and Order*, 19 FCC Rcd 2570 para. 1 (2004).

131. Neda Ulaby, *Kevin Martin's Contentious Turn at Helm of FCC,* NPR (Feb. 5, 2009), https://www.npr.org/templates/story/story.php?storyId=18711487 [https://perma.cc/47MX-SCMH].

132. 2006 Quadrennial Regul. Rev. – Rev. of the Comm'n's Broad. Ownership Rules and Other Rules Adopted Pursuant to Section 202 of the Telecomms. Act of 1996, *Further Notice of Proposed Rulemaking*, 21 FCC Rcd 8834, paras. 1, 7-8 n.10 (2006) [hereinafter *2006 Further Notice of Proposed Rulemaking*].

133. *See id.*

134. Press Release, Mary Diamond, Chairman Kevin J. Martin Proposes Revision to the Newspaper/Broadcast Cross-Ownership Rule 2 (Nov. 13, 2007), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-278113A1.pdf [https://perma.cc/3PEX-582T]; *see also* 2006 Quadrennial Regul. Rev.– Rev. of the Comm'n's Broad. Ownership Rules and other Rules Adopted Pursuant to Section 202 of the Telecomms. Act of 1996, *Report and Order on Reconsideration*, 23 FCC Rcd 2010, para. 13 (2007).

135. *Id.*

136. Prior to the Eligible Entity proposal, the FCC had not put forward a direct minority ownership proposal since the decision in *Metro.*

137. Promoting Diversification of Ownership in the Broad. Servs., *Report and Order and Third Further Notice of Proposed Rule Making*, 23 FCC Rcd 5922, para. 3 (2008) [hereinafter *2007 Minority Ownership Order*].

Entities."[138] The Eligible Entity policy was implemented as part of a larger FCC effort to increase the number of small independent owners of media properties, but did not provide any mechanism to directly promote ownership by women or minorities.[139] Relying instead on the central premise of the FCC's belief in a relationship between ownership and content diversity,[140] the Commission argued that increasing the number of small media owners (owners who operate either a single or small group of stations), would result in an increase in the diversity of programming content, including programming content targeted at minorities.[141]

Despite the agency's stated goal of diversity enhancement, FCC Commissioner Adelstein argued that after *Adarand,* the type of minority enhancements at issue in *Metro* must now be subjected to strict scrutiny.[142] Therefore, for a new minority ownership policy to bypass any constitutional barriers, the policy must be implemented as "race neutral."[143] Rather than providing ownership enhancements to minorities directly, as the policies at issue in *Metro* had done, the FCC argued that the policy could (eventually) include women and minorities as Eligible Entities.[144] In crafting the new policy, the FCC relied on the empirically unsupported contention at the cornerstone of media ownership theory, that internal and external competition between stations will increase diversity.[145] As such, the Eligible Entity policy was promoted as a mechanism that could increase the number of independently owned media outlets. The FCC claims that independently owned outlets are more likely to have ties to a local community, and, by extension, are better able to meet the needs of the local audience.[146]

---

138. *Id.* para. 6 ("The eligible entity must hold: (1) 30 percent or more of the stock/partnership shares and more than 50 percent voting power of the corporation or partnership that will hold the broadcast license; or (2) 15 percent or more of the stock/ partnership shares and more than 50 percent voting power of the corporation or partnership that will hold the broadcast licenses, provided that no other person or entity owns or controls more than 25 percent of the or (3) more than 50 percent of the voting power of the corporation if the corporation that holds the broadcast licenses is a publicly traded company.").

139. *Id.*

140. *See 2002 Ownership Rules*, *supra* note 34, at para. 8.

141. *See 2007 Minority Ownership Order*, *supra* note 137, at para. 41.

142. *Id.* at paras. 5-6.

143. The FCC believed that by implementing the new policy on a race-neutral basis, and avoiding constitutional scrutiny on equal protection grounds, the policy can be implemented, and have demonstrable results much quicker. *Id.* at para. 9.

144. The Commission was seeking comment on whether a special category of "eligible entity" should be created to assist minorities and women with the acquisition of media outlets, but for now the diversity policy will remain race and gender neutral. *Id.* at para. 39.

145. The FCC believes that competition that creates diversity does not always come from external competitors. As more local stations are commonly owned, there is also an incentive for diverse programming to reduce "internal competition." This premise does not account for an economic reality that media companies will target the most valuable audience demographics even if forced to compete for that audience, a process known as rivalrous imitation. *Id.* at para. 17; *see* John Dimmick & Daniel G. McDonald, *Network Radio Oligopoly 1926-1956*: *Rivalrous Imitation and Program Diversity*, 14 J. MEDIA ECON. 197, 201 (2001).

146. *See 2007 Minority Ownership Order*, *supra* note 137, at para. 7.

The Eligible Entity designation was adopted from a previous FCC definition of a station (or stations) with minority ownership.[147] The FCC had previously defined minority ownership of a broadcast outlet as a situation in which the ownership reports identify one or more minorities which, in aggregate, have a greater than 50% voting interest in the broadcast licensee entity.[148] To become an Eligible Entity, an applicant had to meet SBA standards as defined by total annual sales of an organization or its parent company. For radio, the qualifying limit was $6.5 million and for television it was $13 million.[149] In addition, an Eligible Entity must hold:

> 30 percent or more of the stock/partnership shares and more than 50 percent voting power of the corporation or partnership that will hold the broadcast license; or (2) 15 percent or more of the stock/partnership shares and more than 50 percent voting power of the corporation or partnership that will hold the broadcast licenses, provided that no other person or entity owns or controls more than 25 percent of the outstanding stock or partnership interests; or (3) more than 50 percent of the voting power of the corporation if the corporation that holds the broadcast licenses is a publicly traded company.[150]

A legal battle over jurisdiction delayed the judicial review of the FCC's 2006 and 2007 proposals.[151] The Third Circuit claimed that it retained jurisdiction over the FCC's response to the remand issued in *Prometheus I*, while both the FCC and members of the deregulatory petitioner group attempted to move the review to the D.C. Circuit.[152] The petitions failed, and oral arguments occurred in front of the Third Circuit panel on February 11, 2011, ultimately resulting in another significant legal setback for the FCC in a decision released in July.[153] Judge Ambro's opinion included another remand which undermined the FCC's 2007 decisions on media ownership, citing the agency's continuing series of procedural and evidentiary problems.[154] The majority also incorporated the FCC's Eligible Entry program when examining the largely unresolved remand of the minority

147. *Id.* at para. 6.

148. *Id.*

149. *Id.*

150. *See id.*

151. 2006 Quadrennial Regul. Rev., *Consolidation Order*, 73 Fed. Reg. 9481, 1-2 (2008).

152. Order at 1-2, Media All. v. FCC, No. 6695769 (9th Cir. Nov. 4, 2008), ECF No. 43; *see* Final Brief of Petitioners Tribune Co. & Fox Television Stations, Inc. at *14 n.8, Prometheus Radio Project v. FCC, 2010 WL 1133326 (3d Cir. Mar. 23, 2010) (No. 08-3078), 2010 WL 3866781.

153. Petition for Review at 1-2, Prometheus Radio Project v. FCC, No. 003147340 (3d Cir. Feb. 26, 2008).

154. *Prometheus II, supra* note 2, at 437 (3d Cir. 2011) ("[T]he [FCC] failed to meet the notice and comment requirements of the Administrative Procedure Act. We also remand those provisions of the Diversity Order that rely on the revenue-based 'eligible entity' definition, and the FCC's decision to defer consideration of other proposed definitions (such as for a socially and economically disadvantaged business, so that it may adequately justify or modify its approach to advancing broadcast ownership by minorities and women.").

ownership issue in *Prometheus I*.[155] Suggesting that the agency had "in large part punted" on the minority ownership issue,[156] the second *Prometheus* decision provided a clearly stated mandate to the FCC: address the issue of minority ownership policy before the completion of the agency's already in-progress 2010 Quadrennial Review.[157]

> The eligible entity definition adopted in the Diversity Order lacks a sufficient analytical connection to the primary issue that Order intended to address. The [FCC] has offered no data attempting to show a connection between the definition chosen and the goal of the measures adopted—increasing ownership of minorities and women. As such, the eligible entity definition adopted is arbitrary and capricious, and we remand those portions of the Diversity Order that rely on it. We conclude once more that the FCC did not provide a sufficiently reasoned basis for deferring consideration of the proposed SDB definitions and remand for it to do so before it completes its 2010 Quadrennial Review.[158]

The ruling also signaled that the FCC had strained the majority's patience with another failure to develop a rational minority ownership policy. The panel suggested that the FCC should stop stalling, and instructed the agency to resolve the minority ownership issue, regardless of the challenges presented by the precedent from the *Adarand* decision.[159]

---

155. The Third Circuit overturned the FCC's 2003 Order in *Prometheus I*. *See Prometheus I*, *supra* note 2, at 435.

156. "Despite our prior remand requiring the [FCC] to consider the effect of its rules on minority and female ownership, and anticipating a workable SDB definition well before this rulemaking was completed, the [FCC] has in large part punted yet again on this important issue. While the measures adopted that take a strong stance against discrimination are no doubt positive, the [FCC] has not shown that they will enhance significantly minority and female ownership, which was a stated goal of this rulemaking proceeding. This is troubling, as the [FCC] relied on the Diversity Order to justify side-stepping, for the most part, that goal in its 2008 Order." *Prometheus II*, *supra* note 2, at 471-72.

157. *Id.*

158. *Id.*

159. *Id.* at 483.

> Stating that the task is difficult in light of *Adarand* does not constitute considering proposals using an SDB definition. The FCC's own failure to collect or analyze data, and lay other necessary groundwork, may help to explain, but does not excuse, its failure to consider the proposals presented over many years. If the [FCC] requires more and better data to complete the necessary *Adarand* studies, it must get the data and conduct up-to-date studies, as it began to do in 2000 before largely abandoning the endeavor.[160]

In the wake of *Prometheus II*, the FCC nominally continued to conduct the ongoing 2010 Quadrennial Review required under section 202(h).[161] However, the FCC's 2010 Quadrennial Review process quickly became bogged down as it was expanded to incorporate the Third Circuit's directive on minority ownership.[162] The FCC's efforts to conclude the review process or to propose a new minority ownership policy were essentially non-existent.[163] Eventually, the agency was able to run out the clock on the 2010 Quadrennial Review without making another decision.[164] Instead, the FCC incorporated the uncompleted 2010 review process—the agency's response to the remands issued by the Third Circuit in both 2004 and 2011—into the launch of the 2014 Quadrennial Review.[165] But even after the restart, the agency's public commitment to the new proceeding was minimalist (at best), and after a period of apparent inaction by the agency, collectively the deregulatory petitioners, the citizen petitioners, and the FCC returned to the Third Circuit for *Prometheus III* in April 2016.[166] During a hostile oral argument, the judges on the panel pressed the FCC for a straight answer as to when the agency would conclude the open proceedings by taking some type of formal action.[167] Although the FCC was reluctant to commit to a timeline for final agency action, agency lawyers told the court that a draft of new rules would be circulated among FCC commissioners before the end of June 2016.[168]

In response, the Third Circuit panel in *Prometheus III* supported the action promised by agency counsel to conclude the 2010 and 2014

---

160. *Id.* at 484, n.42.

161. *See* 2014 Quadrennial Reg. Rev.– Rev. of the Comm'n's Broad. Ownership Rules and Other Rules Adopted Pursuant to Section 202 of the Telecomms. Act of 1996, *Further Notice of Proposed Rulemaking and Report and Order*, 29 FCC Rcd. 4371, para. 1 (2014) [hereinafter *2014 Further Notice of Proposed Rulemaking and Report and Order*].

162. Christopher Terry, Stephen Schmitz & Eliezer (Lee) Joseph Silberberg, *The Score is 4-0: FCC Media Ownership Policy, Prometheus Radio Project, and Judicial Review*, 73 FED. COMM. L. J. 99, 128 (2021).

163. *Prometheus II*, *supra* note 2, at 465.

164. *See 2014 Further Notice of Proposed Rulemaking and Report and* Order, *supra* note 161, para. 74 in which the FCC explains it disagreed with the Third Circuit's holdings that the agency's rulemaking procedures and outcomes on media ownership were insufficient.

165. *See 2014 Further Notice of Proposed Rulemaking and Report and Order*, *supra* note 161, paras. 1, 7.

166. *Prometheus III*, *supra* note 2, at 37.

167. *See id.* at 51.

168. *See id.* at 53-54.

proceedings and reminded the FCC they were under obligation to deliver a new minority ownership policy.[169] The court argued that the FCC's ongoing delays "keeps five broadcast ownership rules in limbo."[170] The court also observed that the FCC's delay "hamper[ed] judicial review because there is no final agency action to challenge."[171] The FCC's ongoing failure to develop a policy to increase the ownership of stations by women and minorities had also clearly tested the Third Circuit's patience.

> The FCC presents two arguments for why we should not order relief. Both fail. The first is that it is not yet in violation of *Prometheus II* because we instructed it to address the eligible entity definition during the 2010 Quadrennial Review, which is still ongoing. This contention improperly attempts to use one delay (the Quadrennial Review) to excuse another (the eligible entity definition). By this logic, the [FCC] could delay another decade or more without running afoul of our remand. Simply put, it cannot evade our remand merely by keeping the 2010 review open indefinitely.[172]

In response, in August 2016, the FCC released an Order that concluded the open 2010 and 2014 Quadrennial Reviews while serving as the agency's formal response to the *Prometheus III* and *Prometheus II* remands.[173] Most notably, after more than six years without a decision, the FCC decided to do nothing.[174] The agency proposed maintaining all of the existing media ownership rules without any revisions or adjustments.[175] "We affirm our tentative conclusion that the current rule remains consistent with the Commission's goal to promote minority and female ownership of broadcast radio stations."[176] Additionally, the FCC's August 2016 order ignored the directions of the decision in *Prometheus II* and the decision in *Prometheus III* to develop a rational minority ownership policy. Instead, the FCC attempted to recycle the Eligible Entity program proposed in 2007.

---

169. *See id.* at 53-54, 60.
170. *Id.* at 51.
171. *Id.* at 40.
172. *Id.* at 48-49.
173. *2017 Ownership NPRM*, *supra* note 30, at para. 15. *See also 2016 Second Report and Order*, *supra* note 12, at paras. 2-4.
174. *2017 Ownership NPRM*, *supra* note 30, at para. 15.
175. *Id.*
176. *Id.* at para. 125.

> [W]e disagree with arguments that the *Prometheus II* decision requires that we adopt a race- or gender-conscious eligible entity standard in this quadrennial review proceeding or that we continue this proceeding until the [FCC] has completed whatever studies or analyses that will enable it to take race- or gender-conscious action in the future consistent with current standards of constitutional law.[177]

Unsurprisingly, a host of legal challenges to the FCC's non-action quickly followed. But before those challenges reached oral argument, the 2016 presidential election changed the FCC's leadership structure.[178] Under the new leadership of Ajit Pai, in November of 2017, the FCC released a new media ownership policy as an Order on Reconsideration.[179] The Order on Reconsideration, unlike the Second Report and Order from August 2016, did not address the Third Circuit's mandate to develop a viable minority ownership policy.[180]

While consolidated cases challenging the original 2016 Order and 2017 Order on Reconsideration were pending in *Prometheus IV*, the FCC released its initial proposal for a new minority ownership policy, called the "Incubator" program.[181] The Incubator program provided for additional ownership consolidation, including opportunities to exceed the limits set by Congress in the Telecommunications Act for companies that would be willing to "incubate" a startup through assistance for new entrant radio broadcasters.[182] Under the Incubator program, existing operators would provide a range of financial, operational, and technical guidance to new entities and in return, would be granted a waiver of the existing ownership limits which could be applied to station acquisitions in other media markets.[183] The Incubator program was released in August 2018 just ahead of the Third Circuit's order to the FCC to respond to the challenges to the 2016 and 2017 decisions.[184]

---

177. *Id.* at para. 313.

178. *See* Jim Puzzanghera, *Trump Names New FCC Chairman*, L.A. TIMES (Jan. 23, 2017) https://www.latimes.com/business/la-fi-pai-fcc-chairman-20170123-story.html.

179. *2017 Ownership NPRM*, *supra* note 30.

180. *See id.* at para. 7 (noting the Prometheus Radio Project line of cases involve, "various diversity-related decisions, certain media ownership rules and the decision not to attribute SSAs" without mentioning the majority's remand on a functional minority ownership rule).

181. *See id.* at para. 126.

182. *See id.* at para 121.

183. *See id.* at paras. 121-45.

184. Rules & Pol'ys to Promote New Entry & Ownership Diversity in the Broad. Servs., *Report and Order*, 33 FCC Rcd 7911 (2018).

> The program we implement today will apply in the radio market, as radio has traditionally been the more accessible entry point for new entrants and small businesses seeking to enter the broadcasting industry, and a waiver of the local radio rules provides an appropriate reward for incubation. Owning and operating a radio station requires a lower capital investment and less technical expertise than owning and operating a television station, and it also requires less overhead to operate. In addition, we believe that the [FCC]'s existing ownership limitations on local radio markets provide a sufficient incentive for incumbent broadcasters to participate in an incubator program with the promise of obtaining a waiver to acquire an additional station in a market.[185]

To be eligible to participate in the "Incubator" program, an entity was required to meet two criteria. First, eligibility was tied to an update of the FCC's entrant bidding credit standard.[186] To meet this new standard, the incubating entity could not own or have an attributable interest in more than three full-service AM or FM radio stations, and it could not have any attributable interest in any broadcast television stations.[187]

The second requirement for an "Incubator" designation required the entity to meet the criteria for the FCC's 2007 and 2016 Eligible Entity proposals, despite the Third Circuit's explicit remand of that designation in *Prometheus II*.[188] Notably, both the FCC's August 2016 Second Report and Order[189] and the November 2017 proposal for the "Incubator" program[190] used the exact same language and criteria first proposed by the FCC in 2007.[191]

Beyond the potential issue in recycling the already remanded Eligible Entity designation, the FCC's new "Incubator" proposal included two significant and potentially fatal omissions.[192] The FCC made no allocation of additional spectrum for more radio stations, nor did the agency mandate license transfers.[193] As a result, the Incubator program would require that existing radio stations be "donated" from their current owners.[194] Second, and perhaps more importantly, the FCC's Incubator proposal did not resolve the central dilemma of minority ownership policy: the need to explain how the

185. *Id.* at para. 7.
186. *See Prometheus IV*, *supra* note 2, at 576.
187. *Id.*
188. *Prometheus III*, *supra* note 2, at 454.
189. *2016 Second Report and Order*, *supra* note 12.
190. *2017 Ownership NPRM*, *supra* note 30, at para. 121.
191. *2007 Minority Ownership Order*, *supra* note 137, at para. 68.
192. *See 2017 Ownership NPRM*, *supra* note 30, at paras. 121-45.
193. *See id.*
194. *See id.*

agency would ensure new start-ups end up in the hands of underrepresented groups like minorities and women.[195]

A consolidated challenge to all of the 2016, 2017, and 2018 Orders on media ownership returned to the Third Circuit for oral arguments in June of 2019. During oral arguments, the panel again appeared skeptical of the FCC's decision making. One of the attorneys representing a group of the deregulatory petitioners even used her available time to argue for limiting the scope of a potential remand rather than supporting the FCC's proposals.[196] In late September of 2019, the Third Circuit handed down the fourth *Prometheus* decision. In another 2-1 decision penned by Judge Ambro, the panel undermined the FCC's regulatory decisions on media ownership for the entire period between 2011 to 2019 including the 2016 Report and Order, the 2017 Order on Reconsideration, and the 2018 Incubator program.[197]

> Here we are again. After our last encounter with the periodic review by the [FCC] of its broadcast ownership rules and diversity initiatives, the [FCC] has taken a series of actions that, cumulatively, have substantially changed its approach to regulation of broadcast media ownership. First, it issued an order that retained almost all of its existing rules in their current form, effectively abandoning its long-running efforts to change those rules going back to the first round of this litigation. Then it changed course, granting petitions for rehearing and repealing or otherwise scaling back most of those same rules. It also created a new "incubator" program designed to help new entrants into the broadcast industry. The [FCC], in short, has been busy.[198]

The majority ruled the FCC had still failed to resolve the two core issues it had remanded to the agency in the previous cases: the need to provide empirical evidence to support a rational policy decision and propose a policy that would increase ownership by women and minorities.

---

195. The SDB standard is based on the definition employed by the SBA. To qualify for this program, a small business must be at least 51% owned and controlled by a socially and economically disadvantaged individual or individuals. *See Small Disadvantaged Businesses*, U.S. SMALL BUS. ADMIN., https://www.sba.gov/contracting/government-contracting-programs/small-disadvantaged-businesses [https://perma.cc/65CY-KCSZ].

196. Oral Argument at 16:45, 37:19, 1:05:25, *Prometheus IV*, *supra* note 2 (Nos. 17-1107 17-1109 17-1110, 17-1111 18-1092 18-1669 18-1670 18-1671 18-2943 & 18-3335) https://www2.ca3.uscourts.gov/oralargument/audio/17-1107PrometheusRadioProjectv.FCC,etal.mp3.

197. *See Prometheus IV*, *supra* note 2, at 589 ("We do conclude… that the [FCC] has not shown yet that it adequately considered the effect its actions since *Prometheus III* will have on diversity in broadcast media ownership. We therefore vacate and remand the Reconsideration and Incubator Orders in their entirety, as well as the 'eligible entity' definition from the 2016 Report & Order").

198. *See id.* at 572-73.

> We do . . . agree with the last group of petitioners, who argue that the [FCC] did not adequately consider the effect its sweeping rule changes will have on ownership of broadcast media by women and racial minorities. Although it did ostensibly comply with our prior requirement to consider this issue on remand, its analysis is so insubstantial that we cannot say it provides a reliable foundation for the [FCC's] conclusions. Accordingly, we vacate and remand the bulk of its actions in this area over the last three years.[199]

Judge Ambro's decisions argued that by any rational analysis, the FCC's effort to support its choices was inadequate.[200] The majority suggested the FCC's decisions would not stand even if they were provided a more deferential review.[201] Most importantly, the decision in *Prometheus IV* suggests that the FCC had failed to even attempt to argue that it followed the Third Circuit's previous instructions.[202] Judge Ambro's decision vacated and remanded the 2017 Reconsideration Order and the incubator program to the FCC. It also vacated and remanded the definition of "eligible entities" in the 2016 Report and Order[203] while retaining jurisdiction over the remanded issues and all other petitions for review.[204]

---

199. *See id.* at 573.

200. *See id.*

201. *See id.* at 584.

202. *Id.* at 585 ("Problems abound with the FCC's analysis. Most glaring is that, although we instructed it to consider the effect of any rule changes on female as well as minority ownership, the [FCC] cited no evidence whatsoever regarding gender diversity. It does not contest this.").

203. *Id.* at 587-88.

204. *Id.* ("Accordingly, we vacate the Reconsideration Order and the Incubator Order in their entirety, as well as the 'eligible entity' definition from the 2016 Report & Order. On remand the [FCC] must ascertain on record evidence the likely effect of any rule changes it proposes and whatever 'eligible entity' definition it adopts on ownership by women and minorities, whether through new empirical research or an in-depth theoretical analysis. If it finds that a proposed rule change would likely have an adverse effect on ownership diversity but nonetheless believes that rule in the public interest all things considered, it must say so and explain its reasoning. If it finds that its proposed definition for eligible entities will not meaningfully advance ownership diversity, it must explain why it could not adopt an alternate definition that would do so. Once again we do not prejudge the outcome of any of this, but the [FCC] must provide a substantial basis and justification for its actions whatever it ultimately decides.").

> The only "consideration" the FCC gave to the question of how its rules would affect female ownership was the conclusion there would be no effect. That was not sufficient, and this alone is enough to justify remand. . . Even just focusing on the evidence with regard to ownership by racial minorities, however, the FCC's analysis is so insubstantial that it would receive a failing grade in any introductory statistics class.[205]

The FCC and the National Association of Broadcasters (NAB) each requested a rehearing and en banc review on November 7, 2019.[206] Less than two weeks later, on November 20, 2019, Judge Ambro authored another decision denying a review by the full panel.[207] On November 29, 2019, the panel issued a mandate formally implementing the remand.[208] On December 20, 2019, the FCC's Media Bureau responded to the mandate with an order which concluded the 2014 Quadrennial Review, the 2010 Quadrennial Review, and the Incubator Program.[209] The Media Bureau's Order re-implemented the long-standing newspaper-broadcast cross-ownership ban, radio-television cross-ownership rule, local television ownership rule, local radio ownership rule, and television joint sales agreement (JSA) attribution rules.[210] The FCC marked the 2017 Order on Reconsideration and the incubator program as repealed.[211] Finally, the 2016 Order's reinstatement of the eligible entity designation was also repealed in line with the Third Circuit's remand in *Prometheus IV*,[212] functionally leaving most media ownership rules where they have been since the decision in *Prometheus I* in 2004, and arguably since the implementation of the Telecommunications Act of 1996.

After parallel requests for review were filed by the FCC and the industry petitioners, the Supreme Court granted certiorari and heard oral arguments on the last day of Ajit Pai's chairmanship of the agency, January 19, 2021. At oral arguments, there were functionally three sides: the agency,

---

205. *Id.* at 585-86.

206. Petition of FCC and United States of America for Rehearing en banc at 7-8, Prometheus Radio Project v. FCC, Nos. 17-1107 17-1109 17-1110, 17-1111 18-1092 18-1669 18-1670 18-1671 18-2943 & 18-3335 (3d Cir. Nov. 7, 2019); Petition for Rehearing of Industry Intervenors in Support of Respondents, Prometheus Radio Project v. FCC, No. 003113399507 (3d Cir. Nov. 7, 2019).

207. Opinion of the Court, Prometheus Radio Project v. FCC, No. 03113354897 (3d Cir. Sept. 23, 2019).

208. Amended Judgment, Prometheus Radio Project v. FCC, No. 003113419677 (3d Cir. Nov. 29, 2019).

209. 2010 Quadrennial Reg. Rev.– Rev. of the Comm'n's Broad. Ownership Rules and Other Rules Adopted Pursuant to Section 202 of the Telecomms. Act of 1996, *Notice of Inquiry*, 25 FCC Rcd 6086 (2010); *2007 Minority Ownership Order*, *supra* note 137; Rules and Policies Concerning Attribution of Joint Sales Agreements In Local TV Markets, *Order*, 19 FCC Rcd 18166 (2004); Rules and Policies To Promote New Entry and Ownership Diversity in the Broadcasting Services, 83 Fed. Reg. 43.773, 43,774 (Aug. 28, 2018).

210. *See id.*

211. *See id.*

212. *Id.*

the industry petitioners led by the NAB, and the citizen petitioners, functionally led by Prometheus.[213]

The FCC argued for relief from the long process and from lengthy obligations from the standing remands from the Third Circuit.[214] The industry petitioners made a more direct argument, proposing that the Third Circuit had replaced its own judgement for that of the agency.[215] The citizen petitioner group built its case primarily on the premise that the agency's lack of evidence was a long standing procedural problem.[216] Of the three sides, the arguments for and against the inclusion of minority ownership only played a significant role in the industry petitioner arguments that minority ownership concerns were not part of the statutory mandates of section 202(h).[217]

A unanimous Court released a narrow opinion written by Justice Kavanaugh, stating that perfect empirical or statistical data to support an agency's decision making is unusual in the first place. Justice Kavanaugh's opinion argued that the record, or rather the sparse record on minority and female ownership, meant that the FCC's inability to meet the Third Circuit's remands on the issue did not fall outside the zone of reasonableness for the purposes of the APA.[218]

Pointing out that the FCC had attempted to explore the impacts on minority and female ownership, even seeking public comment on it during multiple section 202(h) review processes, Justice Kavanaugh supported the agency's 2017 conclusion that changes to the rules were not likely to harm minority or female ownership.[219] Going further, the decision argues that the Prometheus Challenge to the FCC's 2017 Reconsideration Order targeted the FCC's assessment that altering the ownership rules was not likely to harm minority and female ownership rather than dispute the FCC's conclusion that the existing rules no longer serve the agency's public interest goals of competition, localism, and viewpoint diversity.[220]

Importantly, the court did not resolve an important, and lingering dispute throughout the process: what elements must be included in the review processes mandated by section 202(h). The decision's narrow holding that Third Circuit's judgment should be reversed was only completed by applying ordinary principles of arbitrary and capricious review. Although the agency, the industry petitioners, and the Prometheus-led citizen petitioner group each sought guidance on this unresolved issue from the Third Circuit's remands, in footnote 3, the decision stated:

213. FCC v. Prometheus Radio Project, 141 S. Ct. 1150, 1160 n.3 (2021).
214. *Id.* at 1154.
215. *Id.* at 1155.
216. *Id.*
217. *Id.* at 1156.
218. *Id.* at 1160.
219. *Id.* at 1157.
220. *Id.* at 1160.

> We need not reach the industry petitioners' alternative argument that the text of [s]ection 202(h) does not authorize (or at least does not require) the FCC to consider minority and female ownership when the Commission conducts its quadrennial reviews. We also need not consider the industry petitioners' related argument that the FCC, in its [s]ection 202(h) review of an ownership rule, may not consider minority and female ownership unless promoting minority and female ownership was part of the FCC's original basis for that ownership rule.[221]

In his concurring opinion, Justice Thomas argued that the FCC has never used its ownership rules to foster ownership diversity.[222] While Justice Thomas's opinion uses some selective quotes to support his contention, the FCC has built media ownership around a joint policy implementation on a relationship and diversity as far back as 1975.[223]

Justice Thomas also suggests that the FCC has been focused on consumers rather than on producers since the creation of the agency.[224] While this was formerly true, the FCC expressly changed focus during the Mark Fowler-led deregulation era in the 1980s, who has argued in multiple cases that benefits to the ownership of stations, like economy of scale, will in turn lead to benefits for the consumer or listener. Justice Thomas's opinion borrows from an FCC opinion arguing that the agency has clearly stated "it would be inappropriate to retain multiple ownership regulations for the sole purpose of promoting minority ownership" before concluding with advice that the agency was not under further obligation to consider ownership by women or minorities in future reviews.[225]

Taken as a whole, the decision in *FCC v. Prometheus Radio Project* doesn't address or resolve the minority ownership issue. Instead, Justice Kavanaugh argues that that the 2017 decision to remove cross ownership rules was not arbitrary or capricious, and moving forward, the agency can employ its own judgement in future reviews mandated by section 202(h).[226] The decision does not resolve the standing issue concerning how women and people of color continue to be underrepresented and in control of just a small fraction of broadcast outlets. Both Justice Kavanaugh and Justice Thomas failed to recognize that it is impossible to achieve viewpoint diversity and serve the public if the longstanding imbalance in ownership persists.

There is also the reality that by taking a narrow approach, and focusing only on the FCC's 2017 action, the decision leaves the FCC in a bit of a time crunch. Under section 202(h), the agency must complete an ownership review originally launched in 2018 during the calendar year of 2021 ahead of

---

221. *Id.* at 1160 n.3.

222. *Id.* at 1162.

223. Multiple Ownership of Standard, FM, and TV Broad. Stations, *Second Report and Order*, 50 F.C.C. 2d 1046, 1074 (1975), *reconsidered* 53 FCC 2d 589 (1975), *aff'd sub nom.* FCC v. Nat'l Citizens Comm. for Broad., 436 U.S. 775 (1978).

224. FCC v. Prometheus Radio Project, 141 S. Ct. 1123, 1162-63 (2021).

225. *Id.* at 1163.

226. *Id.* at 1159.

beginning a new review process scheduled and required for 2022. If the FCC continues to focus on the public interest goals through competition, localism, and viewpoint diversity, more data will be needed to demonstrate the link between ownership and diversity of content, and to provide the agency a structural model for moving forward.

VI. MINORITY OWNERSHIP AND THE DIVERSITY "NEXUS": WHAT DOES THE EMPIRICAL RESEARCH SAY?

At least part of the FCC's struggle to resolve minority ownership policy can be explained simply: like much of the FCC's flawed approach to media ownership regulation since the late 1980s, quality empirical evidence to support a minority ownership policy has been in short supply.[227] Researchers using the FCC's ownership data have suggested that the FCC's data on minority and female ownership "is extremely crude and subject to a large enough degree of measurement error to render it essentially useless for any serious analysis."[228]

Although the NTIA was heavily involved in assessing minority ownership after the implementation of the Telecommunications Act, the data produced was focused entirely on racial designations and did not include assessments of ownership by women.[229] The first assessment of ownership that included gender was a study included by the FCC in its 2006 Media Ownership Rulemaking Inquiry. The research explored the quantity of minority and female ownership of traditional media outlets (broadcast radio and television, as well as newspapers).[230] Relying on the FCC's own ownership data for the years between 2002 and 2005, minorities, as a group, never reach 4% combined ownership of broadcast television and radio stations.[231] The authors concluded that minorities and females were both "clearly underrepresented," in comparison to their populations.[232]

By any measure, minority ownership has long represented a small percentage of the overall ownership of broadcast stations across the United States, and, problematically, the changes in ownership structures which followed implementation of the 1996 Telecommunications Act compounded

---

227. Adam Candeub, *Media Ownership Regulation, the First Amendment, and Democracy's Future*, 41 U.C. DAVIS L. REV. 1547, 1600 (2008).

228. ARIE BERESTEANU & PAUL B. ELLICKSON, MINORITY AND FEMALE OWNERSHIP IN MEDIA ENTERPRISES 2 (2007).

229. *See* NAT'L TELECOMMS. & INFO. ADMIN, U.S. DEP'T OF COM., CHANGES, CHALLENGES, AND CHARTING NEW COURSES: MINORITY COMMERCIAL BROADCAST OWNERSHIP IN THE UNITED STATES 36-46, 50, 54, 56-57 (2000), https://www.ntia.doc.gov/files/ntia/publications/mtdpreportv2.pdf [https://perma.cc/ES6L-ZWE6].

230. BERESTEANU & ELLICKSON, *supra* note 228, at 2.

231. The FCC relies on self-reported data for ownership assessments, collected on a biannual basis using forms 323 and 323E. *See generally* Promoting Diversification of Ownership in the Broad. Servs., *Report and Order, Second Report and Order, and Order on Reconsideration*, 31 FCC Rcd 398, paras. 47-50 (2016).

232. BERESTEANU & ELLICKSON, *supra* note 228, at 2.

an existing market regulation failure.[233] Ownership data collected by communication policy scholars in 2003 painted a much bleaker picture of minority ownership after the first major round of ownership mergers.[234] Minority ownership of radio stations was reported to make up 335 of the 13,499 (2.48%) radio stations on the air.[235] Of the 1,748 commercial and educational television stations on the air, only 15 claimed to be owned by racial minorities (0.8%).[236] The FCC compiled similar data from ownership reports filed in 2004 and 2005. Of the 12,844 stations which filed FCC form 323 or 323-E,[237] only 460 broadcast stations (3.6%) met the Commission's defined criteria for minority ownership.[238]

A decade later, in 2013, the FCC's assessments of minority ownership also provided a grim evaluation of media ownership policy.[239] The data from the 2013 Form 323 filings indicated racial minorities collectively or individually held a majority of the voting interests in 41 (3%) of full power commercial television stations, 225 (6%) of commercial AM radio stations, and 169 (3%) commercial FM radio stations.[240] The FCC's 2013 data assessing ownership by gender was equally problematic. Women collectively or individually held a majority of the voting interests in just 87 (6.3%) of full power commercial television stations, 310 (8.3%) of commercial AM radio stations, and 383 (6.7%) commercial FM radio stations.[241]

The FCC's 2015 ownership report continued to demonstrate low levels of minority ownership.[242] Racial minorities collectively or individually held a majority of the voting interests in 402 broadcast stations, consisting of 36 full power commercial television stations (2.6%); 204 commercial AM radio stations (5.8%) and 128 commercial FM radio stations (2.3%).[243]

The FCC's 2017 data on minority ownership, released by the agency in 2020 but ahead of the Supreme Court's grant to hear the FCC and NAB challenges to *Prometheus IV*, continued to illustrate the ongoing problem.[244] Both women and minorities continued to be drastically underrepresented in

---

233. Increasingly, scholars are arguing that in place of a full regulation scheme, selective use of regulations should be used to fix outcome gaps. *See* VICTOR PICKARD, AMERICA'S BATTLE FOR MEDIA DEMOCRACY: THE TRIUMPH OF CORPORATE LIBERTARIANISM & THE FUTURE OF MEDIA REFORM 221-23 (2015).

234. *See* BERESTEANU & ELLICKSON, *supra* note 228, at 6-7.

235. *Id.*

236. *Id.*

237. FCC Form 323 Ownership Report for Commercial Broadcast Stations is an ownership report filed by stations every two years. FCC Form 323-E is filed by educational and noncommercial stations. Form 323-E does not collect information on Minority ownership. *See* 2017 323 REPORT, *supra* note 3.

238. FCC OWNERSHIP MINORITY REPORT FOR 2004-2005 179 (2006), https://www.fcc.gov/ownership/owner_minor_2004-2005.pdf [https://perma.cc/ER9Z-QU2K].

239. 2014 Quadrennial Reg. Rev. – Rev. of the Comm'n's Broad. Ownership Rules and Other Rules Adopted Pursuant to Section 202 of the Telecommns. Act of 1996, *Report on Ownership of Commercial Broadcast Stations*, 29 FCC Rcd 7835 (2014).

240. *Id.* at 7838.

241. *Id.* at 7837-38.

242. 2017 323 REPORT, *supra* note 3, at 3-5.

243. *Id.*

244. FOURTH REPORT ON OWNERSHIP, *supra* note 3, at 4-7.

terms of media control. Women held a majority of the voting interests in 73 of 1,368 full-power commercial television stations (5.3%); 19 of 330 Class A television stations (5.8%); 76 of 1,025 low-power television stations (7.4%); 316 of 3,407 commercial AM radio stations (9.3%); and 390 of 5,399 commercial FM radio stations (7.2%).[245] Racial minorities collectively or individually held a majority of the voting interests in only 26 of 1,368 full power commercial television stations (1.9%); 8 of 330 Class A television stations (2.4%); 21 of 1,025 low-power television stations (2.0%); 202 of 3,407 commercial AM radio stations (5.9%); and 159 of 5,399 commercial FM radio stations (2.9%), for a total of 416 of 11,529 (3.6%) of all commercial broadcast stations.

With the recognition that minority-focused or formatted content does not come from minority ownership alone, other assessments of minority access have examined broadcast station content directly. Todd Chambers explored the ownership and programming patterns of Spanish language radio stations in the 50 metropolitan areas with the highest populations of Hispanics.[246] Using industry definitions for Hispanic formats to identify stations in each individual market, Chambers concluded that just over 20% (314 of 1,545) of the stations in these markets carried a Spanish language format.[247]

The data also indicated that larger radio companies dominated the control of stations within these markets, with then Clear Channel Communications and Infinity controlling almost a third of all the stations in the markets at the time.[248] According to Chambers, HBC (50 of 61 stations) and Entravision (41 of 55 stations) were the radio ownership groups which provided the most service to Hispanic audiences.[249] The results indicated that large radio groups had not diversified their holdings to include stations carrying primarily minority-targeted content, as the FCC had theorized would occur as a result of internal competition between co-owned stations.[250] Instead, mid-size companies, also owned and operated by minorities, were the media organizations providing a large quantity of the minority content to audiences.[251]

Another study designed to assess the structures providing minority content used industry data to examine 1,532 of the commercial radio stations operating in the top fifty media markets.[252] Sixty-eight different owners were operating 225 stations with minority formats across 42 of the top 50 radio markets.[253] The majority of owners operating a minority formatted station in

245. *See id.* at 4-5.
246. Todd Chambers, *The State of Spanish-Language Radio,* 13 J. RADIO STUD. 34, 34 (2006).
247. *Id.* at 42.
248. *Id.* at 41-42.
249. *Id.*
250. *Id.* at 39.
251. *Id.*
252. Terry, *supra* note 37, at 32.
253 *Id.* at 24-27.

the top 50 markets were smaller media operations with 6 or fewer stations, and more than half of these operated only a single station.[254]

Collectively, content focused research supported the FCC's contention in 2007 that an increase in content diversity is more likely to come from smaller broadcast operations that have local ties to a community.[255] While data strongly suggested that the FCC's focus on smaller broadcasters as way to increase content diversity in the Eligible Entity program represented a sound premise, these findings were tied to the top 50 markets.[256] However, when combined with social science research that indicates that minorities are the group most likely to program formats targeted at specific minority groups,[257] a model ownership structure for the production of diverse content appears to be a small owner with a woman or minority as the lead interest in the operation.

The methods used to achieve more diversity have, at times, been arguably counterproductive.[258] The "Incubator" program launched by the FCC in August of 2018, offered already existing media outlets an opportunity to expand beyond the local ownership limits defined by the Telecommunications Act of 1996 in return for fostering start-up operations.[259] In practical terms, this means that FCC's most recent plan for minority ownership policy was based on an empirically unsupportable conceptual premise that more diversity will be created through additional ownership consolidation.[260]

VII. RETHINKING THE ROLE OF STRICT SCRUTINY

In considering the role of strict scrutiny, one must start with a simple premise: strict scrutiny of government action exists to protect liberties which merit special protections.[261] By placing government actions under review focused on the necessity of the action, potential harm is avoided. Strict scrutiny also serves as a check on the government's power by ensuring that the action taken is not over or under inclusive as it relates to the need.[262]

To be necessary under strict scrutiny, government action must address an actual problem that has not been dealt with and for which alternative, less restrictive, actions to resolve that problem do not exist.[263] Proper application of the strict scrutiny standard requires that the government's solution to the

---

254. *Id.* at 25-28.

255. *Id.*

256. *Id.*

257. *See* Laurie Mason, Christine M. Bachen & Stephanie L. Craft, *Support for FCC Minority Ownership Policy: How Broadcast Station Owner Race or Ethnicity Affects News and Public Affairs Programming Diversity*, 6 COMM. L. & POLY 37, 71 (2001).

258. *See* David Pritchard et al., *One Owner, One Voice? Testing a Central Premise of Newspaper/Broadcast Cross-Ownership Policy*, 13 COMM. L. & POL'Y 1 (2008).

259. *See* Terry, *supra* note 4, at 406.

260. *Id.* at 406, 429, 432.

261. Roy G. Spece, Jr. & David Yokum, *Scrutinizing Strict Scrutiny*, 40 VT. L. REV. 285, 294-95 (2015).

262. *Id.* at 291-294.

263. *Id.* at 299-301.

problem represents an important but also logical objective and that the action taken will achieve the objective.[264]

Although many of the agency's legal and policy setbacks can be tied directly to the FCC's overriding regulatory obsession with competition implemented through loosening structural regulation limits and providing mechanisms that incentivize repurposing content for use on more than one station, one cannot not simply ignore the roadblock installed by *Adarand* and the mandate for a strict scrutiny review. The preference programs upheld in *Metro* and then undermined by *Adarand*, were justified not only on the benefits of the program, but on the potential benefits additional viewpoint diversity offers at a societal level. Put another way, if a minority ownership policy must meet strict scrutiny's traditional compelling government interest standard, the assessment of the benefit should not be on the individuals that could obtain a station license, but rather on the citizens in the media market who will have access to additional diversity in their local programming options.[265]

In terms of the narrow tailoring requirement, any program that provides preferential treatment must eradicate a form of prior discrimination.[266] There can be few arguments that the policies upheld in *Metro* were designed to (partially) correct a prior discrimination, specifically, the discriminatory pattern of awarding of 90% of all broadcast licenses to white, male candidates.

In contemporary terms, there can be no question that the FCC's failure to address the four remands related to minority ownership from the *Prometheus* cases functionally extended the existing discrimination which resulted in underrepresentation. When historically marginalized groups are denied access to broadcast ownership, their viewpoints are not included in public discourse. In a democratic society, this is harmful.

VIII. A MODEST AND SIMPLE PROPOSAL

There is no need to bend the legal standards of review to fit this problem, and arguably the deference the FCC was provided by the Supreme Court's opinion in *FCC v. Prometheus Radio Project* makes this proposal even easier to implement. There is a substantial quantity of empirical support for the premise that increasing representation by minorities and women will produce an increase in diversity in programming options as well as viewpoints.[267] Likewise, there is also support for the premise that smaller, locally based broadcast ownership structures are most likely to succeed with

264. *Id.* at 306.

265. This suggestion represents the larger point of this article, that the benefits of increasing diversity of content by increasing the diversity of ownership, especially by increasing the number of racial and ethnic minorities and women who own stations, creates a societal benefit for all, not just the new owners. If the FCC desires to act to promote diversity, it must take the focus off the benefits to the owners and refocus on the larger benefits to the public.

266. Spece, Jr. & Yokum, *supra* note 261, at 318-332.

267. *See* Terry, *supra* note 37; Terry, *supra* note 4.

minority focused programming options.[268] The solutions are clear, the FCC just needs to choose to pursue them.

Developing a minority ownership policy to its logical conclusion is a straightforward exercise. The FCC must develop and implement a minority ownership policy that puts broadcast stations in the hands of (in-market) locally-based owners who are women and/or people of color. By focusing on just two aspects of the media ownership equation, localism and diversity, competition is likely to increase as new entrants are created. There is substantial empirical evidence available that would justify this approach, and unless the FCC intends to lose in court again, this path provides an answer ahead of the next round of media ownership rule review.[269]

Concerns about the costs to the individual in programs which provide preferences are not without merit, and the authors do not intend to make light of them. However, in the context of media ownership policy, any continuing policy stalemate benefits no one. Citizens go without important viewpoints and information sources while the media industry is trapped by the agency's failure to develop a functional minority ownership program.

The narrow decision in *FCC v. Prometheus* has not changed the underlying metrics or obstacles on media ownership policy. The agency has a pair of reviews to complete, and regardless of the outcomes of those reviews, the FCC's decisions in those proceedings is certain to be challenged in court. If heading that way anyway, the agency should choose a different approach.

268. Terry & Carlson, *supra* note 4, at 407-410.

269. *See Prometheus I*, *supra* note 2, at 435.

Leash the Big Dogs, Let the Small Dogs Roam Free: Preserve Section 230 for Smaller Platforms

Tyler Dillon*

TABLE OF CONTENTS

* I dedicate this Note to my partner, Natalie, whose love and support is my foundation. I would also like to thank the student editors and members of the Federal Communications Law Journal for their valuable advice and proofreading; their combined hundreds of hours of unpaid labor keep legal academia running.

I. INTRODUCTION

Section 230 helped create the modern Internet economy by protecting online platforms from legal liability if they were not able to perfectly moderate the actions of and content posted by their users.[1] Passed as part of the Communications Decency Act of 1996, section 230 provided incumbent and new "computer service[s]" the immunity necessary to create innovative new products in the growing Internet economy without the threat of prohibitive legal costs for the actions of their users.[2] Without identical adequate laws in other countries allowing small entrepreneurs such freedom to compete and experiment without uncertain legal costs looming over their heads, section 230 protections helped give rise to U.S. dominance in online services.[3] However, as social media platforms have garnered more power over public discourse, a movement has grown to limit the immunity that these platforms enjoy.[4] While the details of section 230 reform proposals vary and reform proponents span the political spectrum, their premises rely on curbing the power of social media platforms.[5]

Ironically, the broad application of section 230 reforms to all online platforms would likely consolidate even more influence over public discourse into the hands of a select few social media platforms by stifling competition through increased costs on small firms and new entrants.[6] Behemoths like Facebook with billions of dollars in revenue can withstand increased legal and compliance fees; their smaller competitors, however, likely would not be able to and will die, reduce services, or pivot away from social media.[7] Untargeted regulation will therefore help secure the power of large social media platforms by inhibiting their competitors.[8]

This Note argues that by targeting section 230 reforms only to certain companies, policy makers can still achieve their goals without destroying one of the legal foundations of the technology sector that has allowed the American digital economy to flourish. To accomplish these goals, any reforms to section 230 that increase liability for computer services should apply only to content published on (1) social media platforms with (2) more than 50 million monthly active users that (3) generate more than $500 million

---

1. *See* CHRISTIAN M. DIPPON, ECONOMIC VALUE OF INTERNET INTERMEDIARIES AND THE ROLE OF LIABILITY PROTECTIONS 1-3 (June 5, 2017), https://internetassociation.org/wp-content/uploads/2017/06/Economic-Value-of-Internet-Intermediaries-the-Role-of-Liability-Protections.pdf [https://perma.cc/8NE3-ECU3].
2. 47 U.S.C. § 230.
3. *See* JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET 148-50 (2019).
4. *See generally* Kiran Jeevanjee et al., *All the Ways Congress Wants to Change Section 230*, SLATE (Mar. 23, 2021), https://slate.com/technology/2021/03/section-230-reform-legislative-tracker.html [https://perma.cc/GP2W-7L9K]. .
5. *See infra* Part II, Section C.
6. *See infra* Part III, Section B, Part 3.
7. *See infra* Part III, Section B, Part 3.
8. Jeevanjee, *supra* note 4.

in revenue. By requiring all three criteria to be met, changes to liability law that could cost companies millions of dollars would be restricted to companies most able to withstand new legal expenses while still holding accountable platforms that are most responsible for the problems that legislators wish to solve.

Part II, Section A discusses the history of section 230 and how Congress sought to adapt liability law to the Internet Age. Section B discusses how to define social media platforms and measure their performance. Section C analyzes the costs and benefits of section 230 immunity, including how its protections helped shape the modern Internet economy, and proposals to address critiques. Part III, Section A argues that the overarching purpose of reform proposals is to limit the power that social media companies have on public discourse. Section B then discusses the benefits of exemptions to any changes to section 230 immunity and how limiting such restrictions to companies with more than $500 million in revenue that operate social media platforms with more than 50 million monthly active users can fulfill the purported purposes of legislation while reducing the negative consequences of regulation on small and new firms, as well as reducing unintended consequences.

II. BACKGROUND

A. The History and Scope of Section 230

Section 230 is the common name for provisions in the 1996 Communications Decency Act that immunize online service providers from civil or criminal liability for both moderating content and for unlawful content created by third parties.[9] As more people began to have home Internet connection and new companies have started experimenting with new ways for humans to connect with one another, Congress sought to remove legal disincentives for online platforms to moderate content.[10] In doing so, they created legal protections for these new companies that helped create the modern Internet.[11]

1. The Substance of Section 230

Section 230 provides legal protections for companies through two provisions that have come under fire from elected officials and commentators: 47 USC § 230(c)(1), which decrees that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider," and § 230(c)(2), which immunizes interactive computer service providers from liability for moderating content or giving users or content creators the ability

9. 47 U.S.C. § 230.
10. *See* 141 CONG. REC. H8469-70 (daily ed. Aug. 4, 1995) (statement of Rep. Cox.).
11. *See* KOSSEFF *supra* note 3.

to moderate content.[12] Interactive computer services include Internet Service Providers (ISPs), websites, apps, social media platforms, online marketplaces, wikis (websites that permit users to make changes to the site itself)[13] news publications, music or podcast hosting services, and any other website where users can post content.[14]

The prohibition against categorizing online service providers as publishers of third-party content effectively immunized companies with websites that allowed third parties to create and post content from lawsuits arising from that content, regardless of whether the companies knew or should have known about specific unlawful content.[15] As long as those companies did not create the content (or induce its creation), they could not be held criminally or civilly liable for user behavior even if they had actual notice of the content and its potential harm.[16] In the twenty-five years since its introduction, defendants have successfully invoked section 230 to bar claims of defamation, invasion of privacy, and negligence.[17]

2. Why Congress Passed Section 230

Congress passed section 230 after court decisions showed that secondary liability laws could penalize companies who made good-faith, but imperfect, efforts to moderate content, even when companies sought to create family-friendly environments online for moderating content.[18] When deciding whether to hold a party responsible for content hosted on its digital platform but created by others, courts distinguished between two categories: publishers of information who have "editorial control" over the information they publish, and distributors who merely transmit information without such control.[19] Publishers are liable for all unlawful content they furnish, but

12. 47 U.S.C. § 230 ("No provider or user of an interactive computer service shall be held liable on account of (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)."); *see also* Jessica Guynn, *Trump vs. Big Tech: Everything You Need to Know About Section 230 and Why Everyone Hates It*, USA TODAY (Oct. 16, 2020, 5:43 PM), https://www.usatoday.com/story/tech/2020/10/15/trump-section-230-facebook-twitter-google-conservative-bias/3670858001/ [https://perma.cc/WU3K-QKDV].

13. *Definition of Wiki*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/wiki (last visited Oct. 19, 2021) [https://perma.cc/5R2M-8YX6].

14. Jeff Kosseff, *The Gradual Erosion of the Law that Shaped the Internet: Section 230's Evolution Over Two Decades*, COLUM. SCI. & TECH. L. REV., Fall 2016, at 8-9.

15. *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 328, 330, 333 (4th Cir. 1997).

16. *Id.*

17. *See generally* Vanessa S. Browne-Barbour*, Losing Their License to Libel: Revisiting § 230 Immunity*, 30 BERKELEY TECH. L.J. 1505 (2016).

18. *See* 141 CONG. REC. H8469-70 (daily ed. Aug. 4, 1995) (statement of Rep. Cox.); *see also* Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 139-40 (S.D.N.Y. 1991).

19. *See Cubby*, 776 F. Supp. at 140-41.

distributors are only liable if they subjectively or constructively have knowledge of unlawful content.[20]

As the Internet proliferated, Congress found that *how* courts applied these categories produced perverse incentives for interactive computer services to not moderate any content and thus encouraged online platforms to purposely ignore horrific or unlawful content.[21] This approach grew out of judicial attempts to apply print media case law to companies operating online.[22] The distinction first arose in *Smith v. California*, where the Supreme Court ruled that the First Amendment prohibited Los Angeles from holding bookstore operators strictly liable for obscene content contained in books offered for sale because the lack of a scienter requirement indirectly limited the distribution of lawful content.[23] The concern of the Court was practical: if bookstores were responsible for the content of every book they sold, they would only sell those books they could verify were lawful, and such verification would add so much time to store operations that many lawful books would not be sold.[24] After *Smith*, courts continued to hold that publishers who republished a libel can be liable for illegal content and applied this rule to newspapers, magazines, and book publishers.[25] Thus, relatively clear rules formed: vendors such as bookstores and newsstands were only liable for unlawful content if they had constructive knowledge, while publishers that exercised editorial control such as book editors, publishing companies, and newspapers were open to liability for all content published.

The development of online platforms where users could not only easily create millions of pieces of content, but could interact with each other as well, created risks for Internet companies attempting to moderate or curate content without sufficient resources to monitor every post. Two cases, *Cubby v. CompuServe* and *Stratton Oakmont v. Prodigy Services*, demonstrate how the archaic categories of publisher and distributor disincentivized online platforms from moderating any of their content by immunizing companies that permitted all users to post unlawful content, but imposed liability on companies that attempted to moderate content if they were not 100% successful.[26]

In *Cubby*, the Southern District of New York held that CompuServe was not liable for defamatory statements created by a third-party user in a "special interest forum" which CompuServe hosted and to which it offered

---

20. *See id.*

21. 141 CONG. REC. H8468 (daily ed. Aug. 4, 1995) (statement of Rep. Cox).

22. *See generally Cubby*, 776 F. Supp. at 140; Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

23. *See* Smith v. California, 361 U.S. 147, 150-51, 154-55 (1959).

24. *See id.* at 154-55.

25. *See generally* Bindrim v. Mitchell, 92 Cal. App. 3d 61 (Ct. App. 1979); Dixson v. Newsweek, Inc., 562 F.2d 626 (10th Cir. 1977); Pittsburgh Courier Pub. Co. v. Lubore, 200 F.2d 355 (D.C. Cir. 1952); Hoover v. Peerless Publications, Inc., 461 F. Supp. 1206 (E.D. Pa. 1978).

26. *See generally Cubby*, 776 F. Supp. at 140; *Stratton Oakmont*, 1995 WL 323710, at 3.

subscriptions.[27] The court ruled that CompuServe was a distributor, not publisher, of the alleged defamatory statements, which included lies about one company stealing information about another and being a "start-up scam," because CompuServe did not review the contents or have notice of any complaints.[28]

Stratton Oakmont showed the dangers of applying these categories to Internet companies when the court ruled that Prodigy Services, which advertised itself as a "family oriented computer network" that monitored and censored content on its online bulletin boards, was a publisher due to this editorial control.[29] An anonymous user posted content on one of Prodigy's online bulletin boards claiming that financial brokerage Stratton Oakmont was a "major criminal fraud" and a "cult of brokers who either lie for a living or get fired."[30] The court found that Prodigy was a publisher (even though the company did not manually review all 60,000 messages posted on the bulletin boards each day) because Prodigy had an "automatic software screening program" and policy guidelines through which employees were empowered to enforce the removal of user-generated content.[31]

In distinguishing Prodigy's system from that found in *Cubby,* the court found that Prodigy had:

> virtually created an editorial staff of Board Leaders who have the ability to continually monitor incoming transmissions and in fact do spend time censoring notes. Indeed, it could be said that PRODIGY's current system of automatic scanning, Guidelines and Board Leaders may have a chilling effect on freedom of communication in Cyberspace, and it appears that this chilling effect is exactly what PRODIGY wants, but for the legal liability that attaches to such censorship.[32]

Thus, the U.S. legal system punished Prodigy for attempting to create a family-friendly environment by forcing them to spend time and money defending lawsuits regarding its hosting of allegedly unlawful content. At the same time, courts rewarded those who refused to moderate the character of third-party content by immunizing them from liability.

Federal lawmakers recognized the dangerous incentives of punishing companies that made good-faith efforts to moderate content while excusing those that purposefully turned a blind eye, and sought to change U.S. law in response to *Stratton Oakmont*.[33] One of the co-authors of section 230, then-Representative Christopher Cox (R-CA), stated that the purposes of his and his co-author's (then-Representative Ron Wyden (D-OR)), amendment was

---

27. *See Cubby*, 776 F. Supp. at 137.
28. *Id.* at 138.
29. *See Stratton Oakmont*, 1995 WL 323710, at *2, *5.
30. *Id.* at *1
31. *Id.* at *2-3, *5.
32. *Id.* at *5.
33. 141 CONG. REC. H8468 (daily ed. Aug. 4, 1995) (statement of Rep. Cox.).

to "protect computer Good Samaritans [and] online service providers . . . who . . . screen indecency and offensive material" while keeping "an army of bureaucrats" away from "regulating the Internet."[34]

The statute itself enumerates five purposes for its passage, the first two of which advance growth of the Internet economy, and the final three of which encourage content moderation:

> It is the policy of the United States—(1) to promote the *continued development of the Internet* and other interactive computer services and other interactive media; (2) to *preserve the vibrant and competitive free market* that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation; (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services; (4) to *remove disincentives for the development and utilization of blocking and filtering technologies* that empower parents to restrict their children's access to objectionable or inappropriate online material; and (5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.[35]

The Fourth Circuit affirmed the broad immunity section 230 confers in *Zeran v. AOL*, when it categorized distributor liability as a type of publisher liability.[36] Consequently, since section 230 prevented courts from holding online service providers liable as publishers of third-party content, such providers were immune from distributor liability even when the platform had subjective or constructive knowledge of unlawful content.[37] The court found that "[t]he imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech."[38] Other circuits have affirmed this immunity from liability for user-created content.[39]

3. Limits to Section 230 Immunity

There are significant statutory and court-defined limits to section 230 protections. The clearest limit is that section 230 does not protect the actual creators of unlawful content; plaintiffs and prosecutors are free to pursue

---

34. *Id.*
35. 47 U.S.C. § 230(b) (emphasis added).
36. *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 332-33 (4th Cir. 1997).
37. *See id.*
38. *Id.* at 330.
39. *See generally* Chicago Lawyers' Comm. for C.R. Under L., Inc. v. Craigslist, Inc., 519 F.3d 666, 669 (7th Cir. 2008); *see also* Ben Ezra, Weinstein, & Co. v. Am. Online Inc., 206 F.3d 980 (10th Cir. 2000).

those parties.[40] Neither does section 230 protect a company when its agents created unlawful content posted online.[41] At least one court has recognized that when defendants know of unlawful content, approve of the unlawful content, and can edit the unlawful content, section 230 immunity does not apply because defendants are operating as publishers or speakers of their own content.[42]

Congress also has statutorily exempted violations of certain laws from immunity, including violations of patent and copyright law, the Electronic Communications Privacy Act, and federal criminal law.[43] Though section 230 does not broadly exempt violations of state criminal law, Congress has exempted specific state crimes.[44] Most recently, Congress also limited immunity by passing the "Allow States and Victims to Fight Online Sex Trafficking Act of 2017" (FOSTA), which amends section 230 to remove protections from website operations with constructive knowledge of user content used for prostitution or human trafficking.[45]

Section 230 immunity also does not apply when an interactive computer service "materially contributes" to the content at issue.[46] The Ninth Circuit used the material contributions test in *Fair Housing Council of San Fernando Valley v. Roommates.com*, where the court ruled that online service providers may be liable for unlawful housing discrimination when the provider induces users to create illegal content.[47] There, the court held Roommates.com liable because it materially contributed to the creation of unlawful content when it prompted users to violate housing antidiscrimination laws by requiring them to select from a list of answers to certain questions in illegal ways.[48] However, when declining to apply section 230 immunity to Roommates.com, the court also stated that "close cases . . . must be resolved in favor of immunity," and clarified there is no liability for providers when providers do not provide such options or solicit the specific discriminatory

40. *See Zeran*, 129 F.3d at 330-31.

41. *See* Kosseff, *supra* note 14, at 25-27 (discussing cases that survived the motion to dismiss stage based on pleadings that alleged defendants controlled or were the persons responsible for the relevant content).

42. *See* FTC v. LeadClick Media, LLC, 838 F.3d 158, 176-77 (2d Cir. 2016) (finding a defendant not entitled to immunity when it paid affiliates to advertise products and advised affiliates on the content of those products).

43. 47 U.S.C. § 230(e).

44. *See* Letter from Nat'l Ass'n of Att'ys Gen. to Various Cong. Leaders (May 23, 2019), https://1li23g1as25g1r8so11ozniw-wpengine.netdna-ssl.com/wp-content/uploads/pdfs/sign-ons/CDA-Amendment-NAAG-Letter.pdf [https://perma.cc/QE5P-6C3W].

45. *See* Allow States and Victims to Fight Online Sex Trafficking Act of 2017, H.R. 1865, 115th Cong. (2018) (codified at 47 U.S.C. § 230(e)(5)).

46. *See* Matthew Feuerman, *Court-Side Seats? The Communications Decency Act and the Potential Threat to StubHub and Peer-to-Peer Marketplaces*, 57 B.C. L. REV. 227, 237-38 (2016).

47. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1169-72 (9th Cir. 2008) (describing how Roommates.com designed its search system to allow users to hide listings based on sex, sexual orientation, and presence of children).

48. *See id.*

information.[49] Across circuits, courts have developed different standards to test when interactive computer services lose immunity for inducing illegal content.[50]

Since *Roommates.com*, courts have found other scenarios where section 230 does not provide immunity, though not all limiting doctrines are applied consistently across jurisdictions.[51] A survey in 2016 of court opinions found four categories of cases where courts have found that section 230 immunity may not apply when: (1) claims do not arise from third-party content,[52] (2) online providers may have developed the content,[53] (3) providers repeated unlawful statements of others,[54] or (4) providers "failed to act in good faith" when suppressing competitors' content.[55]

B. Defining Social Media Platforms and Measuring the Size of Their User Base

Section 230 is relevant for all interactive computer services but is particularly important for social media platforms. This Note defines social media platforms as those that: (1) are Internet-based programs that are interactive between users and the platform; (2) rely heavily on public or semi-public user-generated content, as opposed to platform-generated content, as the foundation of the service; (3) where users have individualized "profiles"; and (4) facilitate social networks by connecting user profiles to facilitate content sharing.[56] "Public or semi-public" is any sharing of content where the original post or message is viewable by users not within the sharing user's network. Since social media platforms rely on the creation and sharing of user-generated content, section 230 immunity, or the lack thereof, is particularly important. Companies that fall under this definition include not only those similar to Facebook, Clubhouse, or Twitter, but also potentially

---

49. *See id.* at 1173-74 (declining to find Roommates.com liable for comments provided by users in the "Additional Comments" section where Roommates.com did not provide options users must select).

50. *See* Feuerman, *supra* note 46 (identifying two general standards used by appellate courts, the encouragement test and the requirement test, that operate under the umbrella of the *Roommates.com* material contributions test).

51. *See* Kosseff, *supra* note 14, at 31 (categorizing case opinions reflecting limits on section 230 immunity).

52. *See id.* at 23; *see also* Doe v. Internet Brands, Inc., 824 F.3d 846, 851 (9th Cir. 2016).

53. *See* Kosseff, *supra* note 14, at 25-27; *see also* AMCOL Sys., Inc. v. Lemberg L., LLC, No. CV 3:15-3422-CMC, 2016 WL 613896 *9 (D.S.C. Feb. 16, 2016); Congoo, LLC v. Revcontent LLC, No. CV16401MASTJB, 2016 WL 1547171, at *3 (D.N.J. Apr. 15, 2016).

54. *See* Kosseff, *supra* note 14, at 27-28; *see also* Diamond Ranch Acad., Inc. v. Filer, No. 2:14-CV-751-TC, 2016 WL 633351, at *20-22 (D. Utah Feb. 17, 2016).

55. *See* Kosseff, *supra* note 14, at 31-33; *see also* e-ventures Worldwide, LLC v. Google, Inc., 188 F. Supp. 3d 1265, 1269 (M.D. Fla. 2016).

56. *See generally* Jonathan A. Obar & Steve Wildman, *Social Media Definition and the Governance Challenge: An Introduction to the Special Issue*, 39 TELECOMMS. POL'Y 745-750 (2015), https://www.sciencedirect.com/science/article/abs/pii/S0308596115001172?via%3Dihub [https://perma.cc/4V25-CVTV] (describing common traits of social media platforms).

online marketplaces where users create unique profiles, post about the products or services they are selling, and can network with other users.[57]

The size of social media platforms is commonly measured by the number of their monthly active users (MAU). MAUs are the industry standard used by platforms, financial analysts, and the press because it is a baseline measurement that people can use to compare websites that provide different services.[58] The advantages of using MAUs as a metric are that they are easily measurable—most online platforms measure the metric as part of their business operations—and the metric captures not only how many users have ever used a website or created a profile, but how many actively engage. While there is debate on the efficacy of using MAUs because companies use different criteria to determine active users, it is worth noting that a significant number of these criticisms come from industry leaders whose perceived company performances would benefit from changing the criteria[59] Even one of those critics admitted that there is a minimum baseline able to be measured that is sufficient for legislative purposes; as Twitter co-founder acknowledged, a MAU is "[s]omething you did [that] caused some data in their servers to be recorded for the month."[60] Defining the "something" users did as creating or consuming any type of content on the platform at issue, including viewing video, listening to audio, or viewing or writing reviews and comments, ensures that all users who actually interact with the website are counted. This standard solves the issue of counting users who use login credentials of one source website (often Facebook or Google) to sign into other websites, but do not actually engage with the source website itself.[61]

C. The Debate on Section 230

The story of section 230 is a complex and nuanced history that implicates different societal values. Proponents often point to the economic benefits that section 230 immunity provides to new and smaller firms in the Internet space.[62] Critics can be generally categorized into two camps: those that believe section 230 permits online platforms to escape societal responsibilities to moderate certain content, and those that believe section 230 permits online platforms to moderate *too much* content. Both critical camps

---

57. *See infra* Part III, Section A.

58. *See* Kurt Wagner, *The 'Monthly Active User' Metric Should Be Retired. But What Takes Its Place?*, VOX: RECODE (Feb. 9, 2015, 12:26 PM), https://www.vox.com/2015/2/9/11558810/the-monthly-active-user-metric-should-be-retired-but-what-takes-its [https://perma.cc/DQ93-HXXF].

59. *See* Ben Munson, *Deeper Dive—Xumo, Tubi, Pluto TV and the Monthly Active User Debate*, FIERCEVIDEO (Oct. 9, 2020, 10:51AM), https://www.fiercevideo.com/video/deeper-dive-xumo-tubi-pluto-tv-and-monthly-active-user-debate [https://perma.cc/8B3T-8CVC] (founder of video-streaming service claims "There's no standard for MAUs" even though a user who never logged into the website during the month at issue would definitely not be considered an MAU); *see also* Wagner, *supra* note 58 (Twitter CEO critiques the MAU metric based on different web services after Instagram announces more MAUs than Twitter).

60. *See* Wagner, *supra* note 58.

61. *See id.*

62. *See* KOSSEFF, *supra* note 3, at 149-50.

argue that this immunity has permitted companies with substantial power over public discourse to ignore values such as tolerance and presentation of different viewpoints in pursuit of profit.[63] This section discusses how section 230 immunity encourages competition by protecting smaller and new firms and analyzes how both critical camps seek to curb the influence of social media companies.

1. How Section 230 Immunity Is Vital for the Modern Internet Economy by Promoting Competition Through Protecting Small Firms

Section 230 helped create the modern Internet by removing a significant threat to burgeoning companies: existentially-threatening litigation costs for user-created content that was nearly impossible to perfectly monitor.[64] Damages for common claims precluded by section 230, including defamation, can be unpredictable and cost millions of dollars.[65] Additionally, section 230 can end claims relatively early in the litigation process, thereby preventing expensive legal costs.[66] One survey of in-house attorneys estimates that even in a case where an online services provider would be found not liable, legal costs could run over $500,000 just to get through the discovery phase before reaching the trial stage.[67] As one section 230 scholar put it, "[w]ithout [s]ection 230, each user who posted a comment, photo, or video on a website would represent another small but real risk that the website could be sued out of existence."[68] In contrast, successful section 230 defenses can end a case at the motion to dismiss or summary judgment stages, which can cost much less—80,000 or $150,000, respectively.[69] Though some commentators have argued that First Amendment protections would serve the same role as section 230 immunity,[70] there is uncertainty that First Amendment protections are as broad and can be defended as inexpensively as section 230 immunity.[71]

---

63. *See infra* Part II, Section C, Part 2.

64. *See* KOSSEFF, *supra* note 3, at 177-78.

65. *See* Kate Taylor, *ABC Settled 'Pink Slime' Lawsuit for $177 Million, Leaving the Beef Company Feeling 'Vindicated'*, BUS. INSIDER (Aug. 9, 2017, 9:13 AM), https://www.businessinsider.com/pink-slime-case-177-million-settlement-2017-8 [https://perma.cc/7YVU-JVNE].

66. *See* ENGINE, SECTION 230: COST REPORT 1-2 https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/5c8168cae5e5f04b9a30e84e/1551984843007/Engine_Primer_230cost2019.pdf [https://perma.cc/TY56-H48T].

67. *Id.*

68. KOSSEFF, *supra* note 3, at 149-50.

69. ENGINE, *supra* note 66.

70. *See generally* Note, *Section 230 As First Amendment Rule*, 131 HARV. L. REV. 2027, 2028 (2018).

71. *See* Elliot Harmon, *It's Not Section 230 President Trump Hates, It's the First Amendment*, ELEC. FRONTIER FOUND. (Dec. 9, 2020), https://www.eff.org/deeplinks/2020/12/its-not-section-230-president-trump-hates-its-first-amendment [https://perma.cc/FQA5-9FL3].

These protections were vital to create a favorable legal and economic environment for the modern Internet. While today, the Internet may be seen as largely shaped by corporations founded in the United States—such as Amazon, Google, and Facebook—American dominance was not predetermined.[72] As the Internet began to enter the public consciousness and commercial opportunities arose, start-up firms experimented with new ways to connect human beings with one another by creating interactive services where users created and shared their own content.[73] These services necessarily required users to create unprecedented amounts of content—almost impossible for new firms with limited financial resources to effectively monitor and moderate—and section 230 immunity allowed companies to experiment without prohibitively expensive legal or compliance costs.[74]

European and Asian countries, which also grappled with regulating this new Internet economy, declined to extend protections as extensive as those in section 230 to interactive computer services.[75] In part because of this difference, thirteen of the twenty-one largest technology companies are located in the U.S.[76] While differences in privacy and intellectual property laws also added to this disparity, section 230 significantly contributed (and still contributes) to the ability of online companies to invest in their products and services instead of legal fees.[77]

Lower costs and consequently fewer barriers to entry for new firms means that competition and innovation thrived, and continues to thrive, in the United States Internet economy. While market power in certain areas indicates that portions of the Internet economy can be heavily concentrated (84% of advertising investment is spent on Facebook and Google, and Amazon controls almost half of ecommerce)[78] these firms and other large technology firms act in many ways as if they operate in a competitive environment.[79] The relative ease in which consumers and businesses can switch services, competitors can adopt business models of rivals, and new entrants can offer rival services has maintained competitive pressures in the technology and online markets.[80] The consequences: increased spending on research and development, a steady share of revenue for labor (as opposed to

72. *See generally* DIPPON, *supra* note 1.

73. *See* KOSSEFF, *supra* note 3, at 175-78.

74. *See* Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L. J. 639, 670 (2014).

75. KOSSEFF, *supra* note 3, at 179.

76. DIPPON, *supra* note 1, at 5.

77. *See* Chander, *supra* note 74.

78. INTERNET SOCIETY, CONSOLIDATION IN THE INTERNET ECONOMY 19 (2019), https://future.internetsociety.org/2019/wp-content/uploads/sites/2/2019/04/InternetSociety-GlobalInternetReport-ConsolidationintheInternetEconomy.pdf [https://perma.cc/68NP-UMLY].

79. *See* MICHAEL MANDEL, COMPETITION AND CONCENTRATION: HOW THE TECH/TELECOM/ECOMMERCE SECTOR IS OUTPERFORMING THE REST OF THE PRIVATE SECTOR 23 (2018), https://www.progressivepolicy.org/wp-content/uploads/2018/11/PPI_Competition-Concentration-2018.pdf [https://perma.cc/DW46-UACX].

80. *See id.* at 2-4.

other sectors where works have received declining proportions of revenue), massive increases in productivity, and declining prices for consumers.[81]

Section 230 protections particularly help the startup businesses that increase competition, productivity, and innovation across the broader economy, but inherently have less capital and stable funding to pay legal costs.[82] In contrast to other industries and even the popular conception of the technology sector, the number of new technology firms has significantly increased.[83] From 2007 to 2016, the number of technology-based startups has grown by 47%.[84] Technology startups are particularly important to the United States economy, as they have higher pay and longer-lasting jobs compared to new firms in other industries.[85]

Increased competition reduces the power of market-dominant corporations.[86] While major Internet companies have a powerful influence on our lives, the threat of new firms and rivals provides a check on undue influences of that power; if the quality of available products falter or a new entrant provides innovative value for consumers, incumbent firms will lose market share and profits.[87] Without section 230, the companies that benefited from its immunity when they were new entrants with small revenue, but are now valued at hundreds of billions or even over a trillion dollars, would be even more secure in their market dominance as increased costs would lead to fewer competitor startups, and even the surviving startups would have fewer resources to invest.[88] As one academic put it: "[i]f you really want to stick it to Google and Facebook, you should fight to preserve [s]ection 230's competition-enhancing benefits. Otherwise, you are implicitly rooting to squelch the future competitive threats they should face, which only strengthens the Internet giants' marketplace dominance."[89]

Economic analyses show that further reducing section 230 protections would also significantly harm the general economy. One study projects the United States economy would lose $44 billion a year and 425,000 jobs due to lost investment in online companies generally, and especially in new startup firms.[90] These projections likely underestimate the economic harm, as they

---

81. *Id.*; *see also* Matthew Lane, *How Competitive is the Tech Industry?*, DISRUPTIVE COMPETITION PROJECT (July 29, 2019), https://www.project-disco.org/competition/072919-how-competitive-is-the-tech-industry [https://perma.cc/58SH-LPGN].

82. J. JOHN WU & ROBERT D. ATKINSON, HOW TECHNOLOGY-BASED START-UPS SUPPORT U.S. ECONOMIC GROWTH 7 (2017), http://www2.itif.org/2017-technology-based-start-ups.pdf [https://perma.cc/VKY4-2PPP].

83. *See id.* at 6.

84. *Id.*

85. *See id.* at 8-9.

86. *See* Eric Goldman, *Want to Kill Facebook and Google? Preserving Section 230 Is Your Best Hope*, BALKIN (June 3, 2019), https://balkin.blogspot.com/2019/06/want-to-kill-facebook-and-google.html [https://perma.cc/HU3K-ZV7W].

87. *See id.*

88. *The 100 Largest Companies in the World by Market Capitalization in 2021*, STATISTA (Sept. 10, 2021), https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/ [https://perma.cc/4ZWH-QNN3].

89. *See* Goldman, *supra* note 86.

90. *See* DIPPON, *supra* note 1, at 2.

do not even include the value of social media companies often targeted by section 230 reform proposals.[91] Even *uncertainty* of the extent of section 230 immunity can inhibit growth of small and innovative companies.[92]

2. Criticism of Section 230 Immunity

Substantive criticisms of section 230 immunity generally fall into two categories: (1) content moderation of disfavored speech, especially hateful, violent, or illegal content, is insufficient; and (2) content moderation disproportionately censors certain political perspectives. Some proposed legislation targets not only the blatant removal or non-removal of content, but also how social media platforms display such content through algorithms that determine the type and frequency of content seen by users.[93]

a. Inadequate Censorship of Hateful or Violent Speech

Critics charge that section 230 protections not only permit web companies to ignore illegal, harmful, or reprehensible content, but also allows companies to design their services to profit from such content.[94] Commentators and lawmakers have attacked online services for profiting from hosting solicitations for illegal acts, such as prostitution, human trafficking, nonconsensual photos and videos, and, in some jurisdictions, "revenge porn."[95] They have also criticized social media companies for refusing to moderate or inadequately moderating repugnant racist or misogynistic speech, or providing forums for extremist groups to organize violent events or even terrorist attacks.[96] The January 6th U.S. Capitol storming, where extremists allegedly used private Facebook groups to

91. *See id.*

92. *See* DIPPON, *supra* note 1, at 4, 19.

93. Protecting Americans from Dangerous Algorithms Act, H.R. 2154, 117th Cong. (2021).

94. *See* Nicole Phe, *Social Media Terror: Reevaluating Intermediary Liability Under the Communications Decency Act*, 51 SUFFOLK U. L. REV. 99, 129-130 (2018).

95. *See* Amanda L. Cecil, *Taking Back the Internet: Imposing Civil Liability on Interactive Computer Services in an Attempt to Provide an Adequate Remedy to Victims of Nonconsensual Pornography*, 71 WASH. & LEE L. REV. 2513, 2520 (2014); *see also* NAT'L CTR. ON SEXUAL EXPLOITATION, https://endsexualexploitation.org/ [https://perma.cc/YL27-DHHB].

96. *See* Phe, *supra* note 94, at 99-102; *see also* Felix Gillette & Laurence Arnold, *Why Section 230 is Nub of Fights Over Online Speech*, BLOOMBERG (Feb. 2, 2021), https://www.bloomberg.com/news/articles/2021-02-02/why-section-230-is-nub-of-fights-over-online-speech-quicktake [https://perma.cc/7V9N-K8FA].

organize a rally that led to a riotous invasion of the U.S. Capitol, fueled further calls to remove section 230 immunity from social media companies.[97]

These reform proposals would remove immunity for platforms that fail to adequately censor certain speech that falls into certain categories. The Platform Accountability and Consumer Transparency (PACT) Act requires platforms to remove certain content within specific timeframes after receiving knowledge of the content or of court judgments.[98] Another proposal, the Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms (SAFE TECH) Act, would remove section 230 immunity for speech violating civil rights or cyberstalking laws, as well as any type of paid speech – including advertising.[99] Some lawmakers have also suggested to remove immunity for platforms that do not remove or flag fake videos.[100]

Critics have also alleged that not only do social media platforms fail to moderate certain content, but the algorithms these companies use *proactively* encourage disfavored speech by promoting such content by showing or recommending it to more users than other content. A prominent critic in this category, Congresswoman Anna G. Eshoo, has claimed that Internet platforms use "opaque algorithms" that increase engagement on platforms, and that these algorithms, created for increased profits, can create "offline harms."[101] These platforms do not necessarily purposefully promote disfavored speech, but because their algorithms often amplify content already receiving heightened engagement, and because hateful or violent speech often has high engagement, such content can be promoted even though the algorithm mechanics are facially neutral regarding the type of content.[102] By promoting such speech, the criticism goes, social media companies change what is seen as socially acceptable and effectively make it "okay" to have those views. The Protecting Americans from Dangerous Algorithms Act (PADAA) proposes to remove immunity if platforms amplify certain content

---

97. *See* Kevin Collier, *Some Pro-Trump Extremists Used Facebook to Plan Capitol Attack, Report Finds*, NBC NEWS (Jan. 19, 2021), https://www.nbcnews.com/tech/tech-news/some-pro-trump-extremsists-used-facebook-plan-capitol-attack-report-n1254794 [https://perma.cc/49EA-2C32]; *see also* Sara Morrison, *How the Capitol Riot Revived Calls to Reform Section 230*, RECODE (Jan. 11, 2021), https://www.vox.com/recode/22221135/capitol-riot-section-230-twitter-hawley-democrats [https://perma.cc/V9PT-HRZ4].

98. Platform Accountability and Consumer Transparency Act, S. 797, 117th Cong. (2021); *see also* Protecting Americans from Dangerous Algorithms Act, H.R. 2154, 117th Cong. (2021).

99. *See* SAFE TECH Act, S. 299, 117th Cong. (2021).

100. *See* MARK R. WARNER, POTENTIAL POLICY PROPOSALS FOR REGULATION OF SOCIAL MEDIA AND TECHNOLOGY FIRMS 8-10, https://graphics.axios.com/pdf/PlatformPolicyPaper.pdf [https://perma.cc/4V25-CVTV].

101. Press Release, Office of United States Representative Anna Eshoo, Reps. Eshoo and Malinowski Introduce Bill to Hold Tech Platforms Liable for Algorithmic Promotion of Extremism (Oct. 20, 2020), https://eshoo.house.gov/media/press-releases/reps-eshoo-and-malinowski-introduce-bill-hold-tech-platforms-liable-algorithmic#:~:text=The%20bill%20narrowly%20amends%20Section,with%20civil%20rights%20(42%20U.S.C [https://perma.cc/S3US-TTMW].

102. *See* Mark Zuckerberg, *A Blueprint for Content Governance and Enforcement*, FACEBOOK (Mar. 13, 2021), https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/ (last accessed Oct. 11, 2021).

related to violating civil rights and international terrorism,[103] and the 21st Century FREE Speech Act would remove section 230 immunity for *all* content that social media platforms promote through algorithms.[104]

b. Politically Biased Censorship

Other critics lament that when online platforms do moderate user content, they disproportionately moderate certain voices depending on the political views espoused. Conservative elected officials and organizations have received particular attention for their claims of perceived censorship; however, elected officials on the left side of the aisle have expressed similar concerns when social media companies have removed or restricted their content.[105]

Credible evidence of systemic bias remains undiscovered, though there are anecdotes that suggest social media companies struggle with maintaining consistent enforcement of moderation policies.[106] Conservatives have criticized how social media companies treated President Trump while in office, including the widespread de-platforming of the President after the Capitol attack and instances of platforms placing various warnings on his social media posts.[107] Many conservatives have also strongly condemned the shunning of social media site Parler after the Capitol riots.[108] After user posts supporting and organizing the rioters became publicly known, Amazon abruptly banned the website from its web-hosting services for breaking its

---

103. Protecting Americans from Dangerous Algorithms Act, H.R. 2154, 117th Cong. (2021).

104. 21st Century FREE Speech Act, S. 1384, 117th Cong. (2021).

105. *See* Prager Univ. v. Google LLC, No. 17-CV-06064-LHK, 2018 WL 1471939, at *1 (N.D. Cal. 2018); *see also* Sara Morrison, *supra* note 97; Mahita Gajanan, *Facebook Removed Elizabeth Warren's Ads Calling for the Breakup of Facebook*, TIME MAG. (Mar. 11, 2019), https://time.com/5549467/elizabeth-warren-facebook-breakup-ads [https://perma.cc/L9RN-Z4XK].

106. *See* Casey Newton, *The Real Bias on Social Networks Isn't Against Conservatives*, VERGE (Apr. 11, 2019, 6:00 AM), https://www.theverge.com/interface/2019/4/11/18305407/social-network-conservative-bias-twitter-facebook-ted-cruz [https://perma.cc/GEE5-XGBY]; *see also* Jessica Bursztynsky, *Twitter CEO Jack Dorsey Says Blocking New York Post Story Was 'Wrong'*, CNBC (Oct. 16, 2020, 9:25 AM), https://www.cnbc.com/2020/10/16/twitter-ceo-jack-dorsey-says-blocking-post-story-was-wrong.html [https://perma.cc/46G9-3JNX]; Shannon Bond, *Facebook, YouTube Warn of More Mistakes as Machines Replace Moderators*, NAT'L PUB. RADIO (Mar. 31, 2020), https://www.npr.org/2020/03/31/820174744/facebook-youtube-warn-of-more-mistakes-as-machines-replace-moderators [https://perma.cc/X58C-MCS7].

107. *See* Cristiano Lima, *Twitter Boots Trump*, POLITICO (Jan. 8, 2021), https://www.politico.com/news/2021/01/08/twitter-suspends-trump-account-456730 [https://perma.cc/9KPJ-7DGF]; *see also* Shannon Bond, *Trump Threatens to Shut Down Social Media After Twitter Adds Warning to His Tweets*, NAT'L PUB. RADIO (May 27, 2020), https://www.npr.org/2020/05/27/863011399/trump-threatens-to-shut-down-social-media-after-twitter-adds-warning-on-his-twee [https://perma.cc/D5CJ-MTZV].

108. *See* John Paczkowski & Ryan Mac, *Amazon Will Suspend Hosting for Pro-Trump Social Network Parler*, BUZZFEED NEWS (Jan. 9, 2021), https://www.buzzfeednews.com/article/johnpaczkowski/amazon-parler-aws [https://perma.cc/S7NK-D9WT].

terms of service.[109] These claims are not limited to conservatives as progressives have also criticized social media platforms for allegedly unfair treatment; Democratic Senator and then-Presidential candidate Elizabeth Warren accused Facebook of blocking her campaign ads after she called for the government to take antitrust action against the company.[110]

How the removal of section 230 immunity is specifically operationalized depends on the proposed legislation. One proposal would replace the phrase "otherwise objectionable" with the more specific, and presumably smaller scope, "promoting self-harm, promoting terrorism, or unlawful" in section 230 (c)(2)(A), and seeks to limit when section 230 protects online platforms from liability for content moderation decisions.[111] Another proposed bill defines the good faith requirement to prohibit platforms from "intentionally selective enforcement of the terms of service,"[112] and yet another would require online platforms to receive certification from the Federal Trade Commission that its moderation decisions are not biased based on politics.[113] A separate bill would categorize "major internet communications platforms" as common carriers and impose non-discrimination requirements based on political sentiments on such platforms.[114] On the state level, Florida recently passed legislation that purports to prohibit social media platforms from de-platforming statewide candidates, though its survivability in the courts is in question partly because of section 230.[115]

III. ANALYSIS

A. Overarching Purpose of Section 230 Reforms Is to Limit the Power of Large Social Media Companies on Public Discourse

Almost all proposals to reform section 230 center on the goal of limiting the power that large social media companies have on public discourse. Proponents of removing immunity based on biased content moderation policies cite the power social media companies have over public discourse. Senator Ted Cruz called these companies and the immunity they receive under section 230 "the 'single greatest threat to our free speech and democracy.'"[116] After Twitter banned then-President Trump, Senator Lindsey Graham declared "I'm more determined than ever to strip [s]ection

109. *See id.*

110. *See* Gajanan, *supra* note 105.

111. Online Freedom and Viewpoint Diversity Act, S. 4534, 116th Cong. (2020).

112. Limiting Section 230 Immunity to Good Samaritans Act, S. 3983, 116th Cong. (2020).

113. Ending Support for Internet Censorship Act, S. 1914, 116th Cong. (2019).

114. 21st Century FREE Speech Act, S. 1384, 117th Cong. (2021).

115. FLA. STAT. ANN. 106.072 (West 2021); *see also* NetChoice, LLC v. Moody, No. 4:21CV220-RH-MAF, 2021 WL 2690876, at *1 (N.D. Fla. June 30, 2021) (preliminary injunction).

116. *See* Morrison, *supra* note 97.

230 protections from Big Tech that let them be immune from lawsuits."[117] These statements reflect concerns that certain companies have such power over public discourse that they can influence society and politics by removing certain categories of speech or banning certain users, such as the president of the United States, from engaging on their social media platforms.

Proponents of increased content moderation have lambasted the inability or unwillingness of large social media companies to censor certain speech that, when spread, can harm society. Senator Richard Blumenthal argued that the tech platforms' acts after the January 6th, 2021, rally and attack of the U.S. Capitol were too late: "[t]he question isn't why Facebook and Twitter acted, it's what took so long and why haven't others?"[118] Then-presidential candidate Representative Beto O'Rourke, who proposed to remove section 230 immunity if platforms do not censor certain speech, attacked how much power they have "to undermine our democracy and affect the outcomes of our elections."[119] During his campaign, President Biden argued for the absolute revocation of section 230 for Facebook and other large platforms because, he alleged, they are "propagating falsehoods they know to be false."[120] The statements are concerns not only about the initial publication of such information, but primarily about the spread of such information through the general public and the consequences.

Congressional findings in proposed section 230 legislation also indicate that legislators from both parties are primarily concerned with limiting the power of social media companies on public discourse. The Democrat-sponsored Algorithmic Justice and Online Platform Transparency Act notes that "[o]nline platforms have become integral to individuals' full participation in economic, democratic, and societal processes."[121] The Republican-sponsored 21st Century FREE Speech Act states that the internet "offer[s] a forum for a true diversity of political discourse and viewpoints, unique opportunities for cultural development, and myriad avenues for intellectual activity . . . Americans rely on [I]nternet platforms and websites for a variety of political, education, cultural, and entertainment services and for communication with one another."[122] These findings align with the above-

---

117. Cristiano Lima, *Fuming Republicans Find Themselves Powerless Over Tech Clampdown*, POLITICO (Jan. 11, 2021), https://www.politico.com/news/2021/01/11/gop-tech-retaliation-457945 [https://perma.cc/9BKD-Q63D].

118. *See* Morrison, *supra* note 97.

119. Sarah Salinas, *2020 Hopeful Beto O'Rourke Says He'd Rather See Big Tech Regulated Than Broken Up*, CNBC (Mar. 21, 2019), https://www.cnbc.com/2019/03/21/beto-orourke-says-big-tech-needs-regulation-not-a-breakup.html [https://perma.cc/J8S2-88J3]; *see also* Lauren Feiner, *Beto O'Rourke Goes After Key Immunity for Social Media Companies if They Allow Users to Incite Violence*, CNBC (Aug. 16, 2019, 4:24 PM), https://www.cnbc.com/2019/08/16/beto-orourke-goes-after-immunity-for-big-tech-after-el-paso-shooting.html [https://perma.cc/JT8M-ZZK8].

120. *See* Makena Kelly, *Joe Biden Wants to Revoke Section 230*, VERGE (Jan. 17, 2020), https://www.theverge.com/2020/1/17/21070403/joe-biden-president-election-section-230-communications-decency-act-revoke [https://perma.cc/8MV4-H8KK].

121. Algorithmic Justice and Online Platform Transparency Act, H.R. 3611, 117th Cong. § 2(1) (2021).

122. 21st Century FREE Speech Act, S. 1384, 117th Cong. § 2 (2021).

mentioned public statements of section 230 reform proponents by centering on the influence of social media platforms in society.

The shared viewpoint across reform proponents is that large social media companies have too much power over society to have such a broad grant of immunity. Critics of censorship worry about companies deciding what speech hundreds of millions of Americans see and how that power is exercised. Critics of inadequate content moderation worry about how large companies profit from dangerous and radical speech that can change the public discourse of mainstream society. Both groups offer solutions to problems based on the premise that making social media platforms more accountable for removing or moderating certain speech can influence the public.

B. Section 230 Reforms Should be Limited to Content Posted on Social Media Platforms with Over 50 Million Monthly Active Users That Generate Over $500 Million in Annual Revenue

In light of the positive benefits of section 230 immunity on the United States economy and competition, any changes further restricting the immunity should be small, careful, and apply to as few firms as possible. Businesses that would become liable under section 230 reforms should be only those that are responsible for the problems Congress seeks to solve—social media platforms with a sufficient number of users to affect public discourse and opinion. Reforms should also only apply to firms able to survive and profit from their social media platforms even after increased compliance, moderation, and legal costs in order to preserve the competitive market and protect new, innovative companies.

1. Limiting Changes to Section 230 Immunity Will Limit Unpredictable Negative Consequences

When seeking to reform established legislation—especially legislation with such powerful positive benefits such as helping create the modern Internet and economic flourishing of the U.S. tech industry—lawmakers should hesitate before enacting sweeping changes. Humility is especially important when reforms may come at the expense of one of the primary purposes of section 230: competition in the online economy.[123] At the same time, the Internet economy has drastically changed since Congress enacted section 230, and there may be legitimate policy reasons to hold powerful and wealthy companies with online platforms accountable for permitting unlawful content to flourish.

By broadly removing section 230 immunity, lawmakers would effectively impose new regulatory costs on small platforms that can challenge the large incumbents. Regulations can harm competition by increasing costs and barriers to entry, making it more difficult for new and innovative

123. *Id.*

competitors to challenge incumbent firms.[124] Large businesses also gain even more competitive advantages over smaller ones because they often have the financial resources to comply with rules without significantly losing profits or investment in other areas.[125] Carefully targeted changes to section 230 immunity removes these advantages that large social media companies would otherwise have over their competition and reduces the opportunities for increased consolidation in the technology industry.

Section 230 proponents oppose any attempts to reform section 230 partly because restricting section 230 immunity will limit competition and stifle innovation by increasing costs on new and smaller online platforms.[126] One of the original authors of section 230, now-Senator Ron Wyden, argued that "[i]f you unravel 230, then you harm the opportunity for diverse voices, diverse platforms, and, particularly, the little guy to have a chance to get off the ground."[127] Widespread criticism of reforms has arisen from various companies that operate online websites and cybersecurity services as well, including Etsy, Nextdoor, Tripadvisor, Cloudflare, GoDaddy, and the Wikimedia Foundation.[128] These organizations point out that even targeted reforms like FOSTA can have devastating unintended consequences that lead to market consolidation and harms those the law purportedly did not intend to victimize.[129] They also point out that the users themselves remain vulnerable to liability, as section 230 does not immunize the creators or repeaters of the content.[130]

How social media platforms reacted to the passage of FOSTA, which removed section 230 immunity for platforms found to "support" two specific crimes (prostitution and human trafficking), shows how even a targeted law can consolidate more power into large companies while forcing small ones out of the market.[131] By removing section 230 immunity for those "supporting" certain unlawful conduct, Congress actually imposed severe

---

124. *See* HOWARD BEALES ET AL., GOVERNMENT REGULATION: THE GOOD, THE BAD, & THE UGLY 4 (2017), https://regproject.org/wp-content/uploads/RTP-Regulatory-Process-Working-Group-Paper.pdf [https://perma.cc/HQ5U-99MF].

125. *See id.* at 8.

126. *See* Emily Stewart, *Ron Wyden Wrote the Law That Built the Internet. He Still Stands by It - and Everything It's Brought with It*, RECODE (Mar. 16, 2019, 9:50 AM), https://www.vox.com/recode/2019/5/16/18626779/ron-wyden-section-230-facebook-regulations-neutrality [https://perma.cc/KML7-E8YA].

127. *Id.*

128. *See* THE INTERNET WORKS COALITION, https://www.theinternet.works/issue/ (last accessed Oct. 27, 2021) [https://perma.cc/UF8X-CNQQ]. While some of the largest online platforms have supported section 230 reforms, critics are skeptical that support from large internet companies, which began and grew under section 230 immunity but now have the financial resources to survive liability lawsuits and moderate content that smaller competitors do not, to change section 230 are pure or altruistic.

129. *See* Elliot Harmon, *In Debate Over Internet Speech Law, Pay Attention to Whose Voices Are Ignored*, HILL, (Aug. 21, 2019), https://thehill.com/opinion/technology/458227-in-debate-over-internet-speech-law-pay-attention-to-whose-voices-are [https://perma.cc/9QGM-VH2Z].

130. *See* Kosseff, *supra* note 14, at 25-27.

131. *See* Allow States and Victims to Fight Online Sex Trafficking Act of 2017, H.R. 1865, 115th Cong. (2018) (codified at 47 U.S.C. § 230(e)(5)).

moderation requirements that smaller companies or those with less-profitable social media platforms could not meet.[132] In response to the bill's passage, Craigslist shut down its "Personals" section due to concerns that maintaining the service would be "jeopardizing all [of their] other services."[133] Reddit closed several forums that *might* have included unlawful content, but which certainly included lawful content as well.[134] At least one legal niche dating service shut down due to financial liability concerns.[135] Yet even as smaller websites shut down services, Facebook used its vast resources to launch its own dating service just a few weeks after Congress passed FOSTA.[136] If a narrowly tailored law such as FOSTA can cause smaller or less-profitable companies to close lawful services out of fear of legal and compliance costs, more sweeping and fundamental changes to section 230 could cause even more businesses to close or lawful services to discontinue.

2. Reform Proposals Seek to Solve Problems Caused by Social Media Platforms

Restrictions to section 230 immunity should apply only to social media platforms, not to every website where users can provide any type of content. Targeting only social media platforms would limit new liability exposure to those companies with the most influence on public discourse and those that have the greatest power to amplify or censor content.

Limiting immunity to social media platforms holds the most influential companies accountable for unlawful content shared on their platforms while not imposing unnecessary costs on companies with business models not built on sharing content and therefore have less impact on public discourse. The shared primary purposes of section 230 reforms are functional—to prevent the amplification or censorship of certain content.[137] The primary purposes are not the first expression itself of the content (such as original Facebook posts or Twitter tweets), which would be almost impossible for the government or private companies to effectively police, but the widespread sharing or censorship of unlawful or political speech.[138] Social media

---

132. *See* Merrit Kennedy, *Craigslist Shuts Down Personals Section After Congress Passes Bill On Trafficking*, NAT'L PUB. RADIO (Mar. 23, 2018), https://www.npr.org/sections/thetwo-way/2018/03/23/596460672/craigslist-shuts-down-personals-section-after-congress-passes-bill-on-traffickin [https://perma.cc/2XB8-3UTE]; *see also* Elizabeth Nolan Brown, *Hours After FOSTA Passes, Reddit Bans 'Escorts' and 'SugarDaddy' Communities*, REASON (Mar. 22, 2018), https://reason.com/2018/03/22/reddit-bans-escort-subreddits [https://perma.cc/9AGD-489G].

133. *See* CRAIGSLIST, https://www.craigslist.org/about/FOSTA, (wishing "every happiness" to "the millions of spouses, partners, and couples who met through craigslist") [https://perma.cc/7RST-D47H].

134. *See* Brown, *supra* note 132.

135. *See* Samantha Cole, *Furry Dating Site Shuts Down Because of FOSTA*, VICE (Apr. 2, 2018, 10:00 AM), https://www.vice.com/en/article/8xk8m4/furry-dating-site-pounced-is-down-fosta-sesta [https://perma.cc/8KZY-LFXT].

136. *See* Harmon, *supra* note 129.

137. *See supra*, Part IV.

138. *See id.*

companies definitionally are those platforms that most facilitate such sharing of speech because they are the online services where users can share content with friends or strangers, react to others' content, and create identifying user profiles.[139] To hold companies who do not facilitate content sharing liable for third-party content would apply the reforms outside of those necessary to accomplish the goals of reformers and to amplify the costs or unintended consequences.

The social media criteria capture not only to traditionally perceived social media platforms like Facebook and Twitter, but also to certain online marketplaces where users, including individuals or businesses, can sell products or services to other users. Platforms like Airbnb, eBay, Etsy, or Amazon third-party selling require users to create profiles and facilitate social networking in a manner similar to "traditional" social media companies such as Facebook or Twitter.[140] They also provide users areas for reviews or comments, which open the possibility that they host unlawful defamatory statements.[141] However, other criteria such as a minimum number of content-producing users, may preclude application to smaller online marketplaces.

Websites excluded by the social media platform criteria include those where the user has no interaction or only one-way interaction with other users or content creators. These include blogs or news publications with comment sections that lack social networking services or user profiles; companies that operate websites to sell their own products with consumer reviews; and services, such as audio or video streaming, where users consume content but do not create their own. Importantly, the social media criterion would exclude many wikis, even though some require users to create individualized pages that could constitute "profiles," because they effectively funnel volunteers to create a non-interactive end product.[142] Wikis generally do not facilitate networking among users except to discuss the end product, certain users can be banned for inactivity, and the end product is non-interactive with website visitors except for those who sign up to edit the wiki.[143] Websites such as the New York Times or New York Post, Wikipedia, and streaming services that do not allow casual users to post content (such as Netflix, Hulu, or Pandora) would also still have section 230 immunity.

Limiting section 230 immunity restrictions to platforms that share public or semi-public content preserves immunity for private messaging platforms as well. To not exempt these platforms would not only encourage,

---

139. *See supra*, Part II.

140. *See, e.g.*, *Why we require a profile*, AIRBNB, https://www.airbnb.com/help/article/67/why-we-require-a-profile (last visited Nov. 9, 2021) [https://perma.cc/Q8ZS-EG8Z].

141. *See id*.

142. *See Wikipedia: What Wikipedia Is Not*, WIKIPEDIA, https://en.wikipedia.org/wiki/Wikipedia:What_Wikipedia_is_not#Wikipedia_is_not_a_blog,_web_hosting_service,_social_networking_service,_or_memorial_site [https://perma.cc/CE3P-DUGN].

143. *See Wikipedia:Wikipedia Is a Volunteer Service*, WIKIPEDIA, https://en.wikipedia.org/wiki/Wikipedia:Wikipedia_is_a_volunteer_service [https://perma.cc/C4X5-QF3P].

but could actually require, companies to actively monitor and store users' private communications. The costs of this mandatory invasion of user privacy likely do not outweigh the benefits, especially considering that private messages have less influence on public discourse and less ability to broadcast the type of content about which policymakers have expressed concern, such as hate speech or violent speech.[144] This requirement would preserve protections for services like WhatsApp and Signal.

3. Applying Section 230 Restrictions to Smaller Companies Will Unnecessarily Penalize Businesses with Few Active Users and Relatively Little Revenue by Decreasing Competition

Section 230 reforms should only apply to platforms with 50 million MAUs and generate over $500 million in annual revenue. These threshold criteria help avoid both penalizing companies that do not have the user base to influence public discourse and empowering large online platforms even more so by reducing competition by increasing costs on competitive small businesses. The relevant factors to consider are not only the number of users on an online platform, which reflects the influence that a particular social media platform has on public discourse, but also the revenue that the platform generates. A platform with a high number of users but little revenue cannot survive increased legal liability, while a platform with high revenue but with fewer users has insufficient social influence to justify such liability costs. Thus, both standards should be met before new section 230 limits apply.

a. Limiting Reforms to Platforms with Over 50 Million Monthly Active Users Holds Influential Platforms Accountable While Protecting New Services and Competition

By limiting the applicability of section 230 reforms to large online platforms, defined as those with more than 50 million MAUs, the integrity of reformers' purposes will remain as the law applies to the most influential websites while new platforms will still have the ability to establish and generate revenue without crumbling due to legal liability. This section will examine why Congress should use 50 million MAUs as the standard and how small platforms would benefit from an exemption.

Small platforms are less likely to have the type of influence on public society or create offline harms than larger platforms, and to impose increased legal costs on them would throttle competition. Though smaller platforms like

144. Reforms to section 230 do not seek to solve the problem of unpopular or hateful posts, but instead the amplification of those messages.

Parler, which once claimed twelve million MAUs,[145] can serve as hosts for illegal speech, larger platforms are essential for amplification and translation of such speech into movements that involve hundreds or thousands of people.[146] Experts have cited Twitter as important for radical views to reach political and journalism influencers whose amplification can (even unintentionally) spread misinformation or violent speech, and Facebook is used by conspiracy theorists to expose a mainstream audience to their false information and collect adherents.[147]

The roles that Parler and Facebook played in the January 6, 2021, rally and attack of the U.S. Capitol show the essentialness of large platforms in disseminating speech into mainstream public discourse. Though Parler contributed to the January 6th attack by giving users with similar views a place to initially meet and discuss, its twelve million total users is minuscule compared to the immense size of Facebook (200 million American users, including 70% of American adults), [148] the use of which allowed coordinators to organize at the necessary scale.[149] Over 100,000 Facebook users posted content affiliated with causes that prompted the Capitol rally,[150] along with at least seventy Facebook groups dedicated to similar causes such as "Stop the Steal."[151] As one leader of a tech watchdog group noted shortly after the attack, "[i]f you took Parler out of the equation, you would still almost certainly have what happened at the Capitol . . . If you took Facebook out of the equation before that, you would not."[152] In an extensive report analyzing Facebook users and posts, a collaboration of tech-focused organizations concluded not only that Facebook bears "significant responsibility" for January 6th events, but also found that "Facebook, with its vast reach, remains

---

145. Elizabeth Culliford & Jeffrey Dastin, *Parler CEO Says Social Media App, Favored by Trump Supporters, May Not Return*, REUTERS (Jan. 13, 2021), https://www.reuters.com/technology/exclusive-parler-ceo-says-social-media-app-favored-by-trump-supporters-may-not-2021-01-13/ [https://perma.cc/8C48-LQ4Y].

146. *See* Gilad Edelman, *Twitter Cracks Down on QAnon. Your Move, Facebook*, WIRED (July 22, 2020), https://www.wired.com/story/twitter-cracks-down-qanon-policy/ [https://perma.cc/7SSK-QXYJ].

147. *Id.*

148. *Countries with The Most Facebook Users 2021*, STATISTA (Sept. 10, 2021), https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/ [https://perma.cc/QC6M-YJMR]; *see also* Josh Gramlich, *10 Facts About Americans and Facebook*, PEW RSCH. CTR. (June 1, 2021), https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/ [https://perma.cc/HU32-ZCK5].

149. *See* Igor Derysh, *Despite Parler Backlash, Facebook Played Huge Role in Fueling Capitol Riot, Watchdogs Say*, SALON (Jan. 16, 2021), https://www.salon.com/2021/01/16/despite-parler-backlash-facebook-played-huge-role-in-fueling-capitol-riot-watchdogs-say/ [https://perma.cc/LZ4Q-ZHC6].

150. Elizabeth Dwoskin, *Facebook's Sandberg Deflected Blame for Capitol Riot, but New Evidence Shows How Platform Played Role*, WASH. POST (Jan. 13, 2021), https://www.washingtonpost.com/technology/2021/01/13/facebook-role-in-capitol-protest/ [https://perma.cc/576E-JR4J].

151. Kayla Gogarty, *"Stop the Steal" Organizers Used Facebook and Instagram to Promote Events*, MEDIA MATTERS (Jan. 12, 2021), https://www.mediamatters.org/january-6-insurrection/stop-steal-organizers-used-facebook-and-instagram-promote-events-including [https://perma.cc/2H4B-CBM7].

152. Derysh, s*upra* note 149.

an unparalleled organizing tool for right-wing groups, despite recent moves by many Trump supporters to embrace ideological fringe sites like Parler…"[153] That users of smaller platforms need to operate on larger ones in order to effectively organize should cause policy makers to hesitate before regulating those smaller platforms. If policy makers can prevent societal-wide harm such as the public discourse that led to the January 6th attack by selectively removing section 230 immunity only larger platforms, as opposed to almost all social media services, then for the competitive and economic reasons discussed above they should do so.[154]

The 50 million MAU criteria would allow new firms to grow without worrying about being run out of business due to legal costs, thereby helping to maintain the competitive environment section 230 seeks to promote. Multiple legislative proposals include a minimum threshold number of MAUs, and at least one specifically uses 50 million MAUs as the metric.[155] The 50 million threshold ensures the most-used platforms currently would be within the scope of any enacted reforms; not only are Facebook, Twitter, and Reddit included, but so are lesser-known platforms such as Discord and Quora.[156]

b. Limiting Reforms to Platforms with Over 50 Million Monthly Active Users Protects Competition

Exempting smaller platforms with less than $500 million in annual revenue also supports the original purpose of section 230 to "preserve the vibrant and competitive free market" by protecting new entrants from existentially-threatening legal costs.[157] More businesses in an industry leads to greater competition, and lower entry costs, such as legal fees, leads to more businesses.[158] In turn, greater competition leads to more innovation, productivity, and a growing economy.[159] Five hundred million dollars may seem to be a high bar, but online companies are often global enterprises, and

153. TECH TRANSPARENCY PROJECT, JANUARY 6TH: AN INSURRECTION FUELED BY FACEBOOK 65 (Feb. 2, 2021), https://accountabletech.org/wp-content/uploads/January-6th-An-Insurrection-Fueled-by-Facebook.pdf [https://perma.cc/YLH3-JAQM].

154. *See supra* Part III, Section A.

155. Reps. Eshoo and Malinowski Introduce Bill to Hold Tech Platforms Liable for Algorithmic Promotion of Extremism, *supra* note 101; Online Freedom and Viewpoint Diversity Act, S. 4534, 116th Cong. (2020); Limiting Section 230 Immunity to Good Samaritans Act, S. 3983, 116th Cong. (2020).

156. Werner Geyser, *Discord Statistics: Revenue, Users & More*, INFLUENCER MARKETING HUB (Sept. 1, 2021), https://influencermarketinghub.com/discord-stats/ [https://perma.cc/4M6Y-EZDP]; *see also* Theodore Schleifer, *Yes, Quora Still Exists, and It's Now Worth $2 Billion*, RECODE (May 16, 2019), https://www.vox.com/recode/2019/5/16/18627157/quora-value-billion-question-answer [https://perma.cc/5BPY-3N38].

157. 47 U.S.C. § 230(b)(2); *see also* KOSSEFF, *supra* note 3, at 175-78.

158. *See* WU & ATKINSON, *supra* note 82, at 6, 29, 53.

159. *Id.* at 6.

this standard captures at least the largest ninety-four online businesses.[160] Firms with fewer financial resources have less ability to absorb compliance costs, along with unpredictable settlements or damages arising from lawsuits. In contrast, the largest social media companies employ tens of thousands of people to monitor and moderate content.[161] Facebook alone pays for 15,000 workers to monitor its social media posts, and critics argue the company needs to double that in order to be effective.[162] Smaller companies may not be able to meet heightened monitoring and moderation obligations in an environment without section 230 immunity. Even when scaled down to adjust for smaller user bases, the cost of extra employees can be significant or even fatal for smaller or new online platforms.

As discussed above, reactions by companies to the passage of FOSTA shows how increasing legal liability can lead to less competition and consolidate the marketplace in favor of larger incumbent firms. After Congress passed FOSTA, smaller companies shut down dating-related services or even went out of business.[163] On the other hand, Facebook, which has over $85 billion in annual revenue and had lobbied for FOSTA's passage, launched its own dating service just a few weeks later while its competitors in the online dating space began to fold.[164] Though Facebook does not release the number of users who participate in the dating service, the timing suggests that Facebook decisionmakers understood FOSTA could force competitors to leave the online-romance market and could therefore open a profitable avenue for the wealthy company that could withstand liability costs.[165]

The potential for section 230 reforms to limit competition and consolidate the market highlights the danger that not exempting smaller companies can give "Big Tech" even more power over public discourse and its users. Such market consolidation of the social media sector would only serve to prevent competitors, perhaps those with innovative platforms or services, improved algorithms, effective moderation tools, or meaningful content-guidelines policies that reduce perceived political bias, from displacing or reducing the influence of companies that run large social media platforms.

---

160. *List of Largest Internet Companies*, WIKIPEDIA, https://en.wikipedia.org/wiki/List_of_largest_Internet_companies [https://perma.cc/7D9K-LE9H].

161. *See* Elizabeth Dwoskin, Jeanne Whalen, & Regine Cabato, *Content Moderators at YouTube, Facebook and Twitter See the Worst of the Web - and Suffer Silently*, WASH. POST (July 25, 2019), https://www.washingtonpost.com/technology/2019/07/25/social-media-companies-are-outsourcing-their-dirty-work-philippines-generation-workers-is-paying-price [https://perma.cc/PW5J-7CBA].

162. Charlotte Jee, *Facebook Needs 30,000 of Its Own Content Moderators, Says a New Report*, MIT TECHNOLOGY REV. (June 8, 2020), https://www.technologyreview.com/2020/06/08/1002894/facebook-needs-30000-of-its-own-content-moderators-says-a-new-report/ [https://perma.cc/NJR2-ZFCW].

163. *See* Allow States and Victims to Fight Online Sex Trafficking Act of 2017, H.R. 1865, 115th Cong. (2018) (codified at 47 U.S.C. § 230(e)(5)).

164. Harmon, *supra* note 129; *see also Facebook Company Profile*, FORTUNE (Aug. 2, 2021), https://fortune.com/company/facebook/fortune500/.

165. *See* Harmon, *supra* note 136.

Providing regulatory relief for smaller businesses is common in the United States, as lower-revenue businesses are disproportionately impacted by fixed costs of regulation, the consequences of non-adherence to regulations can be smaller, and policy makers often support entrepreneurship.[166] When Congress passed the Small Business Regulatory Enforcement Fairness Act, it recognized that "small businesses bear a disproportionate share of regulatory costs and burdens."[167] Federal agencies can reduce or waive civil penalties for small businesses that violate statutory or regulatory requirements.[168] Agencies must also review regulations to ensure they do not "unduly inhibit the ability of small entities to compete."[169] Minimum wage laws and health insurance requirements for employers are just some of the other ways the law holds smaller firms to more lenient regulatory standards.[170] Only applying section 230 reforms to larger companies would follow this tradition of permitting new firms to grow and flourish before complying with regulations designed to curb actions of large-scale actors.

IV. CONCLUSION

The central concern of many section 230 reformers is to reign in the power that large social media companies with massive number of users and annual revenue exercise over society. In attempting to curb these perceived abuses, Congress should *encourage*, not inhibit the ability of, new and small firms to compete against the larger companies and platforms. Congress can promote such competition by only removing section 230 immunity for the larger companies and platforms most responsible for the perceived harms. While the modern Internet economy has drastically changed since Congress passed section 230, the importance of the free and open Internet to drive competition and innovation has not changed. By narrowing any removal of section 230 immunity to large companies that operate social media platforms with large user bases, Congress can ensure the primary aims of the reforms are met while not overburdening smaller and newer firms that can compete against the largest online companies.

---

166. *See* SUSAN M. GATES & KRISTIN J. LEUSCHNER, IS SPECIAL REGULATORY TREATMENT FOR SMALL BUSINESSES WORKING AS INTENDED? (2007), https://www.rand.org/pubs/research_briefs/RB9298.html#:~:text=Small%20businesses%20are%20a%20critical,percent%20of%20net%20new%20jobs [https://perma.cc/KS6W-LSF8]; *see also* WU & ATKINSON, *supra* note 82.

167. Small Business Regulatory Enforcement Fairness Act of 1996, Pub. L. No. 104-121, § 202, 1996 U.S.C.C.A.N. (110 Stat.) 847 (codified at 5 U.S.C. § 601).

168. *See id.* § 223(a).

169. Letter from Sanford S. Williams, Federal Communications Commission to Government Attic 7 (March 7, 2017), https://www.governmentattic.org/26docs/FCC-MRF2016-SECGM2009.pdf [https://perma.cc/856B-4HL4].

170. *See* Jeanne Sahadi, *Many Low-wage Workers Not Protected by Minimum Wage*, CNN (Apr. 23, 2014), https://money.cnn.com/2014/04/23/smallbusiness/minimum-wage-exemptions/index.html [https://perma.cc/Q2CF-C5ZL]; *see also* GATES & LEUSCHNER, *supra* note 166.

Stitching a Privacy Patchwork Together—for Now: The Constitutionality of State Privacy Regulations Under the Dormant Commerce Clause

Michael DeJesus*

TABLE OF CONTENTS

---

* Michael DeJesus is currently a J.D. Candidate at the George Washington University Law School with an expected graduation date of May 2022. Previously, he has interned at AARP Foundation Litigation, Government Accountability Project, and the CFTC Whistleblower Office. Prior to law school, he was the Public Interest Advocacy Fellow at Taxpayers Against Fraud Education Fund and graduated from American University in 2017.

I. INTRODUCTION

Commentators once hailed the Internet as a force for democratization and freedom, and many had overwhelmingly positive opinions about large technology companies like Google and Facebook—but now, attitudes have shifted drastically, decrying the extent of both state and corporate surveillance.[1] Americans now harbor little trust for large technology companies, and view the Internet as threatening personal privacy: over three out of five Americans say it is "not possible to go through daily life without" either business or the government "collecting data about them."[2] Shifting public attitudes and a newfound concern over privacy have led consumer data privacy advocates to call for consumer protection regulations.

Some advocates look to the European Union's (E.U.) General Data Protection Regulation (GDPR) as a model. But with the U.S. Congress rejecting FCC regulations governing Internet-service provider (ISP) use of consumer data as recently as 2017, consumer data privacy advocates have now focused their efforts on protecting consumers at the state level.[3] Amidst this push, detractors have claimed that a regime of "patchwork privacy" would tear asunder the original liberating impact of the Internet, and would raise nigh-impossible regulatory barriers for the next wave of digital entrepreneurs. They claim state data privacy regulations would simply contribute to the corporate consolidation that many consumer advocates seek to prevent and stymie innovation, without meaningfully protecting consumer

---

1. *See, e.g.,* Astra Taylor, *How the Internet Is Transforming from a Tool of Liberation to One of Oppression*, HUFFINGTON POST (Aug. 4, 2014), https://www.huffpost.com/entry/internet-oppression-liberation_b_5449838; Nicholas Carr, The World Wide Cage, AEON (Aug. 26, 2020), https://aeon.co/essays/the-internet-as-an-engine-of-liberation-is-an-innocent-fraud [https://perma.cc/VB2Q-92VJ].

2. BROOKE AUXIER ET AL., AMERICANS AND PRIVACY: CONCERNED, CONFUSED AND FEELING LACK OF CONTROL OVER THEIR PERSONAL INFORMATION 2 (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/6F64-SZUW].

3. *See* Glenn G. Lammi, Washington Legal Foundation, *The Nullification of FCC's Broadband Privacy Rules: What It Really Means for Consumers*, FORBES (Apr. 12, 2017), https://www.forbes.com/sites/wlf/2017/04/12/the-nullification-of-fccs-broadband-privacy-rules-what-it-really-means-for-consumers/?sh=7f1f99a779ba (acknowledging that consumer advocates were opposed to the move on the grounds that it allowed Internet service providers to collect and sell consumer personal information) [https://perma.cc/2QKX-2TUS]; *see also* Brian Fung, *What to Expect Now that Internet Providers Can Collect and Sell Your Web Browser History*, WASH. POST (Mar. 29, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/29/what-to-expect-now-that-internet-providers-can-collect-and-sell-your-web-browser-history/ (noting that congressional action prevented Internet privacy protections from taking effect that "would have would have banned Internet providers from collecting, storing, sharing and selling certain types of personal information — such as browsing histories, app usage data, location information and more — without [consumer] consent") [https://perma.cc/UY44-P7C4].

privacy.[4] Particularly, they claim state action in this area violates the dormant commerce clause.[5]

But policymakers should not fear patchwork privacy in the face of federal inaction. Instead, they can embrace state-level data privacy legislation as the natural byproduct of federalism. The likely constitutionality of stringent measures like the California Consumer Privacy Act (CCPA), and its successor, the California Privacy Rights Act (CPRA), suggests even the most robust state-level consumer privacy protections do not run afoul of the dormant commerce clause. Accordingly, absent federal action, state legislatures may take the task of consumer data protection upon themselves.

In Section II, I discuss why policymakers might embrace a "patchwork privacy" regime in the face of federal inaction. In Section III, I discuss why the dormant commerce clause does not preclude even the most sweeping state-level consumer data privacy laws, adopting the CCPA as the main statute of focus. Then, in Section IV, I review the different forms of consumer privacy laws at the state level and consider how arguments about the CCPA's constitutionality under the dormant commerce clause might apply. I conclude in Section V by discussing how state consumer data privacy laws might interplay with potential federal regulations in the future, and by recapping the practical necessity of leaning on the states as "laboratories of democracy" at this moment.

II. AMERICANS HAVE LITTLE TO FEAR FROM "PATCHWORK PRIVACY"

Many practitioners and commentators caution against embracing a "patchwork privacy" regulatory framework. Their opposition is rooted in the notion that "the [I]nternet requires a uniform system of regulation," and that state restrictions would tear the "free flow of digital information" asunder.[6] Others have pointed out that patchwork privacy might lead to genuine confusion among consumers and entrepreneurs over which law governs their conduct, and erode Americans' confidence that their personal data will be

4. Jennifer Huddleston, *The Problem of Patchwork Privacy*, TECHNOLOGY LIBERATION FRONT (Aug. 15, 2018), https://techliberation.com/2018/08/15/the-problem-of-patchwork-privacy (arguing "these type of statutes are likely to impact innovation in a misguided attempt to correct issues with data privacy…[and] also unintentionally make it more difficult for small, local companies to compete with Internet giants") [https://perma.cc/Q9TL-7YGC].

5. *See* Jennifer Huddleston & Ian Adams, *Potential Constitutional Conflicts in State and Local Data Privacy Regulations*, REGUL. TRANSPARENCY PROJECT (Dec. 2, 2019), https://regproject.org/paper/potential-constitutional-conflicts-in-state-and-local-data-privacy-regulations/ [https://perma.cc/XD9Q-DKAC].

6. *Id.*

secure.[7] Opponents of state-led action claim also that the regulatory patchwork has little upside for consumers, merely causing a "drag" on the economy, "creat[ing] operational inefficiencies[,] and distort[ing] interstate markets."[8]

However, Americans want their representatives to act. In a 2019 Pew Research Center survey, approximately 75% of Americans expressed support for increased government regulation of how companies handle consumer personal information.[9] So long as Americans' privacy rights and interests remain unprotected at the federal level, state legislators can act to protect their constituents' privacy. Notably, legislators in California passed the CCPA and had it signed into law by the governor in 2018, with the law coming into effect in 2020.[10] Subsequently, California voters passed the CPRA in November 2020, strengthening protections in the CCPA and creating a Privacy Protection Agency to enforce the law.[11]

Not all state consumer data privacy regulations will be perfect or optimal policy. For instance, there are legitimate criticisms of the marginal costs that the CCPA imposes on growing and capitalizing technology companies. However, these legitimate criticisms do not prevent states from taking action to protect their residents now while federal legislation remains elusive.

A. Policymakers Must Deal with the Internet as It Is, Not as They Would Like It to Be—and that Means Embracing Patchwork Privacy in the Interim

Though the Internet was once popularly conceived as a "digital wild west" of innovation, entrepreneurship, and social experimentation, many commentators now claim the Internet is subject to the same institutional

---

7. Michael Beckerman, *Americans Will Pay a Price for State Privacy Laws*, N.Y. TIMES (Oct. 14, 2019), https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html (claiming "[a] patchwork of state laws means that a California woman who orders an item from a Missouri business that manufactures in Florida could have her data regulated by three separate laws, or by no applicable law… [this] will also undoubtedly lead to inconsistent treatment of data… Americans cannot be confident that their data remains protected as they travel from state to state") [https://perma.cc/KZJ5-8QP2].

8. Boyd Garriott et al., *The Case for Uniform Standards Grows as States Sew More Laws into Patchwork of Data-Privacy Regulations*, WASH. LEGAL FOUND., Sept. 27, 2019, https://www.wlf.org/wp-content/uploads/2019/09/09272019GarriottBrownWeeks_LB.pdf [https://perma.cc/B8ZL-GABZ].

9. *See* AUXIER ET AL., *supra* note 2, at 43.

10. Tim Peterson, *Why California's New Consumer Privacy Law Won't Be GDPR 2.0*, DIGIDAY (July 9, 2018), https://digiday.com/marketing/californias-consumer-privacy-law-has-digital-ad-industry-searching-for-answers/ [https://perma.cc/2EB3-58XK].

11. Sara Morrison, *California Just Strengthened Its Digital Privacy Protections Even More*, VOX (Nov. 4, 2020, 12:06 PM), https://www.vox.com/2020/11/4/21534746/california-proposition-24-digital-privacy-results [https://perma.cc/D7VL-J5GC].

sclerosis and consumer rights concerns as the wider economy.[12] Technology companies' claim that sectoral self-regulation is necessary for the open Internet is a claim under increasingly rigorous scrutiny. [13] Policymakers are increasingly moving past the notion "that government intervention would be costly and counterproductive" instead, they are embracing it as a tool.[14]

Patchwork privacy may not be the optimal solution for protecting American consumers or regulating an Internet economy. But thus far, attempts to address the issue legislatively have failed on the federal level. Despite legislators' recognition of the issue, Republicans and Democrats remain unable to marry competing bills, with over thirty bills filed since the election in 2018.[15] Perhaps one of the most serious bipartisan pushes for a federal privacy law recently ended in failure. Senior members on the Senate Committee on Commerce, Science, and Transportation who engaged in bipartisan negotiations failed to produce a bipartisan bill and instead released two separate proposals, with the ranking Republican member proposing the United States Consumer Data Privacy Act (USCDPA) and the ranking Democrat proposing the Consumer Online Privacy Rights Act (COPRA).[16] Though the Biden Administration instructed the Federal Trade Commission (FTC) to begin writing rules governing consumer surveillance in a July 2021 executive order, the rulemaking process "is expected to take years to complete" and legislative efforts have still "failed to gain traction."[17] Additionally, though the U.S. House Energy and Commerce Committee voted fund a data privacy bureau within the FTC as part of a proposed $3.5 trillion

---

12. Shoshana Zuboff, *You Are Now Remotely Controlled*, N.Y. TIMES (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html (describing how technology companies' assurances that "they were capable of regulating themselves and that government intervention would be costly and counterproductive" produced an Internet "operated by private surveillance capital" that takes "behavioral data" and sells it to business customers in the market for "human futures" like targeted online advertising) [https://perma.cc/L657-T6ZB].

13. *See id.* (recounting an "unusually heated" 1997 Federal Trade Commission meeting where technology industry executives vigorously argued against government oversight and disputed civil libertarians' warning that "that the companies' data capabilities posed 'an unprecedented threat to individual freedom'").

14. *Id.*

15. *See* Cameron F. Kerry & Caitlin Chin, *How the 2020 Elections Will Shape the Federal Privacy Debate*, BROOKINGS INST. (Oct. 26, 2020), https://www.brookings.edu/blog/techtank/2020/10/26/how-the-2020-elections-will-shape-the-federal-privacy-debate/ (noting that, in spite of the fact that "the 116th Congress opened with great energy and promise for federal privacy legislation," efforts to pass a bill "fell short" in the wake of the pandemic and "partisan polarization") [https://perma.cc/2BUY-M559].

16. *See id.* (noting "where Chairman Roger Wicker (R-MS) once called for a federal privacy law 'on the books by the end of 2019' and senior members engaged in bipartisan negotiations….[but] [b]y the end of 2019, though, Wicker and Ranking Member Maria Cantwell (D-WA) each released separate proposals").

17. Andrea Vittorio, *Biden's Executive Order Links Data Collection to Competition*, BLOOMBERG L. (July 9, 2021, 4:17 PM), https://news.bloomberglaw.com/privacy-and-data-security/bidens-executive-order-links-data-collection-to-competition [https://perma.cc/C99P-B78X].

domestic policy bill, recent negotiations show a much smaller package is being considered in the Senate and the fate of the proposal is unclear.[18]

Because comprehensive legislation to protect American consumers' privacy rights at the federal level continues to elude proponents, state-level protections are an avenue for protecting consumer data privacy rights in the interim. States have long been recognized as "laboratories of democracy," and have stepped in where the federal government has failed to act. Differing policy approaches towards issues as disparate as marijuana legalization and election regulations have been recognized as an outgrowth of this federalist tradition.[19]

U.S. states' action on privacy is not limited to the patchwork of data breach regulations—rather, states have acted in a number of other pressing areas where federal policy is lacking or nonexistent. Commentators in favor of state action note that "[s]tates have been the source of numerous privacy innovations," favorably citing: "laws on identity theft victim rights, data breach notification, limitations on the use of Social Security numbers, cell phone data privacy, cybersecurity, and cyber-exploitation (sometimes known as 'revenge porn')."[20] These proponents of state action acknowledge that harmonization of competing standards would be ideal, but still recognize these varied policies as "innovative" in the interim.[21]

The patchwork of data breach notification regulations is a counterpoint to those detractors who suggest that state-level regulation only leads to insurmountable regulatory hurdles for business. All fifty U.S. states—as well as the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands—have laws requiring that both public and private entities notify consumers of security breaches that disclose personally identifying information.[22] Though commentators do rue the lack of regulatory consistency and call for the implementation of a national standard, these calls are not accompanied by demands for rolling back all state data breach notification laws in the absence

---

18. *See* Diane Bartz, *U.S. Panel Votes to Approve $1 Billion for FTC Privacy Probes*, REUTERS (Sept. 14, 2021, 7:38 PM), https://www.reuters.com/business/us-panel-votes-approve-1-billion-ftc-privacy-probes-2021-09-14/; Emily Cochrane, *Democrats Are Courting Manchin on Their Agenda. Here's What He Wants*, N.Y. TIMES (Oct. 20, 2021), https://www.nytimes.com/2021/10/18/us/politics/democrats-manchin-domestic-policy-bill.html (noting that Senator Joe Manchin (D-W.V.) "does not want the bill to cost more than $1.5 trillion over the course of a decade…") [https://perma.cc/B6FH-BMK5].

19. *See, e.g.*, Tom Keane, *An Experimental State*, BOS. GLOBE (Jan. 7, 2014), https://www.bostonglobe.com/opinion/2014/01/07/colorado-pot-experiment-testament-founding-fathers/pvUGE1H8lOYktyKzFL1xnL/story.html (calling Colorado's legalization of marijuana a manifestation of states acting as "laboratories of democracy") [https://perma.cc/K4QE-QHGU]; Mark Schmitt et al., *Electoral Systems*, NEW AMERICA, https://www.newamerica.org/in-depth/laboratories-of-democracy/electoral-systems/ (providing information on different states' electoral systems in a wider "Laboratories of Democracy" database) [https://perma.cc/4CD2-637C].

20. Joanne McNabb, *Can Laboratories of Democracy Innovate the Way to Privacy Protection?*, CENTURY FOUND. (Apr. 5, 2018), https://tcf.org/content/report/can-laboratories-democracy-innovate-way-privacy-protection [https://perma.cc/7EM2-7BUU?type=image].

21. *Id.*

22. *Security Breach Notification Laws*, NAT'L CONF. STATE LEGISLATURES, https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/VD3M-XSQC].

of a federal alternative.[23] The patchwork of data breach notification laws has not led to economic ruin or raised impossible hurdles to compliance. Sometimes a subpar regulatory framework is better than the complete lack of one. In the case of data breach laws, states chose to adopt regulation lest consumers suffer from the potential harm of identity theft.[24]

B. The Federal Government Has Declined to Intercede in this Area for the Benefit of American Consumers

The 2017 nullification of the FCC rule governing ISP handling of consumer data, and the FCC's lack of preemption authority over state and local regulation, show that the federal government has thus far failed to act to protect American consumers. The present lack of clear federal guidelines governing the handling of consumers' personal data should not mean that consumers remain unprotected. Indeed, both prior federal action and federal court rulings suggest that—barring a comprehensive law passed by Congress—states can and should provide protection for their resident consumers.

1. The 2017 Nullification of FCC Rules Governing ISP Handling of Consumer Data Illustrate that the Federal Government Is Currently Unable to Safeguard Americans' Privacy

The federal government's inability, so far, to act decisively to protect consumer data privacy is illustrated by the 2017 nullification of FCC regulations under the Congressional Review Act, which allows Congress to repeal federal regulations and prevent the issuing agency from promulgating similar regulation at later date with the approval of the President.[25] The repeal scrapped previously promulgated 2016 FCC regulations which would have required Internet service providers "to obtain consumer consent before using precise geolocation, financial information, health information, children's information and web browsing history for advertising and marketing."[26]

---

23. *See, e.g.*, Joseph Marks, *Equifax Breach Prompts Renewed Calls for National Breach Notification Standard*, NEXTGOV (Sept. 18, 2017), https://www.nextgov.com/cybersecurity/2017/09/equifax-breach-prompts-renewed-calls-national-breach-notification-standard/141098/ (noting policymakers' support for national standard in data breach notification without their contesting the necessity of state-level regulations in the interim) [https://perma.cc/74MC-L67S].

24. Fabio Bisogni & Hadi Asghari, *More Than a Suspect: An Investigation into the Connection Between Data Breaches, Identity Theft, and Data Breach Notification Laws*, J. INFO. POL'Y, 2020 at 46, https://doi.org/10.5325/jinfopoli.10.2020.0045 [https://perma.cc/3W57-8HJW].

25. Kelly Ding, *Congress Rolls Back FCC Broadband ISP Privacy Rules*, JOLT DIGEST (Apr. 04, 2017), https://jolt.law.harvard.edu/digest/congress-rolls-back-fcc-broadband-isp-privacy-rules [https://perma.cc/9FTL-WWU8].

26. David Shepardson, *Trump Signs Repeal of U.S. Broadband Privacy Rules*, REUTERS (Apr. 3, 2017, 7:50 PM), https://www.reuters.com/article/us-usa-internet-trump-idUSKBN1752PR [https://perma.cc/6PEL-PQVH].

Proponents hailed their repeal, while ruing how the regulations were supposedly, according to then-FCC Chairman Ajit Pai, originally intended to "benefit one group of favored companies, not online consumers."[27]

But with repeal of the regulations, consumers' personal data is even less protected, and both groups of businesses may merely sell it to the highest bidder. Instead, Internet service providers can "monitor their customers' behavior online and, without their permission, use their personal and financial information to sell highly targeted ads."[28] And consumer privacy advocates appropriately have noted that "although consumers can easily abandon sites whose privacy practices they don't agree with, it is far more difficult to choose a different Internet provider" given the paucity of options throughout the U.S.[29]

2. Because the Current Internet Regulatory Framework Is Inadequate for Establishing Consumer Protection Online, the States Should Act Where There Is No Clear Prohibition

The federal government has also ceded overarching national regulatory authority over the Internet in other respects. Notably, the courts have struck down expansive arguments by regulatory agencies that, with or without explicit statutory authority, federal regulations can preempt state or local action in certain circumstances. For instance, courts have stated that the FCC does not have overarching authority to preempt all state regulation of communications.[30]

The decision in *Mozilla Corp. v. Fed. Commc'ns Comm'n*, 940 F.3d 1 (D.C. Cir. 2019), is illustrative. Petitioners in *Mozilla* brought suit challenging a 2018 FCC order that reclassified broadband Internet access as an "information service," as opposed to its prior classification as a "telecommunications service" under the 1996 Telecommunications Act.[31] They also sought to strike down its Preemption Directive, which sought to "bar[] states from imposing any rule or requirement that the FCC repealed or

---

27. *See id.*

28. Brian Fung, *The House Just Voted to Wipe Away the FCC's Landmark Internet Privacy Protections*, WASH. POST (Mar. 28, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/the-house-just-voted-to-wipe-out-the-fccs-landmark-internet-privacy-protections/ [https://perma.cc/9K5F-R86M].

29. *See id.* (noting "[m]any Americans have a choice of only one or two broadband companies in their area, according to federal statistics").

30. Louisiana Pub. Serv. Comm'n v. FCC, 476 U.S. 355, 373-74 (1986) (stating that "[a]lthough state regulation will generally be displaced to the extent that it stands as an obstacle to the accomplishment of the full purposes and objectives of Congress, a federal agency may pre-empt state law only when and if it is acting within the scope of its congressionally delegated authority").

31. *See Mozilla*, 940 F.3d at 17 (noting "the 1996 Telecommunications Act creates two potential classifications for broadband Internet: 'telecommunications services' under Title II of the Act and 'information services' under Title I").

decided to refrain from imposing in the Order or that is "more stringent" than the Order."[32]

The Court of Appeals for the D.C. Circuit sided with petitioners with respect to the Preemption Directive, finding the FCC lacked the express or ancillary authority necessary to issue the order.[33] The court also rejected the FCC's assertion that a "statement of policy" in 47 U.S.C. § 230(b)(2) stating "the policy of the United States [is] . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation" conferred the necessary authority.[34] The court took care to note that conflict preemption is "fact-intensive" and only applies when "actual preemption of a specific state regulation occurs."[35] The court further declined to find that the principle of conflict preemption justified issuance of the Preemption Directive, because "[w]ithout the facts of any alleged conflict before us, we cannot . . . [make] a categorical determination that any and all forms of state regulation of intrastate broadband would inevitably conflict with the 2018 Order."[36] It noted that the FCC's 2018 Order survived without blanket application of the preemption doctrine to uphold the Preemption Directive, and that the doctrine could still be invoked on a case-by-case basis as originally intended.[37]

The lack of concerted federal legislation in this area shows the federal government has been dilatory in protecting a key interest in the twenty-first century: the Internet privacy rights of American consumers. Proponents of state consumer data privacy initiatives should heed the D.C. Circuit's ruling. *Mozilla* underscores the ability of states to regulate telecommunications where there is no federal statute controlling. In light of *Mozilla*, states—and even local governments—can now identify areas where the federal government has not yet trod, and can take action on their own behalf in response to constituent calls for additional regulation. However, state policymakers should still remain aware that, though the FCC lacks categorical preemption authority in the Order, *Mozilla* does not preclude state-level regulations from being struck down on a case-by-case basis. At this point, courts have not yet opted to do so, and are loathe to find preemption "absent an actual conflict."[38]

---

32. *Id.* at 18 (internal quotations omitted).
33. *Id.* at 75.
34. *Id.* at 78 (quoting 47 U.S.C. § 230(b)(2)).
35. *Id.* at 81-82.
36. *Id.* at 82.
37. *See id.* at 85 (stating "[i]f the [FCC] can explain how a state practice actually undermines the 2018 Order, then it can invoke conflict preemption. If it cannot make that showing, then presumably the two regulations can co-exist as the Federal Communications Act envisions") (citing 47 U.S.C. § 152(b)).
38. *See* ACA Connects - Am.'s Commc'ns Ass'n v. Frey, 471 F. Supp. 3d 318, 324-26 (D. Me. 2020) (citing Eng. v. Gen. Elec. Co., 496 U.S. 72, 90 (1990)) (rejecting defendant's argument that the State of Maine's consumer data privacy law was preempted by Congress's 2016 abrogation of FCC rules or by the FCC's own RIF order, noting that there is a "strong presumption against implied federal preemption of state law" and that preemption "cannot be a 'mere byproduct of self-made agency policy.'" (quoting *Mozilla*, 940 F.3d at 78)).

C. Proponents of a State "Patchwork" of Data Privacy Regulations Must Grapple with Arguments That These Efforts Violate the Dormant Commerce Clause

Opponents also argue that a regulatory patchwork is not only inefficient, but a violation of the dormant commerce clause. Thus far, the majority of opponents' claims of unconstitutionality have been focused on one piece of consumer data privacy legislation: the CCPA. Many seek to strike down the law due to its "broad, sometimes unclear" language that opponents maintain makes compliance difficult.[39] Other commentators take a broader view of what the CCPA presages for the future of consumer data privacy regulation across the United States. Some fear that similarly comprehensive laws across the country would create an inconsistent patchwork "with different requirements . . . so contradictory that it would be impossible to comply with every state."[40]

Opponents are likely to intensify their efforts with the recent 2020 passage of the CRPA at the ballot box, which clarifies the scope of and expands the protections in the CCPA.[41] The onset of CRPA regulations in 2023—a whole three years after the November 2020 ballot initiative passing it and just after "the ink was barely dry on the CCPA"—underscores how the regulatory environment is in flux.[42] The new regulatory standards in the CRPA are both intended to increase protections for individuals that consumer advocates thought were lacking, and to further harmonize with the higher standards in the E.U. GDPR.

Passage of the CRPA imposes even more stringent checks on businesses in the name of consumer data privacy. The CRPA has been recognized as "the strictest data privacy law in the U.S.," and was intentionally designed to "draw[] on many key aspects of the [E.U.'s]

---

39. *See* Jonathan Ende, *Though CCPA Is Now Live, Questions Concerning Its Constitutionality Linger*, JD SUPRA (Jan. 10, 2020), https://www.jdsupra.com/legalnews/though-ccpa-is-now-live-questions-76600/ [https://perma.cc/7G2F-NWW4].

40. Jennifer Huddleston, *The State of State Data Laws, Part 2: Consumer Data Privacy Legislation*, MERCATUS CTR. (Aug. 6, 2019), https://www.mercatus.org/bridge/commentary/state-state-data-laws-part-2-consumer-data-privacy-legislation (paraphrasing May 2019 Congressional testimony from Commissioner Christine S. Wilson of the Federal Trade Commission) [https://perma.cc/NL98-RVUX].

41. *See CPRA Rivals GDPR's Privacy Protections While Emphasizing Consumer Choice*, AKIN GUMP STRAUSS HAUER & FELD LLP (Nov. 11, 2020), https://www.akingump.com/en/news-insights/cpra-rivals-gdprs-privacy-protections-while-emphasizing-consumer-choice.html (noting that "new CPRA made its way to the November 2020 ballot…" after consumer advocates were "disheartened by the number of statutory amendments proposed by 'special interests' after the CCPA was enacted and the potential that such amendments could eviscerate the statute's key privacy protections") [https://perma.cc/3QEH-U6EZ].

42. *See id.* (stating that "businesses [are] grappl[ing] with the CPRA and prepar[ing] for the majority of the provisions to become operative in 2023…").

GDPR."[43] Though the CRPA raised the threshold application of California privacy law to those businesses serving California residents from 50,000 to 100,000, it also increased other privacy protections for businesses in a manner likely to raise opponents' ire.[44] For instance, the CRPA expands on all consumer rights previously in the CCPA and includes a new right to rectification of incorrect personal data, and a new right to "limit [the] use of disclosure of sensitive personal information."[45] The new Act also increases the fine on businesses that divulge the personal information of minors, and expands consumers' private right of action against noncompliant businesses to include breaches of email addresses, passwords, and security questions.[46]

The measure's originators recognized that detractors might seek to curb some of the regulation's more stringent requirements either in text or in enforcement. Notably, the CRPA also imposes a "one-way ratchet" intended to prevent the measure from being watered down by the California state legislature: though the legislature can impose additional amendments that benefit consumers with a simple majority vote, the CRPA requires that all amendments "enhance privacy and are consistent with and further the purposes and intent of the Act."[47] Yet, perhaps one of the most notable facets of the law is its creation of the California Privacy Protection Agency—the first agency dedicated to consumer privacy in the U.S., and one that consumer advocates have hailed as "a major milestone."[48]

Both the scope of CCPA and CRPA protections and the prospect of similarly broad protections being extended to consumers state-by-state have engendered substantial warnings from commentators. According to opponents of state-level regulation, "[r]egulation of the [I]nternet is inherently cross-jurisdictional."[49] Opponents contend that mandated "changes to the [regulatory] system for out-of-state platforms, content creators, and businesses . . . places an undue burden on commerce conducted or created by these entities."[50] They note that California's actions extend throughout the entire country: that the "practical effect" of state data privacy legislation will "affect entire industries and cost hundreds of millions, if not billions, of

---

43. Karen Schuler, *Federal Data Privacy Regulation Is on the Way — That's a Good Thing,*, INT'L ASS'N PRIV. PROS. (Jan. 22, 2021), https://iapp.org/news/a/federal-data-privacy-regulation-is-on-the-way-thats-a-good-thing/ [https://perma.cc/8PY2-SHEJ].

44. *CCPA vs. CPRA – What Has Changed?*, ONETRUST (Nov. 10, 2020), https://www.onetrust.com/blog/ccpa-vs-cpra-what-has-changed/ [https://perma.cc/L382-W4V6].

45. *See id.*

46. *See id.*

47. *See* Cybersecurity, Privacy & Data Protection Alert, *supra* note 41 (citing CPRA, 2020 Cal. Legis. Serv. Prop. 24 § 25).

48. Stacey Gray et al., *California's Prop. 24, the "California Privacy Rights Act," Passed. What's Next?*, FUTURE PRIV. F. (Nov. 4, 2020), https://fpf.org/blog/californias-prop-24-the-california-privacy-rights-act-passed-whats-next/ [https://perma.cc/9LV8-MSG8].

49. Huddleston & Adams, *supra* note 5, at 10 (noting that "[t]he The 2015 Open Internet Order, promulgated by the Federal Communications Commission . . . declared that the [I]nternet is inherently an interstate service") (citing In the Matter of Protecting & Promoting the Open Internet, *Report and Order on Remand, Declaratory Ruling, and Order*, 30 FCC Rcd 5601, para. 431 (2015), https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf).

50. *See* Huddleston, *supra* note 40.

dollars, including affecting business practices and industries not limited to conduct occurring within California."[51] Commentators have also claimed that this state-level legislation is merely an attempt to implement national policy by other means: proponents' framing of the consumer benefit in national terms does not lend weight to the argument that state legislation is intended to predominately benefit state residents.[52]

Opponents of approaching consumer data privacy on a state-by-state basis make legitimate points with respect to efficiency and the onerousness of complying with a wide set of conflicting state standards. However, their contention that these measures are likely unconstitutional under the dormant commerce clause is not necessarily true. Below, I consider how state data privacy regulations should survive the dormant commerce clause test established in *Pike v. Bruce Church*, with a focus on the CCPA as amended by the CPRA.

III. COURTS HAVE PREVIOUSLY UPHELD STATE REGULATIONS OF INTERNET ACTIVITY TOUCHING INTERSTATE COMMERCE, FINDING NO VIOLATION OF THE DORMANT COMMERCE CLAUSE

Previously, courts have upheld the constitutionality of various state statutes regulating Internet activities and have found they do not violate the dormant commerce clause. Accordingly, applying the same test used in *Pike*, courts will likely find that consumer data privacy regulations in the mold of the CCPA and CPRA are constitutionally sound. Though *Pike* originally concerned the burden on interstate commerce imposed by Arizona's onerous labeling requirements for produce grown in-state, in that case, the Court laid out its approach to determining the constitutionality of those state laws which touch interstate commerce.[53]

Though states may pass legislation exceeding their ordinary power under the dormant commerce clause in limited circumstances, it is likely that arguments that the U.S. Congress's abrogation of FCC regulations in 2017 constitute a substantive authorization of state laws on the matter will fail, as "it has long been the rule that Congress must "manifest its unambiguous intent before a federal statute will be read to permit or to approve . . . a violation of

---

51. Alysa Z. Hutnik et al., *Potential Constitutional Challenges to the CCPA*, KELLEY DRYE & WARREN LLP : AD L. ACCESS (Dec. 12, 2019), https://www.adlawaccess.com/2019/12/articles/potential-constitutional-challenges-to-the-ccpa/ [https://perma.cc/EP4H-HDXK].

52. *See, e.g.,* Andrea O'Sullivan, *Are California's New Data Privacy Controls Even Legal?*, REASON (Dec. 17, 2019), https://reason.com/2019/12/17/are-californias-new-data-privacy-controls-even-legal/ (noting "California Attorney General Xavier Becerra… frames his mandate in national terms, stating that 'Americans should not have to give up their digital privacy to live and thrive in this digital age.' That's *Americans*, not Californians") (emphasis in original) [https://perma.cc/Z2VR-P98R].

53. *See generally*, Pike v. Bruce Church, Inc., 397 U.S. 137 (1970).

the Commerce Clause."[54] Nothing in the Congressional Review Act resolution abrogating the standards unambiguously authorizes the states to enact consumer data protection regulation beyond the scope ordinarily provided to the states by the commerce clause.[55]

Under the *Pike* balancing framework, courts consider first whether the law in question facially discriminates against interstate commerce. If the law is not facially discriminatory, then the court considers whether the benefit that inures to state citizens as a result of the regulation is outweighed by the burden the regulation places on interstate commerce.[56] Per the court:

> Where the statute regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits . . . [if] a legitimate local purpose is found, then the question becomes one of degree. And the extent of the burden that will be tolerated will of course depend on the nature of the local interest involved, and on whether it could be promoted as well with a lesser impact on interstate activities.[57]

Notably, California consumer data privacy laws, as set forth in both the CCPA and CPRA, are not facially discriminatory against out-of-state commerce.[58] Accordingly, the analysis of the constitutionality of state consumer data privacy regulations will mainly consider the balancing test in *Pike*: whether the benefit resulting from the legitimate local purpose outweighs the burden imposed on interstate commerce.

Statutes that "impose such rigidity on an entire industry" that they "preserve or secure employment for the home State" are unconstitutional even if that is not their concealed or express purpose.[59] However, "legislation that may cause businesses to decide to conform nationwide conduct to meet the

---

54. Rousso v. State, 204 P.3d 243, 248 (Wash. Ct. App. 2009) (stating that, despite State's contention, federal statutes in question do not constitute evidence of "unambiguous intent" to permit potential violation of Commerce Clause by State's statute regulating online gambling) (citing *Wyoming v. Oklahoma*, 502 U.S. 437, 458 (1992)) (ruling for the respondent on other grounds).

55. *See* S.J. Res. 34, 115th Congress, 131 Stat. 88 (2017) (expressing "congressional disapproval" and providing that FCC regulations governing ISP use of consumer data have no effect).

56. *Pike*, 397 U.S. at 142.

57. *Id.*

58. *See, e.g.*, CAL. CIV. CODE 1798.140(c), (g) (West 2021) (defining some businesses as those satisfying in-state preconditions and defining consumers as "any natural person who is a California resident"); *Proposition 24: California Privacy Rights Act of 2020*, *in* CAL. SEC'Y OF STATE, OFFICIAL VOTER INFORMATION GUIDE 42, 49, https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf (last visited Nov. 16, 2021) (enacted in CAL. CIV. CODE 1798.199.10–.95) (establishing that the CPRA changes the scope of entities covered, but still only applies to businesses that "[do] business in the state of California" and that consumers are "natural person[s] who [are]… . . . California resident[s]") [https://perma.cc/X78C-54MA].

59. *Id.* at 145-46.

requirements of a given state does not necessarily constitute direct regulation of out-of-state commerce."[60] Additionally, courts have also stated that laws which "[do] not compel any action or conduct of the business with regard to" out-of-state businesses do not violate the dormant commerce clause.[61] Courts have previously considered privacy rights of state residents to constitute a sufficiently weighty interest to pass muster, especially when considering other telecommunications regulations, absent an undue burden on interstate commerce.[62] If so, then the law does not violate the dormant commerce clause.

Nonetheless, courts do not hesitate to strike down laws where the purported public benefit to state citizens is clearly outweighed.[63] They afford "less deference to legislative judgment" with respect to local benefits "where the local regulation bears disproportionately on out-of-state residents and businesses."[64] Courts have previously found that state regulations which "substantially increase the cost of such movement" of goods between states may place a burden on interstate commerce that outweighs the benefit provided to the state's citizens.[65] They have also looked unfavorably upon regulations that have a "speculative contribution" to promoting the intended local interest.[66]

A. State Data Privacy Laws Will Likely Pass the Pike Balancing Test, Because Consumer Data Privacy Protections Are a Legitimate Local Benefit

State data privacy laws of similar scope to the CCPA, as amended by the CPRA, will likely pass the *Pike* balancing test. Contrary to detractors' assertions, protecting the privacy of a state's residents is a legitimate local interest recognized by the courts in previous suits, and can be the basis of a successful defense against charges of dormant commerce clause unconstitutionality.

---

60. Ades v. Omni Hotels Mgmt. Corp., 46 F. Supp. 3d 999, 1014 (C.D. Cal. 2014).

61. Kearney v. Salomon Smith Barney, Inc., 137 P.3d 914, 922 (Cal. 2006) (holding that California's two-party consent recording law does not violate the dormant commerce clause because it "would affect only a business's undisclosed recording of telephone conversations with clients or consumers in California . . . [not] with non-California clients or consumers").

62. *See, e.g.*, *Ades,* 46 F. Supp. 3d at 1014 (holding that a California statute prohibiting nonconsensual recordings "has the purpose of preventing privacy harms to Californians" and that effects to interstate commerce were "incidental" even though "it might create incentives for [defendant] to alter its behavior nationwide"); Rezvanpour v. SGS Auto. Servs., Inc., No. 8:14-CV-00113-ODW, 2014 WL 3436811, at *5 (C.D. Cal. July 11, 2014) (declining to grant a defendant's motion to dismiss a claim under a California statute prohibiting nonconsensual recording of communications involving at least one cell phone on the basis it violated dormant commerce clause, in part because defendant lacked extrinsic evidence to prove their claim of being unable to ascertain geographic location of cell phone calls based on area code).

63. Kassel v. Consol. Freightways Corp. of Del., 450 U.S. 662, 671 (1981).

64. *Id.* at 676.

65. Raymond Motor Transp., Inc. v. Rice, 434 U.S. 429, 4457-48 (1978).

66. *Id.* at 447.

Securing residents' personal privacy is not a frivolous concern—rather, courts have recognized it as a legitimate purpose for state legislation.[67] In *Ades*, the court explicitly rejected a defendant's contention that applying a law intended to protect residents' personal privacy rights "provide[d] 'no real benefit whatsoever,'" and underscored that a properly functioning regulatory regime designed to protect privacy implicates "real local interests."[68] A successful challenger would need to provide clear evidence that protecting residents' privacy rights placed an undue burden on interstate commerce, not merely make a factual supposition that this is the case.[69]

Here, the local interests at stake are identical to those in *Zephyr* and *Rezvanpour*: California residents' privacy interests, and state residents' privacy interests more broadly. The CCPA, both alone and as amended by the CPRA, only seeks to regulate the handling of consumer data of those natural persons living in California.[70] If privacy interests are sufficient to justify a California law regulating the recording of telephone conversations including California residents, it makes little sense to exclude the regulation of consumers' personal data on the grounds that personal privacy is insufficiently weighty as to justify *any* burden placed on interstate commerce. The contemporary extent of surveillance is much more comprehensive than contemplated in the California statue. Surreptitious recordings of telephone conversations are merely one way to infringe on residents' privacy. Smartphones, Internet browsers, particular websites, and smartwatches are all collecting vast amounts of personal data that, even if anonymized, can still identify a consumer and make predictions about a consumer if aggregated—providing the unique snapshot of an individual that consumers commonly associate with "social security numbers [and] account numbers."[71] Even

---

67. Zephyr v. Saxon Mortg. Servs., Inc., 873 F. Supp. 2d 1223, 1229 (E.D. Cal. 2012) (observing that the California Supreme Court previously "held that the federal law does not preempt the application of California's more protective privacy provisions… [and] that states could enact more restrictive privacy laws than those imposed by federal law").

68. *See Ades*, 46 F. Supp. 3d at 1015 (C.D. Cal. 2014) (holding that a refusal to apply the law in this instance would "impair the privacy policy guaranteed by California law," that protection of residents' privacy fell under "real local interests," and that the defendant needed evidence to "[show] clearly excessive burdens on interstate commerce") (internal citations omitted).

69. *See, e.g.*, *Zephyr*, 873 F. Supp. 2d at 1231-32 (ruling against defendant because "Saxon has presented no evidence of any particular burden that would compel this Court to conclude that the burden on interstate commerce so outweighed the benefit to California residents"); *see also* Rezvanpour v. SGS Auto. Servs., Inc., No. 8:14-CV-00113-ODW, 2014 WL 3436811, at *5 (C.D. Cal. July 11, 2014) (finding that extrinsic evidence was necessary to prove contention that interest in protecting privacy was outweighed by burden on interstate commerce).

70. *See CPRA Rivals GDPR's Privacy Protections While Emphasizing Consumer Choice*, *supra* note 41.

71. Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today - and How to Change the Game*, BROOKINGS INST. (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ (noting that "aggregation and correlation of data from various sources make it increasingly possible to link supposedly anonymous information to specific individuals and to infer characteristics and information about them ") [https://perma.cc/ERS2-3HXK].

devices connected via the Internet of things (IoT) are now sources of sensitive personal information "just waiting to be mined" or sold.[72] Experts have gone so far as to call our current age the "Golden Age of Surveillance," with the IoT "providing more access than ever in history."[73]

Detractors and defendants may argue that consumers care little about privacy regulations, and that whatever weight the public places on them is outweighed by any burden that protective regulations place on interstate commerce. But in the case of California, residents have made their desires clear. In a November 2020 referendum, over 55.86% of participating eligible voters—over 9.3 million people—voted in favor of passing the CPRA.[74]

In short, standing caselaw suggests that the protection of state residents' privacy is a justifiable, legitimate local benefit in an age of widespread consumer surveillance. Accordingly, state consumer data privacy laws in the mold of the CCPA should pass the portion of the *Pike* inquiry which implicitly requires a legitimate local interest.

B. The Benefit of State Data Privacy Laws Likely Outweighs the Burden on Interstate Commerce

State consumer data privacy legislation in the mold of the CCPA is also likely constitutional under the dormant commerce clause because it does not place an undue burden on interstate commerce. Despite opponents' arguments, various courts' rulings upheld the constitutionality of other state-level regulations of online conduct as varied as sending "spam" emails to those engaging in online gambling. Therefore, courts may not find that consumer data privacy legislation in the mold of the CCPA is so uniquely onerous as to violate the dormant commerce clause.

Courts across the country have recognized the constitutionality of various state laws that regulate business conduct on the Internet. In *State v. Heckel*, the Washington State Supreme Court concluded that a state law prohibiting spam emails was constitutional under the dormant commerce clause.[75] The court looked at how the law benefited multiple groups—spanning both consumers and industry—as well as how the harms of spam were well-known: "The Act protects the interests of three groups—ISPs, actual owners of forged domain names, and e-mail users. The problems that spam causes have been discussed in prior cases and legislative hearings."[76] Other courts cited *Heckel* in upholding their own laws directed against spamming and reducing fraud, finding that the burden on online senders of

---

72. Elanie McArdle, *The New Age of Surveillanc*e, HARVARD L. TODAY (May 10, 2016), https://today.law.harvard.edu/feature/new-age-surveillance/ [https://perma.cc/RV4H-U8GT].

73. *Id.*

74. Sara Morrison, *Live Results for California's Data Privacy Ballot Initiative*, VOX (Nov. 4, 2020), https://www.vox.com/policy-and-politics/2020/11/3/21546835/california-proposition-24-live-results-data-privacy

75. State v. Heckel, 24 P.3d 404, 409 (Wash. 2001).

76. *Id.*

unsolicited commercial emails "clearly does not outweigh" the local benefits provided by the legislation.[77]

In another suit, the Maryland Court of Special Appeals found the Maryland Commercial Electronic Mail Act did not run afoul of the dormant commerce clause on similar grounds. The Court ultimately held that:

> MCEMA... does not prevent senders of email advertisements from soliciting the residents of other states; *it merely regulates those that are sent to Maryland* residents or from equipment located in Maryland. *The Act does not project Maryland's regulatory scheme into other states because email advertisers remain free to send emails to other states*.[78]

The court also cited *Heckel* favorably throughout the opinion and noted the similarity between the Maryland and Washington laws.[79] Ultimately, *MaryCLE* stands for the proposition that merely regulating Internet conduct involving Internet users in a certain state does not constitute "projecting" that state's regulatory scheme into other states.

Accordingly, courts' application of the dormant commerce clause was not limited to laws regulating spam emails. Instead, courts proved themselves willing to allow states to regulate other activities on the Internet and were not reflexively supportive of plaintiffs' claims that laws regulating Internet-based businesses proved too costly to justify the purported public benefit.

Courts have permitted regulation of Internet payday lending even when "plaintiff contend[ed] that the burden on interstate commerce created by Kansas's regulation of out-of-state Internet payday lenders clearly exceed[ed] the benefits afforded by such regulation . . . "[80] But it held the plaintiff must show evidence "of what those costs might be[;]" simply arguing it is burdensome is insufficient.[81] Courts also have upheld online gambling regulations in the absence of being able to identify nondiscriminatory alternatives, and have found that the future existence of "more sophisticated means of policing the [I]nternet" did not preclude state legislation that treats "online betting differently than gambling that takes place at brick-and-mortar establishments."[82] "The introduction of a new technology" like the Internet

---

77. Ferguson v. Friendfinders, Inc., 115 Cal. Rptr. 2d 258, 269 (2002) (modified Jan. 14, 2002) (upholding the constitutionality of CAL. BUS. & PROF. CODE § 17538.4 (West 2021) (repealed 2003), which regulated the sending of unsolicited commercial emails by entities engaging in business in California).

78. MaryCLE, LLC v. First Choice Internet, Inc., 890 A.2d 818, 843 (Md. Ct. Spec. App. 2006) (emphasis added).

79. *See generally id.*

80. Quik Payday, Inc. v. Stork, 509 F. Supp. 2d 974, 978 (D. Kan. 2007), *aff'd*, 549 F.3d 1302 (10th Cir. 2008).

81. *Id.* at 980.

82. Churchill Downs Inc. v. Trout, 979 F. Supp. 2d 746, 755 (W.D. Tex. 2013), *aff'd*, 767 F.3d 521 (5th Cir. 2014).

makes regulation "more daunting," and further tips the balance away from the finding an undue burden exists on interstate commerce.[83]

The breadth of areas where courts have permitted regulation of online conduct likely bodes well for proponents of state data privacy legislation. Though the CCPA and CPRA are much wider in scope than most state regulatory frameworks that courts considered here, courts' declination to strike down state regulations of online commerce affecting state residents cuts against opponents' arguments that the Internet is such an interstate medium that state-level data privacy regulations are likely to place an undue burden on interstate commerce. Like the statute prohibiting unsolicited email advertisements in *MaryCLE* was not said to "project" Maryland's statutory prohibition into other states because "it merely regulates those that are sent to Maryland residents," the CCPA as amended by the CPRA cannot be said to project California's statutory scheme into other states, because it solely covers California consumers.[84] Just as the court in *Churchill Downs* noted that the introduction of new technologies made the court less likely to find an undue burden existed with the approval of online gambling regulations, so too should future courts find that the rapid expansion of consumer data collection technologies justify the CPRA regulations.[85]

C. State Consumer Data Privacy Laws Are Likely to Pass the Pike Test Where State Regulations Are Similar and Multistate Compliance Is Simple

Opponents of California's consumer data privacy laws often argue that the costs of complying with a "patchwork" of laws in a similar vein create the "undue burden" that defeats these measures under the dormant commerce clause.[86] Indeed, courts have previously considered whether the state regulations at issue are contemporaneously inconsistent with other states' regulations in determining whether they violate the dormant commerce clause.[87]

But commentators have also identified instances when regulatory statutes challenged under the dormant commerce clause prevailed in part because they mirrored regulatory schemes widely adopted throughout the

---

83. *See Churchill Downs Inc.*, 979 F. Supp. 2d at 754 (holding that "When the issue is, as here, the introduction of a new technology into an already difficult to control area like gambling, the state's interest in regulating the conduct becomes even more compelling").

84. MaryCLE, LLC v. First Choice Internet, Inc., 890 A.2d 818, 843 (Md. Ct. Spec. App. 2006).

85. *See Churchill Downs Inc.*, 979 F. Supp. 2d at 755.

86. *See* Huddleston, *supra* note 5 (stating that "even slight differences in state level privacy laws will create [d]ormant [c]ommerce [c]lause-triggering undue burdens as out-of-state companies confront the choice to either comply with the most stringent state laws or create individual and less efficient products for each state or local regulation.").

87. *See, e.g.,* IMS Health Inc. v. Mills, 616 F.3d 7, 28 (1st Cir. 2010), *vacated and remanded by sub nom.* IMS Health, Inc. v. Schneider, 564 U.S. 1051 (2011), (noting that "Maine's law does not risk imposing regulatory obligations inconsistent with those of other states. No other states have erected competing regulations, much less opposing regulations requiring the transfer of Maine prescribers' data").

United States. Arguing for the constitutionality of the CCPA under the dormant commerce clause, Spivak identifies *State v. Maybee* as of particular interest.[88] In *Maybee*, the Oregon Court of Appeals' decision upheld an Oregon statute requiring tobacco producers not party to a prior settlement agreement with the state to provide information to the state attorney general.[89] Spivak stated that, "[i]n performing its balancing test, the court was careful to note that 'the burden on interstate commerce is minimal, in light of the fact that forty-six other states have similar statutes.'"[90]

Some commentators have noted that the CPRA mirrors the E.U. GDPR so closely that "several of the new CPRA provisions are based on the [GDPR] with an eye towards obtaining an adequacy decision from the European Commission."[91] Because many websites have already configured their businesses to comply with the GDPR, compliance with the CPRA is less likely to be found an undue burden than in the regulation's absence.[92]

However, a disharmonious patchwork of consumer data privacy regulations could lead to a court striking down a state's data privacy law under the *Pike* test. In this scenario, contradictory state laws that make interstate compliance effectively impossible would place enough of a burden on interstate commerce to justify striking one of them down. *IMS Health* suggests that inconsistent regulatory standards across state lines might constitute a dormant commerce clause violation.[93] Previously, in *Healy v. Beer Inst.*, the Supreme Court pointedly stated that the dormant commerce clause "protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another [s]tate."[94] Subsequent circuit courts have cited this criterion as one of part of the "principle against extraterritoriality."[95]

However, this element of the principle against extraterritoriality does not necessitate categorically prohibiting state data privacy laws. Harmonious regulations across the several states would not lead to the same burden as in *Healy*, because they would not make interstate compliance impossible. As

---

88. Russell Spivak, *Too Big a Fish in the Digital Pond? The California Consumer Privacy Act and the Dormant Commerce Clause*, 88 U. CINCINNATI L. REV. 512, 512 https://scholarship.law.uc.edu/cgi/viewcontent.cgi?article=1342&context=uclr (citing *State v. Maybee*, 232 P.3d 970, 977 (Or. Ct. App. 2010).

89. *Maybee,* 232 P.3d at 971.

90. Russell Spivak, *supra* note 88 (citing *Maybee*, 232 P.3d at 971).

91. *See CPRA Rivals GDPR's Privacy Protections While Emphasizing Consumer Choice*, *supra* note 41.

92. Caitlin Fennessy, *CPRA's Top 10 Impactful Provisions, International Association of Privacy Professionals* (May 12, 2020), https://iapp.org/news/a/cpra-top-10-impactful-provisions/ (noting that, for a portion of the CPRA, "[t]hese new provisions will be familiar to many businesses already complying with the GDPR, which the CPRA mirrors in this regard") [https://perma.cc/4XBJ-XXDX].

93. *See* IMS Health Inc. v. Mills*,* 616 F.3d 7, 28 (1st Cir. 2010)*, vacated and remanded by sub nom.* IMS Health, Inc. v. Schneider*,* 564 U.S. 1051 (2011).

94. *Healey v. Beer Inst., Inc.*, 491 U.S. 324, 337 (1989).

95. *See Ass'n for Accessible Medicines v. Frosh*, 887 F.3d 664, 669 (4th Cir. 2018) (striking down a Maryland statute prohibiting price gouging in prescription drug sales on the grounds it violated the dormant commerce clause).

discussed above, consumer data privacy laws would likely pass muster so long as compliance is not impossible for covered entities.

IV. THE LIKELY CONSTITUTIONALITY OF A BROAD STATUTE LIKE THE CCPA SUGGESTS DORMANT COMMERCE CLAUSE CHALLENGES TO OTHER STATES' CONSUMER PRIVACY PROTECTIONS MAY FAIL

Because the CCPA or CRPA may pass constitutional muster under the dormant commerce clause, other consumer data privacy statutes in other states will likely survive—especially given that many other states' regulations are of a much more limited scope. According to the National Conference of State Legislatures, over thirty U.S. states and Puerto Rico considered implementing data privacy legislation in 2020.[96]

Nevada and Maine adopted their own versions of consumer data privacy legislation in 2019.[97] However, neither statute is as expansive as the CPRA. The Maine statute, the Act to Protect the Privacy of Online Consumer Information, only applies to Internet service providers in the state, and requires them to get permission from consumers "before selling or sharing their data with a third party."[98] It also prohibits internet service providers "from offering consumers discounts in exchange for selling their data."[99] Nevada passed a similar consumer data protection law more expansive than the Maine statute—the Nevada law does not only apply to Internet service providers, but "operators of Internet websites and online services" as well.[100] However, the statute is narrower than either the CCPA or CPRA—particularly when defining who is a "consumer" under the terms of the Act.[101]

Meanwhile, the recent passage of the Consumer Data Protection Act (CDPA) in the Virginia state legislature is perhaps the most significant development in the state data privacy legislation landscape. Hailed as "the East Coast version of the [CCPA]," the CDPA is of similar scope to both the

---

96. *2020 Consumer Data Privacy Legislation*, NAT'L CONFERENCE OF STATE LEGISLATURES, (Jan. 17, 2021) https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx.

97. Gary Guthrie, *Consumer Privacy Regulation Progresses at the State Level*, CONSUMERAFFAIRS (June 19, 2019), https://www.consumeraffairs.com/news/consumer-privacy-regulation-progresses-at-the-state-level-061919.html.

98. Steven Musil, *Maine Governor Signs Strict Internet Privacy Protection Bill*, CNET (June 6, 2019), https://www.cnet.com/news/maine-governor-signs-internet-privacy-protection-bill/ [https://perma.cc/S6NZ-RFN3].

99. *Id.*

100. Alexandra Scott & Lindsey Tonsager, *Nevada's New Consumer Privacy Law Departs Significantly from The California CCPA*, COVINGTON: INSIDE PRIVACY (June 10, 2019), https://www.insideprivacy.com/united-states/state-legislatures/nevadas-new-consumer-privacy-law-departs-significantly-from-the-california-ccpa/ [https://perma.cc/NUE4-T76X].

101. *See id.* (contrasting the Nevada Act's definition of "consumer" with the expansive definition adopted by the California Legislature in the CCPA, which "includes any California resident").

CCPA and GDPR and is expected to be signed into law by the governor.[102] The act "expands Virginia's definition of personal data" to include "sensitive data" covering sexual orientation, race, religion, medical diagnoses, and biometric data, among other categories.[103] It also, like the CCPA and GDPR, allows consumers to delete or obtain copies of personal data collected by companies, and opt out of company processing and profiling of personal data. The CDPA does, however, contain exemptions "far broader" than other state data privacy laws.[104] It does not apply to individual data obtained from individuals in business-to-business transactions, or to the personal data of employees.[105] The CDPA also "applies to persons who conduct business in Virginia."[106] Additionally, unlike the CCPA, it lacks a private right of action for consumers, and is enforced solely by the state's Attorney General.[107] Under the CDPA, violators would be subject to fines up to $7,500.[108]

Consumer advocates and supporters of the CPRA should be heartened by the adoption of consumer data privacy protections in an increasing number of states. However, these statutes are likely to run into the same criticism and legal opposition as the CPRA, despite many new statutes' more limited scope. Proponents and supporters can reduce the likelihood that courts will find that these new measures impose an undue burden by harmonizing with CPRA guidelines, as well as those in the GDPR. The easier compliance is for businesses, the less likely that state regulations will be struck down as undue and onerous. Accordingly, state policymakers should heed some commentators' distain for a patchwork regulatory framework and avoid unnecessary variation across state statutes.

V. CONCLUSION

A federal framework establishing clear, harmonized national guidelines for consumer data privacy protection would provide American consumers with peace of mind and ease business' efforts to comply with a patchwork of varied regulations. But the current lack of federal regulation is far from ideal. Patchwork privacy, while not necessarily an optimal solution, is necessary in

---

102. Allison Schiff, *CCPA On The East Coast? Meet CDPA, Virginia's Consumer Data Protection Act*, AD EXCHANGER (Feb 2, 2021), https://www.adexchanger.com/privacy/ccpa-on-the-east-coast-meet-cdpa-virginias-consumer-data-protection-act/.

103. Elizabeth Harding & Caitlin A. Smith, *New Virginia Privacy Bill*, 11 NAT. L. REV. 47 (Feb. 16, 2021), https://www.natlawreview.com/article/new-virginia-privacy-bill [https://perma.cc/9ALQ-NAHT].

104. Alexander Koskey III & Matthew White, *Privacy Legislation Floodgates Have Opened: Virginia Passes the Consumer Data Protection Act*, JDSUPRA (Feb. 24, 2021), https://www.jdsupra.com/legalnews/privacy-legislation-floodgates-have-7999102/ [https://perma.cc/4JB9-Q2HL].

105. *See id*.

106. *Id.*

107. *Id.*

108. Matt Dumiak, *CDPA: Virginia's Consumer Data Protection Act*, COMPLIANCE POINT (Feb. 18, 2021), https://www.compliancepoint.com/privacy/cdpa-virginias-consumer-data-protection-act/ [https://perma.cc/MMG5-6A9T].

light of the federal government's inability to safeguard the privacy rights of American consumers.

Here, analysis of dormant commerce clause constitutionality has mainly been confined to the CCPA, as amended by the CPRA, due to sweeping scope of consumer data protection regulations in California. The great weight of commentary on these pieces of legislation has been critical. Many claim that beyond heralding in a completely unworkable patchwork regulatory framework, these provisions burden interstate commerce to such an extent as to be unconstitutional. But as shown above, this is not necessarily true. There is a body of caselaw that has held both that privacy constitutes a legitimate local interest and that state laws regulating online commercial conduct affecting their residents do not necessary constitute an undue burden on interstate commerce. Accordingly, proponents for taking CPRA-style consumer data privacy protections nationwide can point towards this precedent. Harmonizing regulations between states and between widely adopted international standards like the GDPR would further minimize any burden on interstate commerce. And already existing state laws outside of California are likely to continue to stand, if only because their narrower scope likely means that they place a smaller burden on interstate commerce.

Additionally, adopting a patchwork privacy regime now does not preclude a comprehensive federal fix in the future. Whether or not an overarching federal law should preempt then-existing state consumer data privacy regulations depends in large part how unharmonized the future patchwork becomes; commentators are correct to point out that wildly inconsistent regulatory regimes will make business compliance efforts difficult. And contradictory state data privacy regimes that effectively make compliance impossible across states may raise their own discrete questions under the dormant commerce clause. Ultimately, these questions are fertile ground for future research.

The Stored Communications Act and the Fourth Circuit: Resolving the Section 2510(17)(B) Circuit Split in *Hately v. Watts*

James Elustondo*

TABLE OF CONTENTS

* James C. Elustondo, J.D., May 2022, The George Washington University Law School. I want to thank my parents, Patricia and Don, and my brother, Tom, for their unwavering support. I would also like to thank Professor Ethan Lucarelli for his assistance during drafting, as well as the Editorial Board and associates at FCLJ for their work during the editorial process.

I. INTRODUCTION

A person accesses your Gmail account by gaining your password or by hacking in. By viewing only your *opened* emails, those that have been read or opened previously, that person learns you will be away from your home or apartment for some period of time, and they rob you of all your belongings. When the perpetrator is caught, evidence of the robbery is thrown out in court, while evidence of the unauthorized access of your Gmail account remains admitted. Under this set of facts, the Eighth Circuit would likely hold that this perpetrator is not subject to any criminal or civil liability for accessing your inbox under section 2510(17)(B) of the Stored Communication Act (SCA) because he looked exclusively at *opened* emails, rather than viewing *unopened* emails that have not been read or opened previously.[1] If this comes across as an arbitrary, counter-intuitive interpretation of a law meant to protect electronic communications, you are not alone in that opinion.

The Eighth Circuit's narrow interpretation of the SCA, which excludes protections for opened emails, can discourage opening emails in order to protect their contents. Because people tend to open most emails that contain sensitive personal information, this reading of the SCA leaves a major gap in the already minimal protections Americans have against cyber-crime, identity theft, and other forms of fraud. Fortunately, the law regarding this issue is not settled and a substantial circuit split has formed between the Eighth Circuit and two other circuit courts. The other circuits, the Ninth and now the Fourth, have rejected the narrow reading of section 2510(17)(B) which fails to protect opened emails under the SCA's definition of 'electronic storage.'[2] This Note addresses this split and interprets the statutory language broadly to include and protect opened emails under this provision. In its holding in *Hately*, the Fourth Circuit adopted some of the Ninth Circuit's grammatical and superfluity reasoning from the Ninth Circuit's earlier *Theofel v. Farey-Jones* opinion, but the Fourth Circuit's opinion provides far more comprehensive arguments in favor of reading section 2510(17)(B) broadly, as well as addresses counterarguments at length, differs in crucial respects, and accounts for modern technology in its analysis. Courts across the country should adopt the Fourth Circuit's interpretation of section 2510(17)(B) of the SCA protecting opened emails because of the strength of the court's arguments regarding the statute's plain meaning, the superfluity doctrine, the legislative history, the absurdity doctrine, and the substantial, intervening technological developments, in addition to independent policy considerations and common sense.

This Note will first discuss the importance of providing adequate protections for email communications and explore the threats posed by a failure to do so. The Note will then discuss the rationale for passing the

---

1. *See* Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 840-42 (8th Cir. 2015).

2. *See* Hately v. Watts, 917 F.3d 770, 786, 796 (4th Cir. 2019); Theofel v. Farey-Jones, 359 F.3d 1066, 1071, 1075-76 (9th Cir. 2004).

Electronic Privacy Act, which included the Stored Communications Act, a provision specifically providing adequate protection for electronic communications from government overreach and cybercriminals. Next, this Note will cover section 2701, which outlines what is an offense under the SCA and explains the definitions of electronic storage, electronic communication, and electronic communication service for the purposes of interpreting section 2510(17)(B). Next, this Note will discuss the facts and holdings from key cases, including the primary arguments animating the circuit split and inconsistent treatment by the courts. The analysis section will then begin with the assertion that the Fourth Circuit's plain meaning and superfluity arguments for the broad interpretation should prevail over those arguments made by other courts. A discussion of the absurd results created by reading subsection B narrowly and a discussion of the evidence in the legislative history for a broad interpretation will follow. The Note will then analyze the Fourth Circuit's key interpretive innovations in *Hately* compared to the Ninth Circuit's ruling in *Theofel*. The Note will then cover policy considerations independent from the Fourth Circuit's arguments favoring the broad reading of section 2510(17)(B). The final section will discuss some alternative solutions to the circuit split other than adoption of the Fourth Circuit's interpretation.

II. BACKGROUND

A. Widespread Email Usage and Growing Threats Posed to Data Contained in Email Inboxes

Email has become one of the most pervasive forms of communication in the world. In 2020, roughly 306.4 billion emails were sent each day, and, as of 2020, there were 4 billion global email users with that number only set to grow.[3] Among Americans aged 15-64 in 2019, the percentage of Internet users utilizing email did not drop below 90%, and even 84% of Americans aged 65+ used email.[4] Despite the growing use of social media and other messaging platforms, email usage rates continue to increase steadily.[5] As Americans rely on their email accounts more and more during the Covid-19

3. Joseph Johnson, *Number of Sent and Received E-mails per Day Worldwide from 2017 to* 2025, STATISTA (Oct. 19, 2021), https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/ [https://perma.cc/2HUY-6T6E]; Statista Research Department, *Number of E-Mail Users Worldwide 2017-2025*, STATISTA (Mar. 19, 2021), https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide/ [https://perma.cc/KX3R-H4R9].

4. Joseph Johnson, *Share of U.S. E-Mail Users 2019 by Age Group*, STATISTA (Jan. 27, 2021), https://www.statista.com/statistics/271501/us-email-usage-reach-by-age/ [https://perma.cc/C95B-VHNE].

5. THE RADICATI GROUP INC., EMAIL STATISTICS REPORT, 2015-2019, http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf [https://perma.cc/J39H-YBKS].

pandemic, the amount of personal data that can be gleaned from their inboxes grows alongside this reliance.[6]

Email usage in the U.S. is clearly widespread, and the threats posed to the security of these email accounts become more serious every day. For example, in 2016, Yahoo reported that 500 million accounts had been breached, and the company later confirmed the actual number was closer to three billion accounts worldwide.[7] The data stolen included names, email addresses, phone numbers, birthdays, passwords, as well as security questions and their answers; this essentially gave hackers (or those to whom they sell data) the ability to completely control Yahoo webmail accounts.[8] Personal and business email accounts are targeted by cyber-criminals for the treasure trove of personal or business data they hold for identity thieves and data brokers.[9] Most online services also require a user to enter an email address, and if someone else can access your inbox, they can reset the passwords of your accounts to take control of them.[10] In 2021, 3.2 billion emails and their associated passwords were leaked onto a hacker website from a number of different data breaches.[11] Additionally, the threat of identity theft and other types of fraud have grown in recent years. In 2019, the FTC received 3.3 million identity theft and fraud reports; while in 2020, the FTC reported 4.7 million.[12] From January 2021 to August 2021 alone, $519.43 million were lost to identity theft or other fraud often involving the use of personal data.[13] Furthermore, 70% of American adults believe that their personal data is less

6. Geoffrey Fowler, *The Three Worst Things about Email, and How to Fix Them*, WASH. POST (July 21, 2020), https://www.washingtonpost.com/technology/2020/07/21/gmail-alternative-hey/ [https://perma.cc/8SSJ-56MG].

7. Robert McMillan & Ryan Knuston, *Yahoo Triples Estimate of Breached Accounts to 3 Billion*, WALL ST. J. (Oct. 3, 2017, 9:23 PM), https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804.

8. Lily Hay Newman, *Hack Brief: Hackers Breach a Billion Yahoo Accounts.* WIRED (Dec. 14, 2016, 7:27 PM), https://www.wired.com/2016/12/yahoo-hack-billion-users/ [https://perma.cc/29AC-QRYZ].

9. Microsoft 365 Team, *Why a Billion Hacked E-Mail Accounts Are Just the* Start, MICROSOFT (Apr. 2, 2019), https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/why-a-billion-hacked-email-accounts-are-just-the-start [https://perma.cc/PJG2-8EAC].

10. *Id*.

11. Bernard Meyer, *COMB: The Largest Breach of All Time Leaked Online with 3.2 Billion Records*, CYBERNEWS (Feb. 12, 2021), https://cybernews.com/news/largest-compilation-of-emails-and-passwords-leaked-free [https://perma.cc/B9PV-46YD].

12. *Facts + Statistics: Identity Theft and Cybercrime*, INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Feb. 4, 2021) [https://perma.cc/SVL5-AH4B]; *New Data Shows FTC Received 2.2 Million Fraud Reports from Consumers in 2020*, FTC (Feb. 4, 2021), https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers [https://perma.cc/UZ8G-DVGG].

13. Federal Trade Commission, *FTC Covid-19 and Stimulus Reports*, TABLEU PUBLIC, (Oct. 19, 2021), https://public.tableau.com/app/profile/federal.trade.commission/viz/COVID-19andStimulusReports/AgeFraud [https://perma.cc/XMX5-PYLB].

secure than it was five years ago.[14] Simply put, email inboxes contain vital personal information and business data which requires adequate protection.

B. The Electronic Communications Privacy Act of 1986 and Title II of The Stored Communications Act: An Effort to Protect Electronic Communications in Section 2701(a) and the Meaning of "Facility"

Even in the 1980s, before the massive growth in email usage, Congress saw the need for strengthened protections of electronic communications, both from government investigators and criminals.[15] The Electronic Communications Privacy Act of 1986 (ECPA) was the result, passed as an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[16] ECPA has three titles under the general ECPA umbrella.[17] The first title is the Wiretap Act, or Title I, which raised the standards for government search warrants seeking aural communications, or those involving the human voice, while they are in transit.[18] The second title is the Stored Communications Act (SCA), or Title II, which is the key title in the broader law for the protection of email communications.[19] The third title is the Pen Register Act, or Title III, which prohibits the use of pen registers or other devices that capture dialing, routing, addressing, and signaling information absent a court order.[20] Whereas communications in transit are primarily protected by the Wiretap Act, communications within storage fall under the SCA.[21]

The opening section of the SCA, section 2701, lays out the protections afforded to email inboxes. Section 2701(a) makes it an offense to "(1) intentionally access without authorization a facility through which an electronic communication service is provided or (2) intentionally exceed an authorization to access that facility and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage."[22]

---

14. Brooke Auxier et. al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/K4B5-NDJ8].

15. *See* Justice Information Sharing, *Electronic Communications Privacy Act of 1986 (ECPA)*, U.S. DEP'T OF JUST., https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (last accessed Feb.7, 2022) [https://perma.cc/N82G-GZMZ].

16. *Id.*

17. *Id.*

18. *Id.*

19. *Id.*

20. *Id.*

21. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 350 (6th ed. 2018).

22. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701(a).

For the purposes of this Note, the pertinent "facility" is the inbox or web-based server on which email services store a user's communications, rather than a specific computer or cell phone. The violations discussed throughout involve accessing another person's email inbox from a device other than the victim's personal device. The question of whether computers, cell phones, and other physical devices qualify as facilities under the SCA, when someone intentionally accesses a victim's device without authorization rather than using a different device to access a web-based server without authorization, is outside the scope of this argument. First offenses are punishable by a fine per violation, and can be punished by up to a year in prison.[23] Offenses committed for purposes of commercial advantage, malicious destruction, or private commercial gain are subject to a fine and up to five years in prison.[24] The SCA also provides a private right of action for services, subscribers, or any other person aggrieved by a violation of the statute.[25] The court assesses the sum of actual damages suffered by the plaintiff and any resulting profits made by the violator, but in no case "will a person entitled to recover receive less than the sum of $1,000."[26] If the violation is intentional or willful, the court may also assess punitive damages, and, if the civil action is successful, reasonable attorney's fees.[27] While a few courts have held that actual damages are a prerequisite for awarding statutory damages,[28] a substantial number of district courts, as well as the Ninth Circuit, have held that proving actual damages is not required for an award of statutory damages per violation.[29] To fully understand the scope of the SCA's protections, the terms (1) electronic storage, (2) wire or electronic communication, and (3) electronic communication service must be fully defined and explained.

---

23. *Id.* § 2701(b)(2)(A).
24. *Id.* § 2701(b)(1)(A).
25. *Id.* § 2707(a).
26. *Id.* § 2707(c).
27. *Id.*
28. *See* Vista Mktg., LLC v. Burkett, 812 F.3d 954, 971 (11th Cir. 2016); Cornerstone Consultants, Inc. v. Prod. Input Solutions, L.L.C., 789 F. Supp. 2d 1029, 1055-56 (N.D. Iowa 2011).
29. *See* Cline v. Reetz-Laiolo, 329 F. Supp. 3d 1000, 1045-46 (N.D. Cal. 2018) ("I will follow the seemingly unanimous view of my fellow district courts in this circuit to conclude that actual damages are not necessary for a plaintiff to recover statutory damages under the SCA."); Aguiar v. MySpace LLC, No. CV1405520SJOPJWX, 2017 WL 1856229, at *9 (C.D. Cal. May 5, 2017) ("[A] party 'aggrieved by a violation of the Act could obtain the minimum statutory award without proving actual damages.'"); Chavan v. Cohen, No. C13-01823 RSM, 2015 WL 4077323, at *4 (W.D. Wash. July 6, 2015) ("The Court … finds that a plaintiff need not prove actual damages or profits and that multiple violations of the SCA may warrant multiplying the $1,000 minimum statutory award by the number of each discrete violation."); Joseph v. Carnes, 108 F. Supp. 3d 613, 618 (N.D. Ill. 2015); Maremont v. Susan Fredman Design Grp., Ltd., No. 10 C 7811, 2014 WL 812401, at *7 (N.D. Ill. Mar. 3, 2014); Brooks Grp. & Assoc.'s, Inc. v. LeVigne, No. CIV.A. 12-2922, 2014 WL 1490529, at *9-10 (E.D. Pa. Apr. 15, 2014); Shefts v. Petrakis, 931 F. Supp. 2d 916, 917-19 (C.D. Ill. 2013); Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 759 F. Supp. 2d 417, 427-428 (S.D.N.Y. 2010); Wyatt Technology Corp. v. Smithson, 345 Fed. App'x. 236, 239 (9th Cir. 2009) (remanding for determination of statutory damages even in the absence of actual damages).

1. Definition of "Electronic Storage"

The SCA defines electronic storage in section 2510(17) as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for the purposes of backup protection of such communication."[30] The definition focuses on how and why the communication was stored, whether temporarily, intermediately, or purposefully for backup purposes. Many courts have held, supported by legislative history, that the two subsections recognize two discrete types of protected electronic storage: (1) storage "incidental to transmission" and (2) "backup" storage.[31] However, the focus of the circuit split and the discussion in this Note is the meaning of 'for the purposes of backup protection,' and, specifically, whether opened emails fall under this section 2510(17)(B) definition of electronic storage. Congress did not define 'backup protection' in the law and courts have not been able to settle on one interpretation of this specific language, let alone how the language fits into the broader statutory scheme.[32]

2. Definition of "Electronic Communication"

The SCA defines electronic communication broadly, with a few exceptions irrelevant to this discussion, as "any transfer of signs, signals, writing, images, sounds, data, or intelligence for foreign commerce transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce."[33] The plain language of the definition and the SCA's legislative history both confirm that this definition includes email communications.[34] Although section 2510(17)(B) does not explicitly mention "wire or electronic communication," the words "such communication" clearly references this

30. 18 U.S.C. § 2510(17).

31. *See* Hately v. Watts, 917 F.3d 770, 783 (4th Cir. 2019); Theofel v. Farey-Jones, 359 F.3d 1066, 1069 (9th Cir. 2004); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2003), *aff'g in part, vacating in part, and remanding* 135 F.Supp.2d 623 (E.D. Pa. 2001); H.R. REP. NO. 99-647, at 68 (1986); S. REP. 99-451, at 35 (1986).

32. *See Hately*, 917 F.3d at 770; *Vista Mktg.*, 812 F.3d at 976 ("considerable disagreement exists over whether, and if so, under what conditions, opened email transmissions may qualify as being held in 'electronic storage'"); Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 840-42 (8th Cir. 2015); *Theofel*, 359 F.3d at 1066; Orin S. Kerr, *Fourth Circuit Deepens the Split on Accessing Opened E-Mails*, REASON: VOLOKH CONSPIRACY (Mar. 21, 2019; 6:05 AM), https://reason.com/volokh/2019/03/21/fourth-circuit-deepens-the-split-on-civi/ [https://perma.cc/2SAB-QAE5].

33. Stored Communications Act, 18 U.S.C. § 2510(12).

34. *See Hately*, 917 F.3d at 785; *Vista Mktg.*, 812 F.3d at 964 (recognizing that emails are "subject to the protections of 18 U.S.C. § 2701(a)"); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002); In Matter of Application of U.S., 416 F.Supp.2d 13, 16 (D.D.C. 2006) ("[T]here can be no doubt that the definition is broad enough to encompass e-mail communications."); H.R. REP. NO. 99-647, at 34 (recognizing that the definition of "electronic communications" provides "electronic mail" with protection); S. REP. NO. 99-541, at 14.

language in section 2510(17)(A).[35] Proponents of the narrow interpretation, however, disagree that "such communication" references "wire or electronic communication" exclusively, arguing instead that "such communication" references the entirety of "wire or electronic communication incidental to the electronic transmission thereof" from section 2510(17)(A).[36] Under this alternative reading, a stored, previously opened email would no longer be "incidental to the electronic transmission thereof" because the email is no longer in transit to the end viewer, and thereby falls outside the statutory definition.

3. Definition of "Electronic Communication Service"

Electronic communication service (ECS) is also defined broadly as any service which provides users with the ability to send or receive these wire or electronic communications.[37] When the law was originally passed in 1986, only email clients such as Eudora were used primarily by businesses, whereas widely accessible webmail services you can now access using a browser, such as Gmail, did not exist yet.[38] For traditional email clients, a user's email was stored on an Internet service provider's (ISP) server and the email was downloaded to permanent storage on a local computer to be read via a dedicated application.[39] By using webmail instead, anyone with access to a browser and an Internet connection can view their emails after they are pulled from an ECS server.[40] The browser downloads the emails and the messages are loaded to the user's device for temporary storage, remaining on the ECS server until expressly deleted but not permanently on any one device.[41] This ECS definition is broad enough to encompass both types of electronic mail

35. *See e.g. Hately,* 917 F.3d at 787; *Theofel*, 359 F.3d at 1075 (9th Cir. 2004); *Fraser*, 352 F.3d at 114; Strategic Wealth Group, LLC v. Canno, No. CIV.A. 10-0321, 2011 WL 346592, at *3-4 (E.D. Pa. Feb. 4, 2011); Cornerstone Consultants, Inc. v. Prod. Input Sols., L.L.C., 789 F. Supp. 2d 1029, 1055 (N.D. Iowa 2011); Shefts v. Petrakis, No. 10-CV-1104, 2011 WL 5930469, at *5 (C.D. Ill. Nov. 29, 2011); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 983 (C.D. Cal. 2010); United States v. Weaver, 636 F. Supp. 2d 769, 771 (C.D. Ill. 2009); Bailey v. Bailey, 2008 WL 324156, at *6 (E.D. Mich. 2008); Flagg v. City of Detroit; 252 F.R.D. 346, 362 (E.D. Mich. 2008).

36. *See* Jennings v. Jennings, 736 S.E.2d 242, 248 (S.C. 2012) (Toal, C.J., concurring in the result); OFF. OF LEGAL EDUCATION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 125 (3d ed. 2009); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1216-17 (2004).

37. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510(14).

38. *See Weaver*, 636 F. Supp. 2d at 772.

39. *Id*.

40. *See* Melissa Medina, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U. L. REV. 267, 287 (2013); *see also Jennings*, 736 S.E.2d at 245.

41. *See Weaver*, 636 F.Supp. 2d at 772.

services.[42] Also, most email service providers today operate email clients, browser webmail, and mobile applications utilizing temporary storage. Proving that the communications in question fall within the definitions of all three terms (electronic storage, electronic communication, and electronic communication service) is critical for establishing SCA protection.[43]

C. A Circuit Split Over Whether Subsections A and B Should Be Read Together and Whether "Backup Protection" Requires an Original Email and a Backup Copy

The circuit split at issue here that has formed over the interpretation of section 2510(17)(B), whether backup protection includes opened emails, is grounded in three primary cases from three appellate circuits: *Theofel v. Farey Jones* from the Ninth Circuit, *Anzaldua v. Northeast Fire Protection District* from the Eighth Circuit, and *Hately v. Watts* from the Fourth Circuit. The Ninth Circuit's *Theofel* ruling proffered the original superfluity and grammatical arguments for the broad interpretation of section 2510(17)(B), and the Fourth Circuit adopted some of this reasoning.[44] The Eighth Circuit in *Anzaldua* discussed the primary arguments made against the broad interpretation of the subsection.[45] However, the Eighth Circuit case dealt with unauthorized access of a user's sent or draft messages, rather than messages received in an inbox, and the Fourth Circuit in *Hately* rebutted the arguments discussed in *Anzaldua* thoroughly in its application to opened emails.[46] In *Hately*, the appellee claimed to have viewed previously opened emails only, making the case an ideal set of facts under which to analyze the unopened/opened divide bearing on SCA protection.[47] Ultimately, the Fourth Circuit's decision and its underlying arguments are more thorough and more compelling than those made by the Ninth Circuit seventeen years ago.

---

42. *See, e.g.,* Vista Mktg., LLC v. Burkett, 812 F.3d 954, 963-64 (11th Cir. 2016) (holding that the defendant "qualified as an [electronic communication service] because it was a service that provided employees with the ability to send and receive electronic communications, including emails"); Warshak v. United States, 532 F.3d 521, 523 (6th Cir. 2008) (holding that the definition of electronic communication service "covers basic e-mail services"); In re United States for an Ord. Pursuant to 18 U.S.C. § 2705(b), 289 F.Supp. 3d 201, 209 (D.D.C. 2018) (holding that online booking company was an electronic communications service for the purposes of a dispute related to disclosing messages from the company's "user-to-user electronic messaging system").

43. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701(a).

44. *See* Hately v. Watts, 917 F.3d 770, 797 (4th Cir. 2019); Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

45. Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 840-42 (8th Cir. 2015).

46. *Id.*; *Hately*, 917 F.3d at 792-96.

47. *See Hately*, 917 F.3d at 773-74.

1. Ninth Circuit in *Theofel v. Farey-Jones* (2004) Holds that Opened, Previously Read Emails Are Covered by the SCA

Wolf and Buckingham became engaged in commercial litigation against Farey-Jones in their capacity as officers of Integrated Capital Associates, Inc. (ICA).[48] During discovery, Farey-Jones sought access to ICA's email and had lawyer Iryna Kwasny subpoena NetGate, ICA's ISP.[49] Rather than requesting only emails related to the subject matter of the litigation consistent with Fed. R. Civ. P. 45(d)(1), Kwasny "ordered production of "[a]ll copies of emails sent or received by anyone" at ICA, with no limitation as to time or scope."[50] NetGate responded by posting 339 messages on their website where Kwasny and Farey-Jones read them.[51] Most of them were unrelated to the litigation, while many were also privileged and personal.[52] This resulted in Wolf, Buckingham, and other affected ICA employees filing suit against Farey-Jones and Kwasny, which included an SCA claim.[53] In its analysis, the Ninth Circuit compared parties who knowingly take advantage of mistaken consent to trespass violations, in addition to assessing the earlier issued subpoena as being patently unlawful, and determined that Farey-Jones and Kwasny did access the emails without authorization.[54]

The court found that opened emails were in 'electronic storage' under section 2510(17)(B) and thereby subject to SCA protection.[55] The Ninth Circuit originated the arguments that reading subsections (A) and (B) of the "electronic storage" definition together contravenes basic grammar and renders subsection (B) superfluous.[56] With respect to the grammatical argument, the court asserts that because both subsections outline a type of communication and then a type of storage, "such communication" in subsection (B) is simply referencing "wire or electronic communication" in subsection (A), rather than the type of communication and the type of storage.[57] In other words, because the "incidental to the electronic transmission thereof" language modifies the noun "storage," it does not modify "wire or electronic communication."[58] The court also asserts, in making the superfluity argument, that a narrow interpretation of section

48. *Theofel*, 359 F.3d at 1071.
49. *Id.*
50. *Id.*; FED. R. CIV. P. 45(d)(1) (stating "A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense[.]")
51. *Theofel*, 359 F.3d at 1071.
52. *Id.*
53. *Id.* at 1072.
54. *Id.* at 1073-74.
55. *Id.* at 1075-77.
56. *Id.* at 1075-76.
57. *Id.*
58. *Id.*

2510(17)(B) renders subsection (B) superfluous because pre-transmission backup storage would be covered under subsection (A).[59]

2. Eighth Circuit in *Anzaldua v. Northeast Ambulance and Fire Protection Dist.* (2015) Presents the Opposing Arguments

Steven Anzaldua worked for the Northeast Ambulance and Fire Protection District as a full-time paramedic and firefighter.[60] The Fire District suspended Anzaldua for failing to respond to a directive given by Chief Kenneth Farwell regarding an email Anzaldua purportedly sent that had been forwarded from his email account to Chief Farwell.[61] After the suspension, Anzaldua sent another email expressing concerns with the department and Chief Farwell, and it was somehow forwarded from Anzaldua's Gmail account to Chief Farwell once again; his employment was subsequently terminated.[62] Anzaldua had given his password to his ex-girlfriend Kate Welge, later an employee at Chief Falwell's restaurant, for the sole purpose of sending out resumes on his behalf.[63] Anzaldua alleges that she either gave the password to Chief Falwell, or that she forwarded the relevant emails herself, which she deleted from the outbox, in violation of the SCA.[64] The Eighth Circuit found that Anzaldua had sufficiently alleged unauthorized access of his account, but dismissed the SCA claim because the emails were not in "electronic storage" within the meaning of the statute.[65] The court cited to opinions and commentators disagreeing with and differentiating *Theofel* regarding the breadth of the SCA's definition of "electronic storage."[66] The court also raised two primary arguments made against the broad interpretation. The first argument is that subsection (A) and (B) must be read together, meaning that "such communication" in subsection (B) only covers emails stored temporarily during transmission from sender to addressee.[67] The second argument is that "backup protection" implies that there must be an original email which the secondary email copy backs up; this means that an original opened email is not stored for the "purposes of backup protection."[68] The Eighth Circuit decided that sent email stored in due course

---

59. *Id.*
60. *See* Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 827-28 (8th Cir. 2015).
61. *Id.* at 828-30.
62. *Id.*
63. *Id.* at 838.
64. *Id.*
65. *Id.* at 839.
66. *See id.* at 841.
67. *See* Jennings v. Jennings, 736 S.E.2d 242, 248 (S.C. 2012) (Toal, C.J., concurring in the result); Kerr, *supra* note 36, at 1214.
68. *See* Lazette v. Kulmatycki, 949 F.Supp. 2d 748, 758 (N.D. Ohio 2013); *Jennings*, 736 S.E.2d at 245 (2012).

with a sender's ECS, rather than for a user's backup purposes as alleged by *Anzaldua*, does not fall under the SCA's definition of electronic storage.[69]

3. The Fourth Circuit in *Hately v. Watts* (2019) Comprehensively Addresses the Circuit Split

Patrick Hately brought an action alleging that David Watts unlawfully accessed messages in Hately's web-based Gmail inbox.[70] One of Hately's claims was that Watts had violated the SCA when he accessed Hately's emails using login and password information provided by an ex-partner.[71] Watts admitted that he browsed through Hately's emails, but insisted that he did not "change the status of, or modify, any email in anyway," and that he "did not open or view any email that was unopened, marked as unread, previously deleted, or in the 'trash' folder."[72] The Fourth Circuit held that opened emails are protected under section 2510(17)(B), meaning that Watts' actions did violate the statute.[73] This section will cover the court's plain meaning and superfluity arguments, as these were largely taken from the Ninth Circuit, while the remaining arguments will be addressed in the analysis section.

Assuming that section 2510(17) lays out two distinct types of storage, the court stated a need to inquire into whether opened emails fall into (1) storage "incidental to transmission," or (2) "backup" storage.[74] *Hately v. Watts* provides an ideal set of facts under which to analyze the unopened/opened discrepancy in SCA protection, as Watts insisted he exclusively viewed emails that had been opened previously.[75] With respect to the first category, the plain, dictionary meanings of temporary, "existing or continuing for a limited time," and intermediate, "lying or being in the middle," demonstrate that section 2510(17)(A) protects electronic communications for a limited time while they are in the middle of transmission to their final destination.[76] Previously delivered and opened emails are clearly no longer in the middle of transmission, which places them

---

69. *See Anzaldua*, 793 F.3d at 840-42.

70. *See* Hately v. Watts, 917 F.3d 770, 773 (4th Cir. 2019).

71. *Id.*

72. *Id.*

73. *Id.* at 797.

74. *See e.g. Hately,* 917 F.3d at 787; Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2003); Strategic Wealth Grp, LLC v. Canno, No. CIV.A. 10-0321, 2011 WL 346592, at *3-4 (E.D. Pa. Feb. 4, 2011); Cornerstone Consultants, Inc. v. Prod. Input Sols., L.L.C., 789 F.Supp. 2d 1029, 1055 (N.D. Iowa 2011); Shefts v. Petrakis, No. 10-CV-1104, 2011 WL 5930469, at *5 (C.D. Ill. Nov. 29, 2011); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 983 (C.D. Cal. 2010); United States v. Weaver, 636 F. Supp. 2d 769, 771 (C.D. Ill. 2009); Bailey v. Bailey, 2008 WL 324156, at *6 (E.D. Mich. 2008); Flagg v. City of Detroit; 252 F.R.D. 346, 362 (E.D. Mich. 2008).

75. *See Hately*, 917 F.3d at 774.

76. *See Temporary*, WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY (1961); *Intermediate*, WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY (1961); In re DoubleClick Inc. Priv. Litig., 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001).

outside the plain meaning of section 2510(17)(A), but that still leaves questions concerning the plain meaning of section 2510(17)(B).[77]

a. Plain Meaning of "Storage"

The Fourth Circuit properly broke section 2510(17)(B) down into four elements: any (1) storage of (2) such communication (3) by an electronic communication service (4) for the purposes of backup protection of such communication.[78] With respect to electronic storage, the court asserted "storage" should simply mean "reserved for future use."[79] Given the plain meaning and Congress speaking directly to the issue, the Fourth Circuit determined the same result as the Ninth Circuit finding that prior access is irrelevant to whether an email is in storage.[80] When an email user opens an email and then decides to keep the message in their inbox rather than delete it, the message remains "reserved for future use" by the user.[81] In the alternative, email services also "reserve for future use" the relevant communication in case the user needs to subsequently access it or they experience technical issues.[82] In either case, opened emails fall under the section 2510(17)(B) definition of electronic storage.

b. Arguments Regarding the Plain Meaning of "Such Communication" and the Superfluity Doctrine

In the discussion of the "such communication" language, the Fourth Circuit largely adopts the Ninth Circuit's argument regarding the subsections, outlining two discrete types of protected electronic storage. Specifically:

---

77. *See* United States v. Councilman, 418 F.3d 67, 81 (1st Cir. 2005) (holding that Subsection (A) "refers to temporary storage, such as when a message sits in an email user's mailbox after transmission but before the user has retrieved the message from the mail server"); *Theofel*, 359 F.3d at 1075; *Fraser*, 352 F.3d at 114 (holding that an email in "post-transmission storage" was "not temporary, intermediate storage").

78. Stored Communications Act, 18 U.S.C. § 2510(17)(B); *see Hately*, 917 F.3d at 786.

79. *Store*, THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (5th ed. 2018).

80. *See Hately*, 917 F.3d at 786 (citing Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004)).

81. *See Theofel*, 359 F.3d at 1077; Cheng v. Romo, No. CIV.A. 11-10007-DJC, 2013 WL 6814691, at *7-9 (D. Mass. Dec. 20, 2013) (holding that copies of delivered and opened emails accessed through a web-based email client were in "storage" for purposes of Subsection (B)); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008) ("The majority of courts which have addressed the issue have determined that e-mail stored on an electronic communication service's systems after it has been delivered … is a stored communication subject to the SCA."); Bailey v. Bailey, No. 07-11672, 2008 WL 324156, at *5-6 (E.D. Mich. Feb. 6, 2008) ("The plain language of the statute seems to include emails received by the intended recipient where they remain stored by an electronic communication service.").

82. *See Hately*, 917 F.3d at 786.

> Subsection (A) identifies a type of communication ('a wire or electronic communication') and a type of storage ('temporary, intermediate storage … incidental to the electronic transmission thereof') … The phrase 'such communication' in subsection (B) does not, as a matter of grammar, reference attributes of the type of storage defined in subsection (A).[83]

The phrase "temporary, intermediate … incidental to the electronic transmission thereof" modifies the noun "storage," but does not modify the noun "communication"—the term referred to in subsection (B).[84]

As the statute is written, "such communication" is then simply an easy way to reference "wire or electronic communication," meaning the statute does cover post-transmission, opened emails.[85]

In addition to the Fourth Circuit's grammatical analysis,[86] the court argues a narrow interpretation excluding opened emails would also render section 2510(17)(B) superfluous.[87] Courts should generally avoid an interpretation that renders a clause, sentence, or word "inoperative … void, superfluous, or insignificant."[88] In theory, if "such communication" were read to only encompass wire or electronic communications in "temporary, intermediate storage," subsection (B) would become superfluous because temporary backup storage pending transmission would already be in "temporary, intermediate storage… incidental to the electronic transmission thereof" within the meaning of subsection (A).[89]

However, the broad interpretation of the statutory language has not been universally accepted. For example, Judge Toal of the South Carolina Supreme Court asserted that the two statutory provisions, section 2510(17)(A) and (B), must be read together.[90] Judge Toal emphasized the statute's use of the word "and," rather than "or," at the end of subsection A to support this argument, asserting that the Fourth Circuit's reading would essentially provide two definitions for "electronic storage" when the term is meant to subsume both subsections.[91] Under this reading, "electronic storage" would refer "only to temporary storage, made in the course of transmission,

---

83. *Hately*, 917 F.3d at 787, *citing Theofel*, 917 F.3d at 1076.
84. *Hately*, 917 F.3d at 787.
85. *Id.*
86. *Id.*
87. *Id.*
88. *See* Panjiva, Inc. v. U.S. Customs & Border Prot., 342 F. Supp. 3d 481, 490 (S.D.N.Y. 2018) ("[C]ourts must give effect to all of statute's provisions so that no part will be inoperative, void or insignificant.") (citing *United States v. Harris*, 838 F.3d 98, 106 (2d Cir. 2016)).
89. *See Hately*, 917 F.3d at 787 (citing *Theofel*, 359 F.3d at 1075-76 ("Were we to construe "such communication" as encompassing only wire or electronic communications in "temporary or intermediate storage," Subsection B would be rendered "essentially superfluous, since temporary backup storage pending transmission would already seem to qualify as 'temporary or intermediate storage' within the meaning of [S]ubsection A.")).
90. Jennings v. Jennings, 736 S.E.2d 242, 247-48 (S.C. 2012) (Toal, C.J., concurring in the result).
91. *Id.*

by an ECS provider, and to backups of such intermediate communications," excluding opened emails.[92] This interpretation also finds support from the Department of Justice and other commentators.[93]

c. Arguments Regarding the Plain Meaning of "Purposes of Backup Protection"

Having already addressed that "electronic communication service" includes both email clients and webmail,[94] the plain meaning interpretation of "for the purposes of backup protection," which has generated the most legal controversy, will be addressed next. The term "backup protection" is not defined in the statute and the Fourth Circuit properly turned to the dictionary meaning of the statutory definition's language. The court defined "backup" as a copy of computer data, and "protection" as the act of covering or shielding from exposure, injury, damage, or destruction.[95] A wire or electronic communication is therefore stored for "purposes of backup protection" if it is a copy of the communication stored to prevent destruction or damage.[96] Copies of previously delivered and opened emails retained on the servers of email service providers fall within this reading of section 2510(17)(B). The primary argument made against this plain meaning interpretation of "backup protection" is that the plain meaning of the term implies the existence of an original copy and a backup copy.[97] Under this understanding of the statutory language, the opened email, as the original copy, cannot be stored for the "purposes of backup protection."[98]

III. ANALYSIS

This section will first argue that the Fourth Circuit's arguments favoring its plain meaning interpretation of the statutory language are far

---

92. *Id.*

93. *See* U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 125 (3d ed. 2009); Kerr, *supra* note 36, at 1216.

94. *See, e.g.,* Vista Mktg., LLC v. Burkett, 812 F.3d 954, 963-64 (11th Cir. 2016) (holding that the defendant "qualified as an [electronic communication service] because it was a service that provided employees with the ability to send and receive electronic communications, including emails"); Warshak v. United States, 532 F.3d 521, 523 (6th Cir. 2008) (holding that the definition of electronic communication service "covers basic e-mail services"); In re United States for an Ord. Pursuant to 18 U.S.C. § 2705(b), 289 F. Supp. 3d 201, 209 (D.D.C. 2018) (holding that online booking company was an electronic communications service for the purposes of a dispute related to disclosing messages from the company's "user-to-user electronic messaging system").

95. *See* Hately v. Watts, 917 F.3d 770, 791 (4th Cir. 2019); *Backup*, Merriam-Webster.com, https://www.merriam-webster.com/dictionary/backup [https://perma.cc/RCW8-5SCS]; *Protection*, Merriam-Webster.com, https://www.merriam-webster.com/dictionary/protection [https://perma.cc/86FA-U5BQ].

96. *Id.*

97. *See* Lazette v. Kulmatycki, 949 F. Supp. 2d 748, 758 (N.D. Ohio 2013); Jennings v. Jennings, 736 S.E.2d 242, 245 (S.C. 2012).

98. Electronic Communications Privacy Act, 18 U.S.C. § 2510(17)(A), (B).

more compelling than those of the dissenting voices. Following this discussion, the analysis will cover the legislative history of the SCA and the absurd results created by the narrow interpretation of section 2510(17)(B). Next, this Note will analyze the Fourth Circuit's key interpretive innovations, and address counterarguments further. The analysis will then look to policy considerations that strongly point towards the broader reading of section 2510(17)(B). Finally, this analysis will conclude by presenting alternative solutions to the circuit split and the inconsistent application of this SCA language across jurisdictions.

A. The Fourth Circuit Settles Differences in the Interpretation of Section 2510(17)(B) Among Courts

1. Reading Section 2510(17)(A) and (B) Together Does Not Make Grammatical Sense and Does Create a Superfluity Issue

The argument that the two subsections must be read together contravenes basic grammar principles and does not resolve the superfluity issue, consistent with the Fourth Circuit's argument. Subsection (A) outlines a type of storage, "temporary, intermediate . . . incidental to the electronic transmission thereof," and a type of communication, "wire or electronic."[99] Common sense dictates that subsection (B) should be read the same way, with the type of storage being "any storage . . . by an electronic communication service for the purposes of backup protection," and the communication being "such communication" as a reference to "wire or electronic" from the previous subsection.[100] "Such communication" was just an easy way to reference the previously used "wire or electronic communication" language.[101] Also, the language "temporary, intermediate . . . incidental to the electronic transmission thereof" in the first subsection simply does not refer to the type of communication used in the subsection, when its purpose is to modify the type of storage.[102] Additionally, if Congress had intended this language to carry over into subsection (B), they certainly could have said so explicitly rather than leaving the answer ambiguous. Furthermore, Judge Toal's argument, mentioned in Part II, Section C of this Note, overemphasizes the importance of the word "and."[103] The word "and" does not preclude subsection (B) from outlining a different kind of electronic storage under the same definition. It is not uncommon for statutory definitions to include more than one category under the umbrella of one term.

---

99. *Id.*
100. *Id.*
101. *Id.*
102. Hately v. Watts, 917 F.3d 770, 787 (4th Cir. 2019).
103. *See* Jennings v. Jennings, 736 S.E.2d 242, 247-48 (S.C. 2012); U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 125 (3d ed. 2009); Kerr, *supra* note 36.

Reading the subsections together, or, rather, inserting subsection (A) language into subsection (B), also creates a major superfluity issue. If the definition in subsection (B) is read to refer to "any storage . . . for the purposes of backup protection," but only "incidental to the electronic transmission thereof," subsection (B) is stripped of independent meaning.[104] If an email is stored for backup protection before the email has been delivered, this would be precisely "any temporary, intermediate storage . . . incidental to the electronic transmission thereof" language from subsection (A).[105] This alternative reading violates the canon of surplusage by making subsection (B) completely unnecessary.[106] A statute should not be interpreted in such a way that congressionally drafted language is left without a purpose.[107] Some commentators claim subsection (B) was added in order to clarify that permanent or semi-permanent copies of communications made by ISPs back in 1986 during transmission do not lose strong SCA protection from cybercriminals and from government overreach, hence the insertion of the "temporary, intermediate . . . incidental to the transmission thereof" language into subsection (B).[108] However, subsection (A) can be easily interpreted to cover this form of storage "incidental to the transmission thereof," truly making subsection (B) superfluous under the narrow interpretation of section 2510(17)(A) and (B).[109] Also, given how much faster Internet connections have become and the advancements in cloud storage,[110] the question remains: how many copies of emails are made intermediately during transmission from place to place, rather than by the webmail providers of the sender and recipient upon being sent and received? Even if Congress's intention was to clarify subsection (A) protections, the usefulness of this subtle clarification has disappeared. For these reasons, the Fourth Circuit's arguments demonstrate that these two subsections should not be read together by inserting subsection (A) language into subsection (B), and that the definition

---

104. *See Hately*, 917 F.3d at 787 (citing *Theofel*, 359 F.3d at 1075-76 ("Were we to construe "such communication" as encompassing only wire or electronic communications in "temporary or intermediate storage," Subsection B would be rendered "essentially superfluous, since temporary backup storage pending transmission would already seem to qualify as 'temporary or intermediate storage' within the meaning of [S]ubsection A.")).

105. Electronic Communications Privacy Act, 18 U.S.C. § 2510(17)(A).

106. *See* Panjiva, Inc. v. U.S. Customs & Border Prot., 342 F. Supp. 3d 481, 490 (S.D.N.Y. 2018) (citing *United States v. Harris*, 838 F.3d 98, 106 (2d Cir. 2016)).

107. *Id.*

108. Kerr, *supra* note 36, at 1217 n.61.

109. Electronic Communications Privacy Act, 18 U.S.C. § 2510(17)(A).

110. Antonio Villas-Boas, *'Red Dead Redmption 2' Would Have Taken Almost 48 Hours to Download a Decade Ago – Here's How Far Internet Speeds Have Come*, BUS. INSIDER (Nov. 5, 2019), https://www.businessinsider.com/internet-speeds-have-gotten-dramatically-faster-over-past-decade-2019-11#:~:text=Indeed%2C%20as%20more%20of%20us,%2Dtesting%20site%20Speedtest.net ("Average internet speeds in American homes grew from around 5 Mbps in 2009 to 96.25 Mbps in 2018…") [https://perma.cc/W3MV-ZZVS]; *The Dawn of the Cloud*, MINDFIRE TECHNOLOGIES (June 23, 2018), https://www.mindfireit.com/cloud-computing/the-dawn-of-the-cloud/ ("Public cloud adoption in recent years is expected to reach a whooping £197 billion ($274 billion) in spending within just three years…").

of "electronic storage" in section 2510(17)(B) does in fact lay out two discrete forms of storage.

2. The Distinction Between an Original Email and a Copy Does Not Undermine the Broad Interpretation of "Backup Protection"

The other argument made against the broad reading of "backup protection," that the terminology only applies to copies retained in case the "original" email is rendered unusable, thereby presupposing the existence of an "original" email, also fails under closer scrutiny.[111] The logic is that emails opened by email users are the originals, rather than copies, and retaining this original for future viewing does not fall within the meaning of "for the purposes of backup protection."[112] However, the true original under this analysis would be the email typed in the sender's email service, while copies of this original would then be transmitted to the recipient's email service.[113] The recipient's email service never receives nor stores this true original.[114] Every copy held by the recipient email service would then be a copy of the true original, undermining this line of argument. Even if opened emails that a user decides to keep were interpreted to be an "original," this would still fall under the "backup protection" definition because of the redundancy built into the systems of these services, which will be discussed subsequently.[115]

B. Congress's Intent in Passing the Stored Communications Act and the Absurdity Doctrine

To the extent the SCA's legislative history articulates Congress's purpose in enacting the SCA, the House and Senate reports clearly point towards broader protections for email communications.[116] The SCA was born from congressional recognition that neither existing federal statutes nor the Fourth Amendment protected against potential intrusions on individual privacy via illicit access to "stored communications in remote computing operations and large data banks that stored e-mails."[117] To Congress, this legal uncertainty created potential problems in a number of areas.[118] First, the

111. *See, e.g.*, Cobra Pipeline Co. v. Gas Natural, Inc., 132 F. Supp. 3d 945, 952 (N.D. Ohio 2015) (holding the term "stored for backup purposes" does not encompass "primary" copies); Lazette v. Kulmatycki, 949 F. Supp. 2d 748, 758 (N.D. Ohio 2013); Jennings v. Jennings, 736 S.E.2d 242, 250 (S.C. 2012) ("Congress's use of 'backup' necessarily presupposes the existence of another copy to which this e-mail would serve as a substitute or support.").

112. *See* Hately v. Watts, 917 F.3d 770, 796 (4th Cir. 2019).

113. *Id.*

114. *See* S. REP. NO. 99-541, at 8 (1986).

115. *See infra* notes 143-148.

116. *See* King v. Burwell, 135 S. Ct. 2480, 2496 (2015) ("[A] fair reading of legislation demands a fair understanding of the legislative plan."); *Hately*, 917 F.3d at 782-83.

117. *See* H.R. REP. NO. 99-647, at 18 (1986); S. REP. NO. 99-541, at 2 (1986).

118. *See* H.R. REP. NO. 99-647, at 19.

former uncertainty surrounding legal protections afforded to electronic communications "promote[d] the gradual erosion of the precious right [to privacy]."[119] This potential for erosion connects to the negative sentiment Americans have about their privacy and to a potential restoration of agency through expanding the circumstances under which a civil action can be brought under the private right of action. Second, it "unnecessarily discourage[d] potential customers from using innovative communications systems."[120] This aligns closely with the concept that current uncertainty rooted in the circuit split can discourage people from opening their emails unless absolutely necessary. Third, the former legal uncertainty "encouraged unauthorized users to obtain access to communications to which they are not a party."[121] This concern clearly lines up with the issue of limited protections emboldening cyber-criminals and identity thieves when they can easily avoid liability for unauthorized access of email accounts. The three primary issues Congress sought to address in passing this legislation, issues which still exist today, are better served by interpreting the statutory language broadly to protect opened emails, rather than by leaving these emails vulnerable to cybercriminals. In fact, the narrow interpretation fatally clashes with Congress's intent.

Congress's discussion of the issues involved points to the need to protect the privacy and security of emails, regardless of whether someone has opened them previously. In addition, the Office of Technology Assessment, in a report cited extensively throughout the House and Senate reports, also emphasized the lack of legal protection for email.[122] The report identified "stages at which an electronic message could be intercepted and its contents divulged to an unintended receiver," critically including messages "in the electronic mailbox of the receiver" as one of these stages.[123] Given this evidence, to protect unopened and opened emails differently under the SCA is an absurd result that Congress almost certainly did not intend, as the Fourth Circuit asserts.[124] The absurdity of this result only grows when one recognizes that opened emails tend to have more sensitive personal or business information than emails the user never even viewed, including spam. In the words of the Fourth Circuit, "[i]t defies logic that the unopened junk and spam email messages that a user leaves in his or her inbox or designated folder without opening would be entitled to *more* protection than those messages the user chooses to open *and* retain."[125] From the United States' earliest days,

---

119. *Id.*

120. S. REP. NO. 99-541, at 5; *see* H.R. REP. NO. 99-647, at 19.

121. *Id*

122. *See* S. REP. NO. 99-541, at 3 (quoting OFF. OF TECHNOLOGY ASSESSMENT, OTA- CIT-293, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 44 (1985)); H.R. REP. NO. 99-647, at 18 (quoting OFF. OF TECHNOLOGY ASSESSMENT, OTA- CIT-293, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 44 (1985)).

123. OFF. OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 45 (1985).

124. *See* Hately v. Watts, 917 F.3d 770, 798 (4th Cir. 2019).

125. *Id.*

the Supreme Court and lower courts have subscribed to the idea that judges may deviate from even the clearest statutory texts when a given application would produce otherwise absurd results, as is the case here.[126]

1. The Legislative History's Description of Email Communications in 1986 Provides Support for the Broad Interpretation of Section 2510(17)(B)

While some courts, including the Eighth Circuit, have asserted that the SCA enacted in 1986 is often difficult to reconcile with modern email services,[127] the common form of email outlined in the SCA's legislative history bears many similarities to modern webmail.[128] For example, the Senate Report used the following language:

> [M]essages are typed into a computer terminal, then transmitted over telephone lines to a recipient computer operated by an electronic mail company. If the intended addressee subscribes to the service, the message is stored by the company's computer 'mailbox' until the subscriber calls the company to retrieve its mail, which is then routed over the telephone system to the recipient's computer.[129]

Similarly, modern webmail services have senders from one service transmit a message to the recipient's webmail service.[130] The webmail service then stores the messages on a cloud server until the recipient retrieves it through an Internet connection on a browser, mobile application, or email client.[131] Congress's understanding of email in 1986 could apply to webmail simply by replacing "telephone lines" with 'internet connection.'[132]

Congress also seems to explicitly envision protection for emails in inboxes, opened or unopened, in the legislative history. For example, "[a]n 'electronic mail' service, which permits a sender to transmit a digital message to the service's facility, where it is held in storage until the addressee requests it, would be subject to Section 2701."[133] In modern parlance, emails stored on a webmail provider's servers until someone opens their inbox to view those emails closely aligns with this language. The House Report provides very little evidence that Congress intended to limit section 2701's protections to the period before a recipient opens an email.[134] The Senate Report notes that

---

126. John F. Manning, *The Absurdity Doctrine*, 116 HARV. L. REV. 2387, 2388 (2003).

127. *See* Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 839 (8th Cir. 2015) ("It is not always easy to square the decades-old SCA with the current state of email technology.").

128. *See Hately*, 917 F.3d at 792.

129. S. REP. NO. 99-541, at 8 (1986).

130. *See Hately*, 917 F.3d at 792.

131. *Id.*

132. S. REP. NO. 99-541, at 8.

133. H.R. REP. NO. 99-647, at 63 (1986).

134. *See Hately*, 917 F.3d at 793.

"a computer mail facility authorizes a subscriber to access information in their portion of the facilit[y]'s storage. Accessing the storage of other subscribers without specific authorization to do so would be a violation of the [SCA]."[135] Here, the cloud as supported by a webmail provider's servers matches up closely with "computer mail facility."[136] This report also does not draw a distinction between the periods before and after a user first views a message.[137] Technology may have advanced significantly, but email still works similarly enough to reconcile how Congress understood email in 1986 with modern email services. This again points to the unopened/opened divide in legal protections being an unnecessary, judicially created distinction contravening Congress's intent.

C. The Fourth Circuit's Key Interpretive Innovations

The Fourth Circuit's key interpretive innovations in *Hately*, compared to the Ninth Circuit's opinion in *Theofel*, should make the more recent opinion's advocacy for a broad reading of section 2510(17)(B) and protecting opened emails under the SCA a definitive next step for courts. Most importantly, *Hately* recognizes that modern email services create any number of backup copies of a given email for their own purposes and those of a user: meaning that an opened email is just another copy made for the "backup purposes" of both the email service and the user.[138] The court also directly addressed the counterargument to the broad reading of section 2510(17)(B) that "backup protection" only refers to messages stored for the purposes of the email service.[139]

1. Mass Data Redundancy Maintained by Email Service Providers Should Control the Interpretation of Section 2510(17)(B)

One of the weaknesses of the Ninth Circuit's *Theofel* ruling is that it was decided in the context of an email client before webmail had gained widespread adoption.[140] The Fourth Circuit, on the other hand, brings the broad reading of section 2510(17)(B) into the modern era in its discussion of the email services provided today. The *Hately* ruling both acknowledges and incorporates the reality of modern email services. Specifically, the court recognizes that services such as Gmail or Outlook typically "utilize completely redundant systems consisting of multiple data servers."[141] In these systems, a single email is stored on multiple servers, likely in different

135. S. REP. NO. 99-451, at 36.
136. *Id.*
137. *See Hately*, 917 F.3d at 793.
138. *Id.* at 793-94.
139. *See infra* notes 150-57.
140. *See generally* Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).
141. Brief for the Center for Dem. & Technology et al. as Amicus Curiae Supporting Plaintiff-Appellant and Reversal at 22, Hately v. Watts, 917 F.3d 770 (4th Cir. 2019).

locations around the country, or even around the world.[142] Email services store copies of messages on multiple servers to decrease email downtime and prevent loss of information from servers.[143] For email services, each copy of an email message serves as a substitute for the many other copies stored by the service.[144] Furthermore, when a recipient of an email chooses to view the email via a web browser or application on some device, a copy of the message is sent to the user's device and temporarily stored in the device's short-term or long-term memory.[145] For this reason, the copies retained by the email service also provide backups for any copies downloaded to a physical device and vice versa.[146] In light of this redundancy and the plain meaning of backup protection being to protect computer data from damage or destruction, the argument that unopened emails are stored for the "purposes of backup protection," but opened emails are not, strains credulity. Using the Eighth Circuit's understanding of the statutory language in *Anzaldua*, the emails are stored in due course *and* for the purposes of backup protection by email service providers.[147]

2. "Backup Protection" Does Not Just Apply to Copies Made for the Service Provider's Purposes

One argument made against the broad interpretation of "backup protection"—that this language exclusively covers copies made for the service provider's own administrative purposes rather than also covering copies made for a user's purposes—does not pass analytical muster.[148] Theoretically, this reading would exclude opened emails, as these would be considered copies made solely for the user's purposes when the user decided not to delete them. This argument is based on the assertion that section 2704's

---

142. *See Id*.

143. *See Id.*

144. *See id.*; *see also Reliability*, GOOGLE CLOUD HELP, https://support.google.com/googlecloud/answer/6056635?hl=en (last visited Feb. 6, 2021) ("[A]ll Google systems are inherently redundant by design, and each subsystem is not dependent on any particular physical or illogical server for ongoing operation. Data is replicated multiple times across Google's clustered active servers so that, in the case of machine failure, data will still be accessible through other systems."); Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECHNOLOGY L. 359, 361 (2010) ("Cloud computing services provide consumers with vast amounts of cheap, redundant storage and allow them to instantly access their data from a web-connected computer anywhere in the world.").

145. *See* Hately v. Watts, 917 F.3d 770, 792 (4th Cir. 2019).

146. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004); Cheng v. Romo, No. 11-10007-DJC, 2013 WL 6814691, at *7-9 (D. Mass. 2013) (holding that copies of delivered and opened emails accessed through a web-based email client were in "storage" for purposes of Subsection (B)); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008); Bailey v. Bailey, No. 07-11672, 2008 WL 324156, at *5-6 (E.D. Mich. 2008) ("The plain language of the statute seems to include emails received by the intended recipient where they remain stored by an electronic communication service.").

147. *See* Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 840-42 (8th Cir. 2015).

148. *See Anzaldua*, 793 F.3d at 842.

definition of backup copy, "a copy made by the service provider for administrative purposes," should be interchangeable with that of "backup protection."[149] However, section 2704 reads in full that the government "may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of contents of the electronic communications sought in order to preserve communications."[150] The term "backup copy" in the context of section 2704 then refers to copies of electronic communications created by a service provider pursuant to a court order, rather than copies made during an email service's day-to-day operations. Also, nothing in the SCA's definition of "electronic storage," section 2704, or the statute's legislative history provides support for the argument that Congress intended for "backup protection" and "backup copy" to have the same meaning.[151]

Even assuming that "backup protection" does only refer to copies made for the service provider's own administrative purposes, opened emails would still fall under this definition because of the redundancy discussed above.[152] "Administrative" simply means "relating to the running of a business, organization, etc."[153] Numerous copies of emails are created for the administrative purposes of decreasing email downtime, protecting against data loss, and advertisement targeting.[154] Therefore, even under this more restrictive definition of "backup protection," copies made by the service provider of both unopened and opened emails are made for administrative purposes under the "backup copy" definition from section 2704. However, this insertion of section 2704's definition of "backup copy" into section 2510(17)'s definition of "electronic storage" does not make sense. Furthermore, nothing in the SCA requires that "backup protection" be solely for the benefit of the email service provider, while conversely, the legislative history expressly envisions "backup protection" for the benefit of the user.[155]

D. Policy Considerations

1. Unopened/ Opened Distinction as an Unreliable Proxy for the Receipt of Email Communications

Because modern email services have a feature that enables a user to mark an email as read or unread, the unopened/opened distinction advocated by some courts and commentators becomes even more arbitrary, and possibly

149. Kerr, *supra* note 36, at 1217.

150. Stored Communications Act, 18 U.S.C. § 2704(a)(1).

151. *See Hately*, 917 F.3d at 794.

152. *Id.*; *see supra* Part III, Section C1.

153. *Administrative*, Meriam-Webster.com, https://www.merriam-webster.com/dictionary/administrative [https://perma.cc/VS2S-URY9].

154. Brief for the Center for Dem. & Technology et al. as Amicus Curiae Supporting Plaintiff-Appellant and Reversal at 22, Hately v. Watts, 917 F.3d 770 (4th Cir. 2019).

155. *See* H.R. NO. 99-647, at 68 (1986) (noting "[b]ackup protection preserves the integrity of the electronic communication system and to some extent preserves the property of users of such a system.").

unworkable. Under the narrow reading of section 2510(17)(B), opened emails do not fall under the SCA's definition of electronic storage because their storage is not incidental to the transmission of that message.[156] Essentially, once the email message has been opened, it no longer falls under this interpretation's understanding of electronic storage because the communication is complete, received, and no longer stored "incidental to the electronic transmission thereof."[157] However, if protections under the law are supposed to turn on this distinction, raising the ability to mark emails as read or unread as a defense would require courts to perform an inquiry into whether emails were actually opened, instead of simply being marked as read. Alternatively, an email could have been opened and then marked as unread by the user. Otherwise, courts ascribing to this interpretation would not know the truth of whether the transmission of the email had actually been completed under their own standard. Furthermore, cybercriminals and hackers could simply mark an unopened email that they opened as unread to cover their tracks, potentially requiring further investigation by courts.

The unopened/opened distinction can raise serious judicial efficiency issues if most section 2701 cases involving email would require forensic analysis of metadata by Google or Microsoft employees to determine whether this feature was used to distort the relevant facts under what is already an arbitrary, absurd interpretation. The email service provider may not retain this data indefinitely or may not have the capability to perform analysis with the granularity required to differentiate actions taken by the user from those of a cybercriminal using their username and password. This process could also substantially increase litigation costs, depending on whether an email service can proffer this information or whether further experts would need to be brought in. The very first rule of the Federal Rules of Civil Procedure outlining their scope and purpose focuses on securing just, speedy, and inexpensive determinations of every action or proceeding.[158] From a policy perspective, interpreting section 2510(17)(B) narrowly to exclude previously opened emails directly contravenes the goal of both speedy and inexpensive determinations.

2. Holding Cybercriminals Accountable, Making Americans Feel Safer and More in Control of Their Personal Data, and Providing Standing for Victims of Certain Data Breaches

Other practical policy considerations also weigh heavily in favor of the broad interpretation of section 2510(17)(B). Holding a cyber-criminal accountable for accessing your emails, unopened and opened, prior to full-fledged identity theft or other fraud, is a substantial government interest consistent with the SCA's intended purpose: to address the growing problem of unauthorized persons deliberately gaining access to electronic

156. Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 842 (8th Cir. 2015).
157. Kerr, *supra* note 36, at 1216.
158. FED. R. CIV. P. 1 (last amended Dec. 1, 2015).

communications not intended for the public.[159] Protecting email inboxes more thoroughly can also contribute to more positive views of data security by making citizens feel safer, or, at a minimum, to restore some agency by expanding the SCA's private right of action. Another practical rationale for this form of protection is the difficulty data breach plaintiffs face in demonstrating Article III standing, in particular, the injury-in-fact element, following *Clapper v. Amnesty International*.[160] Taking a broader view on inbox protections can enable victims of hacks, including those affected by the Yahoo incident, to hold wrongdoers accountable for their efforts to take personal or business data from inboxes, despite some divided authority on whether actual damages are a prerequisite for awarding statutory damages.[161]

3. The Supreme Court Should Grant Certiorari or Congress Should Amend the SCA

Although widespread adoption of the *Hately* decision's broad interpretation of section 2510(17)(B) is a starting point for consistent application of the relevant statutory language, the depth of the circuit split and the sheer number of courts that have weighed in on the issue may make this adoption difficult. For this reason, the Supreme Court should take up a case involving the unopened/opened divide concerning SCA protections to resolve the circuit split once and for all. Some such cases have been appealed to the Supreme Court, including *Jennings v. Jennings*, but certiorari has never been granted.[162] In the alternative, Congress should update and amend the SCA to clearly protect opened emails. Congress could also take steps to protect email inboxes even further by removing the outdated "facility" language, which does not protect against someone simply accessing your email account through your personal device, from any subsequent proposed legislation.[163]

IV. CONCLUSION

Congress passed the SCA to fill gaps in legal protections for electronic communications and the resulting legal uncertainties.[164] Although technology has developed rapidly in the last thirty-five years, Congress's discussion of email services in 1986 bears striking resemblance to modern webmail.[165] The arbitrary distinction between the protections afforded to unopened and opened emails is an absurd result Congress almost certainly did not intend, even back

159. H.R. REP. NO. 99-647, at 62.

160. *See* Clapper v. Amnesty Int'l, 133 S. Ct. 1138, 1140-1141 (2013) (holding speculative, future harms do not establish Article III standing).

161. *See supra* notes 29-30.

162. Jennings v. Jennings, 736 S.E.2d 242, 250 (S.C. 2012), *cert. denied sub nom.* Jennings v. Broome, 133 S. Ct. 1806, 1806 (2013).

163. *See generally* Electronic Communications Privacy Act, 18 U.S.C. § 2701(a).

164. *See supra* Part III, Section B.

165. *See supra* Part III, Section B1.

in 1986.[166] The jurisprudential influence of the Ninth Circuit's *Theofel* decision is inhibited by its discussion of traditional email clients, rather than webmail, and its failure to respond to some of the key arguments against the broad reading of section 2510(17)(B). The Fourth Circuit's *Hately* decision resolves both issues while accounting for other facets of modern technology. Most importantly, the *Hately* decision recognizes the reality of mass email redundancy within the systems of email service providers and the impact this has on the interpretation of "for the purposes of backup protection."[167] Furthermore, the ability to mark an email as read or unread may make the unopened/opened distinction advocated by some courts and commentators unworkable if this were to be raised as a defense. In the meantime, Americans face uncertainty in the protection of their email inboxes which leaves them vulnerable to cybercriminals and identity theft. Courts across the country should adopt the Fourth Circuit's interpretation of section 2510(17)(B) of the SCA which protects opened emails because of the comprehensive nature of the court's arguments regarding the statute's plain text, legislative history, the absurdity doctrine, the superfluity doctrine, and technological developments, as well as common sense and independent policy considerations. The last thirty-five years have seen technologies, including email communications, evolve and develop at an unprecedented rate. Given the compelling arguments made by the Fourth Circuit and the important policy considerations discussed above favoring the broad reading of section 2510(17)(B), opened emails should be and must be protected under the Stored Communications Act.

166. *See supra* Part III, Section B.
167. *See supra* Part III, Section C1.