EDITOR'S NOTE

Welcome to the third Issue of Volume 66 of the *Federal Communications Law Journal*, the nation's premier communications law journal and the official journal of the Federal Communications Bar Association.

The centerpiece of this Issue is a series of four essays on the D.C. Circuit's decision in *Verizon v. FCC*, which struck down the core provisions of the Commission's 2010 Open Internet Order. The court's holding in that case has prompted vigorous discussion over the past year on the scope of the Commission's authority to adopt rules promoting the Open Internet and the policy consequences of doing so. In this Issue, five distinguished telecommunications experts contribute essays which variously evaluate the *Verizon* court's legal analysis of the Commission's authority, suggest novel regulatory solutions to challenges facing the Open Internet, and weigh the costs and benefits of regulating last-mile broadband services.

The series begins with an essay by Christopher Yoo, the Founding Director of the Center for Technology, Innovation and Competition and a Professor of Law at the University of Pennsylvania Law School. Prof. Yoo writes to question the propriety of an expansive reading of the Commission's section 706 authority. He articulates meaningful limits on this authority by drawing on precedent relating to section 4(i) ancillary jurisdiction and cautions policymakers against wholesale reclassification of broadband Internet access services.

Next in the Open Internet series is an essay co-authored by Tim Wu, a Professor of Law at Columbia Law School, and Tejas Narechania, the Julius Silver Research Fellow, also from Columbia Law School. In their thought-provoking essay, Prof. Wu and Mr. Narechania evaluate the Commission's authority for regulating broadband Internet access services under Title II of the Communications Act. They describe two potential paths forward for the Commission, one involving the classification of a new "sender-side" telecommunications service that would regulate response transmissions from edge providers, and the other contemplating wholesale reclassification of broadband Internet access service as a telecommunications service under Title II.

The series continues with a contribution from James Speta, Professor of Law at Northwestern University Law School. Pivoting the discussion to a focus on competitive harm, Prof. Speta argues that the Commission should adopt rules based on antitrust principles that would forbid anti-competitive behavior that might have the effect of foreclosing competition.

The series concludes with an essay from former Commissioner Deborah Taylor Tate, who now serves on the Board of Directors for the Minority Media and Telecommunications Council and as a Distinguished Senior Adjunct Fellow at the Free State Foundation, among other positions. Highlighting the poor track record of Commission rules and enforcement actions regarding net neutrality in the courts, Commissioner Tate presents

the case for a light-touch regulatory process that ensures broadband connectivity for all Americans while promoting innovation throughout the Internet ecosystem.

Following the Open Internet series, the Issue presents an essay from Gerald Faulhaber, former Chief Economist at the Commission and Professor Emeritus of Business Economics and Public Policy at the Wharton School of the University of Pennsylvania. In his piece, Prof. Faulhaber responds to Prof. Kevin Werbach's article in Issue 2 about the impending sunset of the public switched telephone network and the corresponding legal, policy, and technological questions raised by such a transition.

In addition to these pieces, this Issue contains two student Notes. In the first Note, Carla Voigt discusses privacy issues in the modern telecommunications environment, uncertainty about the Commission's authority to regulate interception of unencrypted Wi-Fi signals, and possible policy solutions. In the second Note, Michael Sherling examines the FCC's ability to use its ancillary authority to require ISPs to implement cybersecurity standards, concluding that because of critical infrastructure vulnerabilities, the FCC has jurisdiction to implement minimum cybersecurity standards.

The *Journal* is committed to providing its readership with substantive coverage of relevant topics in communications law, and we appreciate the continued support of contributors and readers alike. We welcome your feedback and submissions—any questions or comments about this Issue or future issues may be directed to fclj@law.gwu.edu, and any submissions for publication consideration may be directed to fcljarticles@law.gwu.edu. This Issue and our archive are available at http://www.fclj.org.

Andrew Erber
Editor-in-Chief

FEDERAL COMMUNICATIONS LAW JOURNAL

VOLUME 66 ISSUE 3

JUNE 2014

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 2,500 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 http://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 is 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, D.C., area, the FCBA has ten active regional chapters: Atlanta, Carolina, Florida, Midwest, New England, New York, Northern 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 is the oldest law school in Washington, DC. The school is accredited by the American Bar Association and is a charter member of the Association of American Law Schools. The Law School is located on the GW campus in the downtown neighborhood familiarly known as Foggy Bottom.

GW Law has one of the largest curricula of any law school in the nation with more than 250 elective courses covering every aspect of legal study. GW Law's home institution, the George Washington University, is a private, nonsectarian institution founded in 1821 by charter of Congress.

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 St. NW, Suite LL-020, Washington, D.C., 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 St. NW, Suite 325, Washington, D.C., 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 send all requests for address changes or other subscription-related questions to fcljsubscribe@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 fcljsubscribe@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* (19th ed., 2010), copyright by the *Columbia*, *Harvard*, and *University of Pennsylvania Law Reviews* and the *Yale Law Journal*. 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 66 FED. COMM. L.J. ___ (2014).

35573-fcl_66-3 Sheet No. 3 Side B 10/21/2014 10:02:02

FEDERAL COMMUNICATIONS LAW JOURNAL

GW LAW

FCBA FEDERAL COMMUNICATIONS BAR ASSOCIATION

VOLUME 66 ISSUE 3

JUNE 2014

ESSAYS

The D.C. Circuit's January 2014 decision in *Verizon v. FCC* represented a major milestone in the debate over network neutrality that has dominated communications policy for the past decade. This article analyzes the implications of the D.C. Circuit's ruling, beginning with a critique of the court's ruling that section 706 of the Telecommunications Act of 1996 gave the Federal Communications Commission (FCC) the authority to mandate some form of network neutrality. Examination of the statute's text, application of canons of construction such as *ejusdem generis* and *noscitur a sociis*, and a perusal of the statute's legislative history all raise questions about the propriety of the court's conclusion. Moreover, the precedents on ancillary jurisdiction and common carriage impose limits to the FCC's section 706 jurisdiction, preventing the FCC from regulating content before or after it is in transit and likely barring the FCC from imposing a strict nondiscrimination mandate. A revised rule based on commercial reasonableness as initially proposed by the FCC could accomplish many of the goals of network neutrality without running afoul of these prohibitions.

Reclassification of broadband Internet access to bring it within the regulatory regime governing traditional telephone service (known as Title II) faces substantial statutory obstacles, would not prevent prioritization of services, and ignores the longstanding problems associated with common carriage regulation and forbearance. The legislative history of section 706 also suggests that the FCC has the authority to preempt the concurrent jurisdiction accorded to state retaliatory authorities. Moreover, calls to extend network neutrality to interconnection between networks overlooks the fact that such arrangements are not universal and instead are based on some type of reciprocity and that requiring zero-price interconnection would ignore the important role played by prices and by bilateral negotiations. The article closes by examining five early examples of network neutrality disputes: MetroPCS/YouTube, AT&T/Apple FaceTime, Verizon/Google tethering apps, Verizon/Google Wallet, and the Amazon Kindle/zero-rating. These cases demonstrate the difficulties surrounding the implementation of network neutrality rules.

In January 2014, the U.S. Court of Appeals for the D.C. Circuit struck down the FCC's 2010 Open Internet Order, which contained the Commission's net neutrality rules. The Commission has since indicated that it will take up the D.C. Circuit's invitation to implement rules that, consistent with historic practice, meet the court's test for preventing improper blocking and discrimination of Internet traffic. In this essay, we consider the Commission's options for a path forward under Title II of the Communications Act. We find that the FCC has at least two available paths. The first is predominantly legal: by adopting the two-stage framework articulated by the D.C. Circuit characterizing broadband transactions as including a call and a response, the Commission can conclude that response, or sender-side, transmissions are a telecommunications service under the statute. The second path is predominantly factual: the Commission can consider whether it is still swayed by its analysis, now well over a decade old, that analogizes broadband subscription services to dial-up Internet access. Regardless of the path the Commission chooses, it will reach a similar destination. Either course allows the Commission to meet the promise to prevent improper blocking and discrimination.

The D.C. Circuit's decision in *Verizon v. FCC*, holding that the FCC may regulate broadband but that its nondiscrimination rules were impermissible common carrier regulation of information services, leaves the FCC with few options going forward. Somewhat surprisingly, the D.C. Circuit did not leave the FCC the customary administrative law option of a better explanation for why its nondiscrimination rules were different from common carriage (even though, as I discuss here, such an explanation may have been possible). As a result, the Commission's best path—both doctrinally and as a policy matter—is to adopt rules based on an antitrust foundation: rules that forbid behavior that may have the effect of foreclosing competition. To be sure, the very best option would be for Congress to act to set fundamental policy in this area (one way or another), but the prospects of that seem slim. This short essay discusses why a competition-law based rule would meet many of the FCC's Open Internet goals and why the FCC should act, even though both the Department of Justice and the Federal Trade Commission have specific antitrust authority.

35573-fcl_66-3 Sheet No. 4 Side B 10/21/2014 10:02:02

In January 2014, the Federal Communications Commission suffered its second defeat before the U.S. Court of Appeals for the D.C. Circuit regarding the agency's authority to impose so-called "net neutrality" regulation on broadband Internet providers. Despite these losses, the FCC is now developing a third version of net neutrality rules. As a former FCC Commissioner who experienced firsthand the investigation of Comcast's network management practices, I fear that net neutrality rules would undermine competition and consumer choice.

The Internet has enabled unfathomable innovation and investment, democratizing commerce and unleashing the entrepreneurial forces of countless individuals—including many women and minorities. Net neutrality regulation would endanger this virtuous cycle, turning the clock backwards toward the highly regulated era of telephone service as a public utility. Broadband providers should be free to negotiate with content companies to finance the networks of tomorrow. The FCC, like the nation, faces real challenges, from spectrum allocation to broadband adoption. We must refrain from regulation taking aim at shadows if we are to realize the promise of unleashing the very best America has to offer to our consumers, our creators, our children and, indeed, the world.

Professor Kevin Werbach's excellent article in Issue 2, *No Dialtone: The End of the Public Switched Telephone Network*, tees up an extremely important emerging issue for telecommunications policy: how are we to deal with the imminent demise of the PSTN? As telephony moves from copper wire to IP-based technology, functionality will improve and costs will decrease—but in getting from here to there, regulators, telephone companies, and customers face a very costly transition. Werbach outlines the problems quite well; however, his conclusion and recommendations include not only continued regulation, but the extension of such regulation to the Internet. His rationale for extending regulation to the Internet is quite weak, and in my view, potentially devastating to the Internet as we know it. We are in danger of allowing the telephony tail to wag the Internet dog, to its ultimate detriment.

35573-fcl_66-3 Sheet No. 5 Side A 10/21/2014 10:02:02

NOTES

FCC has jurisdiction to implement minimum standards because of the potential for cybersecurity flaws, due to a lack of minimum security standards, to cause catastrophic failure of the communications network.

Because of the FCC's knowledge, institutional competence, and experience with the communications industry, it is in a better position to examine potential regulations and solutions to cybersecurity woes than other government agencies. This Note considers whether the FCC *should* exercise its ancillary authority, concluding that government intervention is justified by the market failure in information about vulnerability to cyber-attacks, together with the compelling need for reliable communications. The Note concludes with a brief discussion of the costs and benefits of potential regulation.

35573-fcl_66-3 Sheet No. 6 Side A 10/21/2014 10:02:02

35573-fcl_66-3 Sheet No. 6 Side B 10/21/2014 10:02:02

Wickard for the Internet? Network Neutrality After *Verizon v. FCC*

Christopher S. Yoo*

TABLE OF CONTENTS

* John H. Chestnut Professor of Law, Communication, and Computer & Information Science and Founding Director of the Center for Technology, Innovation and Competition, University of Pennsylvania.

I. INTRODUCTION

The U.S. Court of Appeals for the District of Columbia Circuit's long-awaited decision in *Verizon v. FCC*[1] represents a major milestone in the debate over network neutrality that has dominated communications policy for the past decade. In upholding some parts while striking down other parts of the FCC's Open Internet Order,[2] the court reached two major conclusions that together represent both a partial victory and partial defeat for proponents and opponents of network neutrality alike. First, the court ruled that section 706 of the Telecommunications Act of 1996[3] affirmatively grants the FCC the authority to regulate broadband access providers' treatment of Internet traffic.[4] Second, the court ruled that the Order's nondiscrimination and anti-blocking rules represented an invalid exercise of that authority because they contravened other express statutory mandates.[5]

In striking down these rules, the court appeared to provide a roadmap showing a way to reconstitute nondiscrimination and anti-blocking rules that would withstand judicial scrutiny.[6] Wanting to avoid the risk of being rebuked on network neutrality a third time, FCC Chairman Tom Wheeler proposed rules that adhered closely to the path laid out by the court with respect to the nondiscrimination and anti-blocking rules, while beefing up the transparency rules that withstood judicial review.[7] Advocates of network neutrality criticized the proposal for its failure to reinstate a nondiscrimination mandate.[8] The resulting political pressure led Chairman Wheeler to include language in the proposed rule seeking comment on the more radical step of bringing broadband access within the regulatory regime that governs traditional telephone service.[9] Nondiscrimination has thus emerged as the focus of the network neutrality debate. Although the Open Internet Notice of Proposed Rulemaking that the FCC adopted on May 15, 2014, attempts to characterize nondiscrimination as part of a decade-long,

---

1. 740 F.3d 623 (D.C. Cir. 2014).
2. Preserving the Open Internet, *Report and Order*, 25 FCC Rcd. 17905 (2010) [hereinafter *2010 Open Internet Order*], *aff'd in part, rev'd in part sub nom.* Verizon v. FCC, 740 F.3d 623, 636–42 (D.C. Cir. 2014).
3. 47 U.S.C. § 1302 (2006).
4. 740 F.3d at 635–49.
5. *Id.* at 649–59.
6. *Id.* at 657–58.
7. Protecting and Promoting the Open Internet, *Notice of Proposed Rulemaking*, 29 FCC Rcd. 5561, 5585–92 paras. 66–86, 5595–98 paras. 94–104, 5602–08 paras. 116–136 (2014) [hereinafter *2014 Open Internet NPRM*], *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-14-61A1.pdf.
8. *See, e.g.*, Edward Wyatt, *F.C.C., in a Shift, Backs Fast Lanes for Web Traffic*, N.Y. TIMES, Apr. 24, 2014, at A1, *available at* http://www.nytimes.com/2014/04/24/technology/fcc-new-net-neutrality-rules.html?_r=0.
9. 2014 Open Internet NPRM, *supra* note 7, at 5612–16 paras. 148–155.

bipartisan policy,[10] nondiscrimination did not appear in either Chairman Michael Powell's initial 2004 exposition of Internet freedoms[11] and from the FCC's 2005 Policy Statement.[12] Instead, nondiscrimination emerged as an issue somewhat later in the debate, when Commissioner Michael Copps began to call for it in a series of separate statements and speeches.[13] Moreover, the FCC attempts to characterize its actions in the SBC/AT&T, Verizon/MCI, and AT&T/BellSouth mergers and the Adelphia spinoff as supporting network neutrality.[14] As a formal matter, however, in each of those cases the FCC actually found competition to be sufficiently robust and the record sufficiently bare of evidence of discrimination to justify declining to mandate nondiscriminatory access to their last-mile broadband networks, although the FCC did accept voluntary commitments to abide by the 2005 Policy Statement as being in the public interest.[15]

---

10. *Id.* at 5565–69 paras. 11–24.

11. Michael K. Powell, Chairman, FCC, Preserving Internet Freedom: Guiding Principles for the Industry, Remarks Delivered to the Silicon Flatirons Symposium (Feb. 8, 2004), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-243556A1.pdf.

12. *See* Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, *Policy Statement*, 20 FCC Rcd. 14986 (2005).

13. *See, e.g.*, Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications, *Memorandum Opinion and Order*, 23 FCC Rcd. 13028, 13080 (2008) (statement of Copps, Comm'r); Broadband Industry Practices, *Notice of Inquiry*, 22 FCC Rcd. 7894, 7903 (2007) (Copps, Comm'r, concurring); Applications for Consent to the Assignment and/or Transfer of Control of Licenses, Adelphia Communications Corp., (and Subsidiaries, Debtors-in-Possession), Assignors, to Time Warner Cable Inc. (Subsidiaries), Assignees Adelphia, Communications Corp., (and Subsidiaries, Debtors-in-Possession), Assignors and Transferors, to Comcast Corp. (Subsidiaries), Assignees and Transferees, Comcast Corp., Transferor, to Time Warner Inc., Transferee, Time Warner Inc., Transferor, to Comcast Corp., Transferee, *Memorandum Opinion and Order*, 21 FCC Rcd. 8203, 8368 (2006) (Copps, Comm'r, dissenting); Michael J. Copps, Acting Chairman, Fed. Commc'ns Comm'n, Remarks at the Free Press Summit: Changing Media. (May 14, 2009), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-290735A1.pdf; Michael J. Copps, Comm'r, Fed. Commc'ns Comm'n, Remarks at Pike & Fischer's Broadband Policy Summit IV (June 12, 2008), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-282890A1.pdf; Michael J. Copps, Comm'r, Fed. Commc'ns Comm'n, Remarks at En Banc Hearing on Broadband Network Management Practices, Stanford University (Apr. 17, 2008), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-281625A1.pdf; Michael J. Copps, Comm'r, Fed. Commc'ns Comm'n, Remarks at En Banc Hearing on Broadband Network Management Practices, Cambridge, Massachusetts (Feb. 25, 2008), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-280440A1.pdf.

14. 2014 Open Internet NPRM, *supra* note 7, at 5566 para. 14.

15. AT&T Inc. and BellSouth Corporation Application for Transfer of Control, *Memorandum Opinion and Order*, 22 FCC Rcd. 5662, 5724–27 paras. 116–120, 5738–39 paras. 151–153 (2007); Applications for Consent to the Assignment and/or Transfer of Control of Licenses: Adelphia Commc'ns Corp., Assignors, to Time Warner Cable Inc., Assignees, Applications for Consent to the Assignment and/or Transfer of Control of Licenses: Adelphia Communications Corporation (and subsidiaries, debtors-in-possession), Assignors, to Time Warner Cable Inc. (subsidiaries), Assignees et al., *Memorandum Opinion and Order*, 21 FCC Rcd. 8203, 8296–99 paras. 217–223 (2006); Verizon Communications, Inc. and MCI, Inc. Applications for Approval of Transfer of Control, *Memorandum Opinion*

This essay explores both of these conclusions. Part I critiques the *Verizon* court's potentially expansive reading of section 706, examining how it may expand FCC's authority beyond broadband access providers to encompass content and application providers (dubbed "edge providers" by the court)[16] and showing how this reading runs counter to standard principles of statutory interpretation. Part II discusses the limitations the court placed on how the FCC can exercise its section 706 authority, concluding that these limits prevent the FCC from imposing the type of nondiscrimination mandate that many regard as the central focus of network neutrality. Part III explores the implications of the court's decision, examining the potential for state broadband regulation, the possibility of Title II reclassification, the future of the wireless exception, and the prospects for a regime based on case-by-case adjudication.

II. SECTION 706 AS A GRANT OF AUTHORITY

The portion of the *Verizon* opinion with the most potentially sweeping implications for the future of the Internet is the court's expansive reading of section 706.[17] Understanding these implications requires some background on the federal communications statute, the Communications Act of 1934. When first enacted, the Act contained six titles, four of which were procedural, not substantive.[18] Title I laid out the general provisions regarding the number, qualifications, and terms of FCC Commissioners and defined a number of statutory terms.[19] Title IV contained provisions governing procedural and administrative matters.[20] Title V addressed penal enforcement and forfeitures.[21] Title VI dealt with miscellaneous housekeeping matters, such as abolishing the Federal Radio Commission—the precursor to the FCC—and transferring its property and personnel to the FCC.[22]

The Act's primary substantive provisions were contained in Title II, which governed common carriers,[23] and Title III, which governed radio

---

and Order, 20 FCC Rcd. 18433, 18507–09 paras. 139–142 (2005); SBC Communications Inc. and AT&T Corp. Applications for Approval of Transfer of Control, *Memorandum Opinion and Order*, 20 FCC Rcd. 18290, 18366–67 paras. 140–143 (2005).

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

17. 47 U.S.C. § 1302 (2006).

18. Ch. 652, 48 Stat. 1064 (codified as amended at scattered sections of 47 U.S.C.).

19. *Id.* §§ 1–5, 48 Stat. at 1064–70 (codified as amended at 47 U.S.C. §§ 151–162 (2006)).

20. *Id.* §§ 401–416, 48 Stat. at 1092–1100 (codified as amended at 47 U.S.C. §§ 401–416 (2006)).

21. *Id.* §§ 501–505, 48 Stat. at 1100–01 (codified as amended at 47 U.S.C. §§ 501–505 (2006)).

22. *Id.* §§ 601–609, 48 Stat. at 1101–05 (codified as amended at 47 U.S.C. §§ 601–609 (2006)).

23. *Id.* §§ 201–221, 48 Stat. at 1070–81 (codified as amended at 47 U.S.C. §§ 201–231 (2006)).

communications.[24] In 1984, Congress replaced the old Title VI with a new substantive title to govern cable communications and renumbered the old procedural Title VI as Title VII.[25]

Three provisions of Title I are particularly relevant to the network neutrality debate. Section 1 recognizes that Congress created the Commission "[f]or the purpose of regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all people of the United States . . . a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges."[26] Section 2(a) provides that "[t]he provisions of this chapter shall apply to all interstate and foreign communication by wire or radio and all interstate and foreign transmission of energy by radio, which originates and/or is received within the United States."[27] Section 4(i) states that "[t]he Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions."[28]

The FCC has sometimes cited these provisions of Title I as if they represented substantive grants of authority.[29] The problem with this approach should be apparent to every law student and lawyer. The FCC has conceded that statements of purpose, like those contained in section 1, delegate no regulatory authority.[30] Moreover, courts and the FCC have analogized section 4(i) to the Necessary and Proper Clause of the Constitution,[31] which authorizes Congress "[t]o make all Laws which shall be necessary and proper for carrying into Execution" the federal government's enumerated powers.[32] Although the Necessary and Proper

---

24. *Id.* §§ 301–329, 48 Stat. at 1081–92 (codified as amended at 47 U.S.C. §§ 301–329 (2006)).

25. Cable Communications Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (codified as amended at 47 U.S.C. §§ 521–559 (2006)).

26. 47 U.S.C. § 151 (2006).

27. 47 U.S.C. § 152(a) (2006).

28. 47 U.S.C. § 154(i) (2006). A similar provision in Title III (governing broadcasting) similarly provides that "the Commission from time to time, as public convenience, interest, or necessity require shall . . . [m]ake such rules and regulations and prescribe such restrictions and conditions not inconsistent with law, as may be necessary to carry out the provisions of this Act." *Id.* § 303(r).

29. *See, e.g.*, Implementation of Video Description of Video Programming, *Report and Order*, 15 FCC Rcd. 15230, 1525–53 para. 54 (2000), *rev'd sub nom.* Motion Picture Ass'n of Am. v. FCC, 309 F.3d 796, 802, 803–06 (D.C. Cir. 2001).

30. Comcast Corp. v. FCC, 600 F.3d 642, 652 (D.C. Cir. 2010).

31. *See, e.g.*, N. Am. Telecomm. Ass'n v. FCC, 772 F.2d 1282, 1292 (7th Cir. 1985); Stale or Moot Docketed Proceedings, 1993 Annual Access Tariff Filing Phase I, *Order*, 19 FCC Rcd. 2527, 2531 para. 12 (2004); Adoption of a Mandatory FCC Registration Number, *Notice of Proposed Rulemaking*, 15 FCC Rcd. 24370, 24378 n.31 (2000); Review of the Pioneer's Preference Rules, *Memorandum Opinion and Order on Remand*, 9 FCC Rcd. 4055, 4062 para. 29 & n.70 (1994); Application of Nationwide Wireless Corp., *Memorandum Opinion and Order*, 9 FCC Rcd. 3635, 3641 para. 26 & n.75(1994).

32. U.S. CONST. art. I, § 8, cl. 18.

Clause extends Congress' authority beyond the strict letter of the enumerated powers, it is not itself a separate grant of authority. It still must be exercised with respect to some enumerated power granted to Congress by Article I, Section 8, or some other explicit provision of the Constitution.[33]

Nonetheless, the FCC has repeatedly invoked these provisions as if they were independent grants of authority to regulate Internet access. For example, in the *Second Computer Inquiry*, the FCC ruled that the enhanced services that were the direct antecedent to the Internet[34] were not subject to Title II.[35] Instead, the FCC relied on its Title I jurisdiction, explicitly rejecting the argument that the provisions of Titles II or III in any way limited its authority.[36] The D.C. Circuit affirmed both conclusions on judicial review.[37] Over two decades later, dicta in the Supreme Court's decision in *National Cable & Telecommunications Association v. Brand X Internet Services* similarly suggested that the FCC possessed ancillary authority under Title I to impose access requirements on broadband access providers.[38] However, the D.C. Circuit's 2005 decision in *American Library Association v. FCC* made clear that the FCC must do more than simply cite the general provisions from Title I to justify regulating under its ancillary jurisdiction.[39] Ancillary jurisdiction must be invoked with respect to one of the specific statutory responsibilities Congress delegated to the FCC in the substantive titles of the Communications Act.[40] In 2010, the D.C. Circuit reaffirmed this principle in *Comcast v. FCC*, which overturned the FCC's attempt to sanction Comcast for rate-limiting certain peer-to-peer applications.[41] Together, these decisions stand for the very reasonable proposition that Title I ancillary jurisdiction is not an independent grant of authority. Instead, it must be asserted in conjunction with some explicit substantive grant of

33. For the classic citation, see *McCulloch v. Maryland*, 17 U.S. (4 Wheat.) 316, 421 (1819). For a more recent restatement of this principle, see *Kinsella v. U.S. ex rel. Singleton*, 361 U.S. 234, 247 (1960) ("[T]he Necessary and Proper Clause . . . . is not itself a grant of power, but a caveat that the Congress possesses all the means necessary to carry out the specifically granted foregoing powers of [section] 8 and all other Powers vested by this Constitution." (citations and internal quotation marks omitted)).

34. Nat'l Cable & Telecomm. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 976–77 (2005); Verizon v. FCC, 740 F.3d 623, 629–30 (D.C. Cir. 2014).

35. Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry), *Final Decision*, 77 384, 428–32 paras. 115–123 (1980), *aff'd sub nom.* Computer & Commc'ns Indus. Ass'n v. FCC, 693 F.2d 198 (D.C. Cir. 1982) (*CCIA*).

36. 77 F.C.C.2d at 432 paras. 124–125.

37. *CCIA*, 693 F.2d at 209–11, 213–14.

38. 545 U.S. 967, 976, 996, 1002 (2005), *aff'g* Inquiry Concerning High-Speed Access to the Internet over Cable and Other Facilities, *Declaratory Ruling and Notice of Proposed Rulemaking*, 17 FCC Rcd. 4798, 4841–42 paras. 75–79 (2002) [hereinafter *Cable Modem Declaratory Ruling*].

39. 406 F.3d 689, 691–93, 699–700 (D.C. Cir. 2005).

40. *Id.*

41. 600 F.3d 642, 654–56 (D.C. Cir. 2010).

authority from Congress in Titles II, III, or VI.[42] Simply put, Title I jurisdiction cannot be "ancillary to nothing."[43]

The *Comcast* court then reviewed the statutory provisions that the FCC offered to support its exercise of ancillary jurisdiction, only to find them wanting.[44] Most importantly for this essay's purposes, the court rejected the FCC's attempt to tie its ancillary jurisdiction to section 706, reasoning that the FCC had ruled in an earlier order that section 706 did not represent an independent grant of authority.[45] The opinion implied that the FCC remained free to revisit this conclusion so long as it did so through official agency action and offered a sufficient explanation of its decision to change policies.[46]

The FCC took the D.C. Circuit up on this invitation in issuing the 2010 Open Internet Order, in which the agency explicitly disavowed its earlier conclusion that section 706 was not an affirmative grant of authority.[47] Instead, the FCC concluded that section 706 indeed gave it the authority to regulate broadband service providers' network management practices, such as blocking Voice over Internet Protocol ("VoIP") communications or degrading online video.[48] The D.C. Circuit affirmed this conclusion in *Verizon* on judicial review.[49]

A. The Text of Section 706

Given that section 706 represented the sole basis for the *Verizon* court's conclusion that the FCC has the authority to regulate network management practices,[50] the text of that provision merits close examination. The full statutory provision is as follows:

> (a) The Commission and each State commission with regulatory jurisdiction over telecommunications services shall encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans

42. *See id.* at 654; *Am. Library Ass'n,* 406 F.3d at 699–700.
43. *Am. Library Ass'n,* 406 F.3d at 702.
44. *Comcast*, 600 F.3d at 651–61.
45. *Id.* at 658–59.
46. *See* Nat'l Cable & Telecomm. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 981 (2005) ("Agency inconsistency is not a basis for declining to analyze the agency's interpretation under the *Chevron* framework . . . . For if the agency adequately explains the reasons for a reversal of policy, change is not invalidating, since the whole point of *Chevron* is to leave the discretion provided by the ambiguities of a statute with the implementing agency.") (citations and internal quotation marks omitted); Chevron USA Inc. v. NRDC, 467 U.S. 837, 863 (1984) ("An initial agency interpretation is not instantly carved in stone."); Motor Vehicle Mfrs. Ass'n of U.S. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 42 (1983) ("[R]egulatory agencies . . . must be given ample latitude to adapt their rules and policies to the demands of changing circumstances.") (citations and internal quotation marks omitted).
47. *2010 Open Internet Order*, *supra* note 2, at 17969 n.370.
48. *Id.* at 17969 para. 120.
49. Verizon v. FCC, 740 F.3d 623, 636–42 (D.C. Cir. 2014).
50. *Id.*

> (including, in particular, elementary and secondary schools and classrooms) 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.
>
> (b) The Commission shall, within 30 months after February 8, 1996, and annually thereafter, initiate a notice of inquiry concerning the availability of advanced telecommunications capability to all Americans (including, in particular, elementary and secondary schools and classrooms) and shall complete the inquiry within 180 days after its initiation. In the inquiry, the Commission shall determine whether advanced telecommunications capability is being deployed to all Americans in a reasonable and timely fashion. If the Commission's determination is negative, it shall take immediate action to accelerate deployment of such capability by removing barriers to infrastructure investment and by promoting competition in the telecommunications market.[51]

The *Verizon* court deferred to the FCC's conclusion that subsections (a) and (b) of section 706 each represent affirmative grants of authority.[52] Subsection (a) explicitly authorizes the FCC to use four types of regulatory measures: (1) price cap regulation,[53] (2) regulatory forbearance, (3) measures that promote competition in the local telecommunications market, and (4) other regulating methods that remove barriers to infrastructure.[54] The court held that, although subsection (a) could be read as simply setting forth a statement of congressional policy, it "could just as easily be read to vest the Commission with actual authority to utilize such 'regulating methods' to meet this stated goal."[55] The fact that the court's discussion of subsection (a) focuses exclusively on the scope of "regulating methods" indicates that the court saw (4) as the basis for the FCC's jurisdiction.[56]

---

51. 47 U.S.C. § 1302 (2006).
52. *Verizon*, 740 F.3d at 637–42.
53. Price cap regulation is an alternative approach to setting rates that differed from traditional cost-of-service ratemaking. The traditional approach based rates on the costs incurred by the provider plus a rate of return. Price caps set rates by calculating a base year and then adjusting the rates for inflation and increases in productivity. Because rates were no longer determined by costs, it was hoped that price caps would provide stronger incentives to innovate and reduce costs and eliminate any biases towards capital-intensive solutions. Price caps are generally characterized as a less intrusive approach to setting rates. *See* Christopher S. Yoo, *Is There a Role for Common Carriage in an Internet-Based World?*, 51 HOUS. L. REV. 545, 595–600 (2013).
54. 47 U.S.C. § 1302(a) (2006).
55. *Verizon*, 740 F.3d at 637–38.
56. *Id.*

By its own terms, subsection (b) serves as a grant of authority only if the FCC finds that advanced telecommunications capability is not being deployed in a "reasonable and timely fashion."[57] If so, the FCC is authorized to employ two remedies: (1) removing barriers to infrastructure investment and (2) promoting competition in the telecommunications market.[58] These are essentially identical to the fourth and third measures, respectively, authorized by subsection (a),[59] making the analysis of the scope of the two subsections essentially parallel.

The *Verizon* court held that section 706(b) also gives the FCC statutory authority to regulate broadband providers.[60] Under this provision, if the FCC concludes that "advanced telecommunications capability is [not] being deployed to all Americans in a reasonable and timely fashion," it "shall take immediate action to accelerate deployment of such capability by removing barriers to infrastructure investment and by promoting competition in the telecommunications market."[61] Again, the specified means of "removing barriers to infrastructure investment and . . . promoting competition in the telecommunications market" mirror the language of the third and fourth clauses of section 706(a).[62] Therefore, the same arguments advanced above apply.

More importantly, the FCC is authorized to act under section 706(b) only if it finds that advanced telecommunications capability—defined by the statute to include broadband[63]—is not "being deployed to all Americans in a reasonable and timely fashion."[64] The first five annual reports the FCC issued pursuant to its section 706 inquiry each concluded that broadband deployment met the requisite standard.[65] Only in the FCC's sixth section 706 report—the first one following the D.C. Circuit's decision in *Comcast Corp. v. FCC* to reject the statutory provisions the FCC first proffered as bases for its jurisdiction and the last one issued prior to the *Open Internet Order*—did the FCC find broadband deployment to be inadequate.[66] The *Verizon* court recognized that "[t]he timing of the Commission's determination is certainly

57. 47 U.S.C. § 1302(b) (2006).
58. *Id.*
59. *Id.* § 1302(a).
60. Verizon v. FCC, 740 F.3d 623, 640–42 (D.C. Cir. 2014).
61. 47 U.S.C. § 1302(b) (2006).
62. *Id.*
63. *Id.* § 1302(d)(1) ("The term 'advanced telecommunications capability' is defined, without regard to any transmission media or technology, as high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology.").
64. *Id.* § 1302(b).
65. Inquiry Concerning the Deployment of Advanced Telecomms. Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecomm. Act of 1996, as Amended by the Broadband Data Improvement Act, *Sixth Broadband Deployment Report*, 25 FCC Rcd. 9556, 9693–94 (2010) (McDowell, Comm'r, dissenting).
66. *Id.* at 9558 para. 2.

suspicious."[67] The agency continued to find broadband deployment to be inadequate in its two subsequent section 706 reports.[68]

Under the Bush administration, the FCC was criticized for its tardiness in issuing annual reports.[69] Under the Obama administration, the agency has better adhered to statutory deadlines,[70] consistently issuing its annual section 706 reports somewhere between May and August each year from 2009 to 2012. Had the FCC adhered to this historical pattern, it should have issued its ninth section 706 report no later than August 2013. Instead, two years elapsed until August 2014 when the agency solicited input on its tenth annual section 706 report instead of issuing its ninth annual report despite the fact that two years had passed since the issuance of the eighth report.[71] One can only speculate as to why.

Interestingly, the primary basis for the FCC's 2012 finding that broadband deployment was not reasonable and timely was the fact that, as of June 2011, 19 million Americans—or 6% of the population—lacked access to broadband, which the FCC defined as service providing download speeds of 4 Mbps or higher.[72] As Commissioner Pai pointed out in his dissent, however, if the report had taken into account mobile wireless broadband, it would have reduced the number of unserved Americans to 5.5 million—or 1.7% of the population.[73] Moreover, the 2012 report was based on data

---

67. *Verizon*, 740 F.3d at 642.

68. Inquiry Concerning the Deployment of Advanced Telecomms. Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecomms. Act of 1996, as Amended by the Broadband Data Improvement Act, *Eighth Broadband Progress Report*, 27 FCC Rcd. 10342, 10344 para. 1 (2012) [hereinafter *Eighth Broadband Progress Report*]; Inquiry Concerning the Deployment of Advanced Telecomms. Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecomms. Act of 1996, As Amended by the Broadband Data Improvement Act, *Seventh Broadband Progress Report and Order on Reconsideration*, 26 FCC Rcd. 8008, 8009 para. 1 (2011).

69. MAJORITY STAFF OF H. COMM. ON ENERGY & COMMERCE, 110TH CONG., DECEPTION AND DISTRUST: THE FEDERAL COMMUNICATIONS COMMISSION UNDER CHAIRMAN KEVIN J. MARTIN 13–14 (Comm. Print 2008).

70. *But see* 2014 Quadrennial Regulatory Review — Review of the Commission's Broadcast Ownership Rules and Other Rules Adopted Pursuant to Section 202 of the Telecommunications Act of 1996, *Notice of Proposed Rulemaking*, 29 FCC Rcd. 4371, 4583 (2014) (statement of Wheeler, Chairman) (acknowledging the FCC's failure to complete its quadrennial review of media ownership rules by the 2010 statutory deadline and committing to complete the process by June 2016), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-14-28A1.pdf.

71. Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecomms. Act of 1996, as Amended by the Broadband Data Improvement Act, *Tenth Broadband Progress Notice of Inquiry*, 29 FCC Rcd. 9747 (2014), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-113A1_Rcd.pdf.

72. *Eighth Broadband Progress Report*, *supra* note 68, at 10344 para. 1, 10370 para. 46, 10400–01 para. 135.

73. *Id.* at 10519–20 (Pai, Comm'r, dissenting).

reflecting the earliest stages of the deployment of the fourth-generation wireless technology known as Long-Term Evolution ("LTE").[74] Since that time, Verizon has completed its LTE buildout,[75] while AT&T's LTE network now reaches 80% of the U.S. population and is scheduled for completion by the end of 2014.[76] Sprint and T-Mobile are racing to catch up: each carrier reached at least 200 million people by the end of 2013 and is projected to reach 80% of the country sometime during 2014.[77] In addition, recent studies indicate that Verizon's, AT&T's, and T-Mobile's LTE offerings provide average download speeds of 12 to 19 Mbps and peak download speeds of 49 to 66 Mbps.[78] The near ubiquity of LTE suggests that the number of people who cannot access broadband that meets or exceeds the FCC's 4 Mbps standard is now likely considerably less than the 1.7% reported as of June 2011.[79] And, again, if broadband deployment is reasonable and timely, section 706(b) provides the FCC no authority to act.

B. The Court's Expansive Reading of Section 706

The *Verizon* court made no claim that the nondiscrimination and anti-blocking rules fell within the first three measures authorized by section 706(a). Instead, the court explicitly invoked the fourth type of measure authorized by the statute, focusing its discussion entirely on "regulating methods."[80]

At first glance, a regulation blocking broadband access providers from charging edge providers premium prices for premium services would seem more likely to create barriers to infrastructure investment than to remove

74. *Id.* at 10347–48 para. 6.

75. Christopher S. Yoo, *Technological Determinism and Its Discontents*, 127 HARV. L. REV. 914, 923–24 (2014).

76. *Id.*

77. *Id.*

78. *Id.* at 923. Some commentators argue that even though LTE is able to delivery faster download speeds, monthly data caps prevent wireless broadband from being a true substitute for fixed broadband. *See* Hibah Hussain et al., New Am. Found. Open Technology Inst., *Capping the Nation's Broadband Future?* 12 (2012), *available at* http://newamerica.net/sites/newamerica.net/files/policydocs/CappingTheNationsBroadbandFuture.pdf. This argument ignores the fact that while LTE providers initially focused on the broadest possible coverage, they have now turned towards densification, which increases the capacity of the network. These arguments are also undercut by the fact that two of the national providers (T-Mobile and Sprint) offer unlimited data plans.

79. *Eighth Broadband Progress Report*, *supra* note 68, at 10519–20 (Pai, Comm'r, dissenting).

80. Verizon v. FCC, 740 F.3d 623, 636–40 (D.C. Cir. 2014).

them.[81] Such a rule would, after all, benefit edge providers at the expense of broadband Internet access providers.[82]

Nevertheless, the court accepted the FCC's assertion that fostering and preserving edge providers represented an important indirect way to promote infrastructure investment.[83] The FCC reasoned that nondiscrimination and anti-blocking rules facilitate innovation by edge providers, thereby leading to increased demand for bandwidth by end users and spurring greater investment in infrastructure in turn.[84] Read in this manner, section 706 authorizes the FCC not only to adopt measures that promote investment in infrastructure directly, but also to promote activities that tangentially encourage infrastructure investment.

What is most striking about this reasoning is its potential expansiveness. Under this approach, the FCC would not only have the authority to institute measures that promote infrastructure investment directly, but also to regulate anything that indirectly affects infrastructure investment as well. In this sense, the court's reasoning is similar to the reasoning followed in a case well known to every first-year law student: *Wickard v. Filburn*.[85] The explicit terms of the Commerce Clause of the Constitution give Congress the power to regulate only commerce "with foreign Nations, and among the several States, and with the Indian Tribes."[86] Before *Wickard*, the Supreme Court forbade the federal government from asserting jurisdiction over commerce that was purely intrastate.[87] In *Wickard*, however, the Court abandoned this vision of dual sovereignty and extended federal jurisdiction to purely intrastate activities that had a tangential impact on interstate commerce.[88] Because almost everything has a putative tangential impact on commerce, *Wickard* opened the door to an expansion of the commerce power such that left few activities outside its scope.[89]

The *Verizon* court's reasoning about section 706 could potentially have a similar effect. Expanding the FCC's jurisdiction beyond activities that

---

81. *See* Brief for Appellant at 30–31, Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014) (No. 11-1355) ("[T]he Commission's daisy chain of speculative inferences that the rules will encourage deployment is contradicted by the record and common sense: regulations that require providers to carry all traffic and prohibit compensation from edge providers for carriage will have precisely the opposite effect, as world-renowned economists explained below.").

82. *Id.*

83. 740 F.3d at 634, 643–45.

84. *Id.*

85. 317 U.S. 111 (1942).

86. U.S. CONST. art. I, § 8, cl. 3.

87. *See, e.g.*, Hammer v. Dagenhart, 247 U.S. 251 (1918).

88. *Wickard*, 317 U.S. at 124.

89. *See, e.g.*, Gonzales v. Raich, 545 U.S. 1 (2005); Hodel v. Va. Surface Mining & Reclamation Ass'n, 452 U.S. 264 (1981); Perez v. United States, 402 U.S. 146 (1971); Katzenbach v. McClung, 379 U.S. 294 (1964); Heart of Atlanta Motel v. United States, 379 U.S. 241 (1964). For the exceptions, which are notable primarily for their rarity, see *United States v. Morrison*, 529 U.S. 598 (2000); and *United States v. Lopez*, 514 U.S. 549 (1995).

have a *direct* impact on infrastructure investment to encompass those that have a *tangential* impact on infrastructure investment represents a significant extension of the FCC's power. Indeed, it potentially leaves the door open for the FCC to take measures aimed directly at the content and application industries—a prospect widely feared by advocates and critics of network neutrality alike.[90] The history of FCC regulation of broadcast television networks is instructive. After initially denying that it had the authority to regulate television networks directly, the FCC later invoked an expansive reading of ancillary jurisdiction to impose a wide range of restrictions on them.[91] The FCC could well follow the same course here and eventually regulate edge providers, although, as discussed below, the D.C. Circuit's precedents on ancillary jurisdiction do impose some limits on the FCC's authority.

C. The Impact of the Canons of Construction

Proper application of well-established principles of administrative law and statutory construction indicate that the *Verizon* court should not have condoned the FCC's construction of section 706 so readily. As the *Verizon* court correctly observed,[92] the proper standard for reviewing an agency's construction of its statutory authority is the familiar two-step analysis established by the Supreme Court in *Chevron USA Inc. v. Natural Resources Defense Council, Inc.*[93] In step one, a reviewing court asks whether the statute's text "directly addresse[s] the precise question at issue."[94] If not, step two requires that the court defer to the agency's construction of the statute so long as it is reasonable or permissible.[95]

Arguably, the *Verizon* court's analysis of section 706 fails at step one. *Chevron* itself recognizes that in step one, a court should employ the "traditional tools of statutory construction."[96] These tools are generally recognized to include descriptive canons of construction that reflect the

---

90. *See, e.g.*, Comments of Public Knowledge and Common Cause at 28, Open Internet Remand, *Public Notice*, FCC GN Docket No. 14-28 (rel. Feb. 19, 2014), *available at* https://www.publicknowledge.org/assets/uploads/documents/Public_Knowledge_Common_Cause_Open_Internet_706_Public_Notice_Comments.pdf ("The breadth of authority contained with these principles raises the possibility of the Commission having authority to promulgate rules of all sorts, so long as they could rationally be said to contribute to the deployment of broadband. For instance, the case could be made that the prevalence of adult content online was discouraging certain households from adopting broadband; therefore, decency regulations on online content could be promulgated under section 706.").

91. *See* Thomas G. Krattenmaker & A. Richard Metzger, Jr., *FCC Regulatory Authority Over Commercial Television Networks: The Role of Ancillary Jurisdiction*, 77 NW. U. L. REV. 403, 432–33, 440–45 (1982).

92. 740 F.3d at 635.

93. 467 U.S. 837 (1984).

94. *Id.* at 843.

95. *Id.* at 845.

96. *Id.* at 843 n.9.

normal rules of syntax and linguistics.[97] When applying *Chevron* step one, the Supreme Court has held that "under the established interpretative canons of *noscitur a sociis* and *ejusdem generis*, where general words follow specific words in a statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words."[98] Indeed, it is not even clear that these principles can be properly regarded as canons. The Supreme Court has noted that "[i]t is a familiar principle of statutory construction that words grouped in a list should be given related meaning" and that "[o]ne hardly need rely on such Latin phrases as *ejusdem generis* and *noscitur a sociis* to reach this obvious conclusion." [99] Consequently, courts have routinely included *ejusdem generis* and *noscitur a sociis* in their *Chevron* step one analyses.[100]

The phrase on which the *Verizon* court relied, "other regulating methods that remove barriers to infrastructure investment," is a classic "catchall" clause. *Ejusdem generis* thus requires that its scope be limited to the terms that precede it.[101] All of the items in the list preceding this catchall—"price cap regulation," "regulatory forbearance," and "measures that promote competition in the local telecommunications market"[102]— are deregulatory in focus. This renders problematic the court's interpretation of the catchall to justify imposing more restrictive regulation.[103]

Despite the court's emphasis on "regulatory methods," a brief passage later in the opinion suggests that the court may have relied on the provision of section 706 authorizing the FCC to adopt "measures that promote

---

97. *See* Curtis A. Bradley, Chevron *Deference and Foreign Affairs*, 86 VA. L. REV. 649, 675 (2000); Nina A. Mendelson, Chevron *and Preemption*, 102 MICH. L. REV. 737, 745 (2004); Caleb Nelson, *Statutory Interpretation and Decision Theory*, 74 U. CHI. L. REV. 329, 348–49, 351 (2007) (reviewing ADRIAN VERMEULE, JUDGING UNDER UNCERTAINTY: AN INSTITUTIONAL THEORY OF LEGAL INTERPRETATION (2006)). Descriptive canons, which are textual and syntactical rules governing language and structure, stand in stark contrast to normative canons, which import substantive principles into statutory interpretation and thus are more controversial. Kenneth A. Bamberger, *Normative Canons in the Review of Administrative Policymaking*, 118 YALE L.J. 64, 71–72 (2008); Bradley, *supra*, at 675–76; Nelson, *supra*, at 348–50, 355–60; *see also* VERMUELE, *supra*, at 198–202 (criticizing allowing descriptive canons to trump *Chevron* deference, but acknowledging that normative canons are more problematic).

98. Wash. State Dep't. of Soc. & Health Servs. v. Guardianship Estate of Keffeler, 537 U.S. 371, 384 (2003) (internal quotation marks and alterations omitted).

99. Third Nat'l Bank in Nashville v. Impac Ltd., 432 U.S. 312, 322 & n.16 (1977) (internal quotation marks omitted).

100. *See, e.g.*, *Guardianship Estate of Keffeler*, 537 U.S. at 384 (*noscitur a sociis* and *ejusdem generis*); Dole v. United Steelworkers of Am., 494 U.S. 26, 36 (1990) (*noscitur a sociis*); Cal. Indep. Sys. Operator Corp v. FERC, 372 F.3d 395, 400 (D.C. Cir. 2004) (*noscitur a sociis*).

101. *See, e.g.*, Harrison v. PPG Indus., Inc., 446 U.S. 578, 601 (1980) ("The rule of ejusdem generis ordinarily 'limits general terms which follow specific ones to matters similar to those specified.'" (citing Gooch v. United States, 297 U.S. 124, 128 (1936)).

102. 47 U.S.C. § 1302(a) (2006).

103. Verizon v. FCC, 740 F.3d 623, 636–40 (D.C. Cir. 2014).

competition in the local telecommunications market."[104] This does not change the analysis, however. As the Supreme Court has explained, terms in an enumerated list are construed using "[t]he familiar canon of *noscitur a sociis*, the interpretive rule that words and people are known by their companions."[105] Thus, just as *ejusdem generis* counsels in favor of construing a catchall term in light of the other terms in a list, *noscitur a sociis* leads to the same conclusion with respect to enumerated terms. The same logic would militate in favor of construing this term as being limited to deregulatory measures.

D. The Legislative History of Section 706

The legislative history of section 706 also casts doubt on the *Verizon* court's construction of the statute. According to the conference report accompanying the Telecommunications Act of 1996, section 706 originated in a provision in the Senate bill that had no counterpart in the House version.[106] The Senate provision was part of a title of the bill entitled "An End to Regulation" and was preceded by provisions entitled "Transition to competitive pricing," "Biennial review of regulations; elimination of unnecessary regulations and functions," and "Regulatory forbearance."[107] The overall sweep of these provisions was to lessen regulation, not increase it.

Moreover, during the preceding Congress, the Senate Commerce Committee reported a bill in 1994 containing a provision that appears to be the antecedent to section 706.[108] This provision, the final provision of the bill, stated:

> (a) PROMOTION OF ADVANCED TELECOMMUNICATIONS NETWORK CAPABILITY – The Commission shall promote to all Americans, regardless of location or disability, the deployment of switched, broadband, telecommunications networks capable of enabling users to originate and receive affordable and accessible high quality voice, data, graphics, and video telecommunications services. In promoting the deployment of such networks, the Commission shall, to the maximum extent feasible, rely on competition among telecommunications providers. In the event the Commission determines that users are not gaining reasonable and timely access to switched, broadband, telecommunications network capabilities, the Commission shall have the authority to provide sufficient incentives such that this access is achieved.

104. *Id.* at 642–43.
105. Maracich v. Spears, 133 S. Ct. 2191, 2201 (2013).
106. S. REP. NO. 104-230, at 210 (1996) (Conf. Rep.).
107. Telecommunications Competition and Deregulation Act of 1995, S. 652, 104th Cong. (1995), *reprinted in* 141 CONG. REC. 16346, 27846 (1995).
108. Communications Act of 1994, S. 1822, 103d Cong. (1994).

> (b) RULEMAKING.-If the Commission finds in its inquiry proceedings or any other time that switched, broadband, telecommunications network capabilities are not being deployed to all Americans in a reasonable and timely fashion, it shall commence a rulemaking to prescribe regulations using incentives to promote, to the maximum extent technically feasible and economically reasonable, the availability of switched, broadband, telecommunications network capabilities.[109]

This language clearly identifies "competition among telecommunications providers" as the preferred method for promoting broadband deployment. Indeed, as the Senate Commerce Committee's report that accompanied the bill emphasized:

> The Committee anticipates that this goal will be achieved through competition that is enhanced under the terms of this bill. But if this goal is not being achieved in a timely fashion, the FCC is authorized to act under this section to expedite deployment through the use of incentive regulation.[110]

The legislative history thus evinces a clear emphasis on deregulation and competition among broadband access providers as the preferred way to promote broadband deployment. Moreover, the legislative history contains no hints that Congress regarded promoting innovation in content and applications as an appropriate course of action.

E. The Questionable Empirical Foundation for the Court's Reasoning

The natural reading and the legislative history of the provisions authorizing the FCC to "promote competition in the local telecommunications market" and "remove barriers to infrastructure investment"[111] suggest that these provisions are best construed as authorizing measures deregulating broadband access. The FCC nonetheless concluded that more intrusive regulation was justified because greater innovation in content and applications would create greater demand that would stimulate greater investment infrastructure.[112] The *Verizon* court held that this conclusion was backed by substantial evidence, citing two theoretical

---

109. *Id.*

110. S. REP. NO. 103-367, at 103 (1994). Here, "incentive regulation" refers to price cap regulation. *See* Howard A. Shelanski, *Adjusting Regulation to Competition: Toward A New Model for U.S. Telecommunications Policy*, 24 YALE J. ON REG. 55, 59 (2007).

111. *See* 47 U.S.C. § 1302 (2006).

112. 2010 Open Internet Order, *supra* note 2, at 17910–11 para. 14, 18018 para. 4.

studies, one anecdote, and comments filed with the agency by two interested parties.[113]

A close examination of the FCC's 2010 order, however, reveals that its empirical record was quite thin. For example, the FCC based its conclusion in part on an empirical study that it claimed showed that consumers would be harmed if broadband access providers discriminated against particular edge providers on a single empirical study.[114] Problematically, this study focused on the cable television industry, not on broadband providers—and even then, the study found no clear evidence of discrimination.[115] Indeed, the peer reviewer for the FCC questioned whether the instrument on which this study relied could isolate the effect of the lack of openness.[116]

Both the FCC and the *Verizon* court cited a well-known article on general purpose technologies ("GPTs") by Timothy Bresnahan and Manuel Trajtenberg for the proposition that openness promotes infrastructure investment.[117] But this paper actually concludes that GPTs create positive externalities and that the best way to mitigate the market failure created by these externalities would be to permit providers of GPTs to internalize those externalities through vertical integration or by entering into strategic alliances rather than forced openness.[118] Ironically, the FCC cited this paper as support for a proposition contrary to the conclusion the authors actually reached.

Arrayed against this claim is a growing corpus of empirical studies finding little evidence that access requirements promote investment and competition in broadband access networks.[119] The broader empirical literature on vertical restraints reveals that exclusivity or preferential contracts between suppliers and retail distributors are either neutral or welfare enhancing in the vast majority of cases.[120] That said, the fact that the

---

113. 740 F.3d at 644–45.

114. 2010 *Open Internet Order*, *supra* note 2, at 17918 para. 23 n.60 (citing Austan Goolsbee, *Vertical Integration and the Market for Broadcast and Cable Television Programming*, Paper for the Federal Communications Commission 31–32 (Sept. 5, 2007)).

115. *Id.*

116. David Waterman, Peer Review of *Vertical Integration and the Market for Broadcast and Cable Television Programming*, by Austan Goolsbee (2007), http://transition.fcc.gov/mb/peer_review/prstudy9.pdf.

117. *Id.* at 17909 n.12; *Verizon*, 740 F.3d at 644.

118. Timothy F. Bresnahan & M. Trajtenberg, *General Purpose Technologies: "Engines of Growth"?*, 65 J. ECONOMETRICS 83, 95 (1995).

119. CHRISTOPHER S. YOO, UNIV. OF PA. CTR. FOR TECH., INNOVATION, & COMPETITION, U.S. VS. EUROPEAN BROADBAND DEPLOYMENT: WHAT DO THE DATA SAY? 9 (2014), *available at* https://www.law.upenn.edu/live/files/3352-us-vs-european-broadband-deployment (surveying the literature and finding the overwhelming majority of studies found that access requirements failed to promote investment in next generation networks).

120. James C. Cooper et al., *Vertical Antitrust Policy as a Problem of Inference*, 23 INT'L J. INDUS. ORG. 639, 648–58 (2005); Francine Lafontaine & Margaret Slade, *Exclusive Contracts and Vertical Restraints: Empirical Evidence and Public Policy*, *in* HANDBOOK OF ANTITRUST ECONOMICS 391, 408–09 (Paolo Buccirossi ed., 2008).

D.C. Circuit has already upheld the conclusion that regulations mandating that broadband access providers give nondiscriminatory carriage to edge providers promotes infrastructure investment[121] means that the FCC is likely to adopt the same reasoning in the current NPRM and that the Court of Appeals reviewing the most recent Open Internet Order is likely to uphold this conclusion. If the conclusion is erroneous, any correction will have to come from the Supreme Court.

III. LIMITS ON THE FCC'S SECTION 706 AUTHORITY

To say that section 706 grants the FCC affirmative authority to regulate broadband access is not to say that that authority is unbounded. The general subject matter limitations restrict the scope of the FCC's authority, as does the *Verizon* court's holding that section 706 cannot be used to impose common carriage. In addition, the jurisprudence on ancillary jurisdiction identifies other statutory provisions that limit the FCC's exercise of authority.

A. Statutory Limits on the FCC's Jurisdiction

The FCC and the *Verizon* court both recognized that the FCC's jurisdiction is limited to "interstate and foreign communication by wire and radio" and the fact that any measures enacted under section 706 must be designed to "encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans."[122]

As noted in Part I.B, limiting an agency to interstate matters has long ceased to be a meaningful restriction on governmental power. Moreover, expanding section 706 authority to include all activities that have a tangential impact on infrastructure investment makes just about any measure affecting content and applications part of promoting broadband deployment.

There is one aspect of prior court decisions on ancillary jurisdiction that may provide a limit on the FCC's authority to regulate. In these decisions, once courts concluded that that the authority asserted by the agency was reasonably ancillary to some authority enumerated in Titles II, III, or VI, they proceeded to evaluate whether the particular exercise of ancillary jurisdiction ran afoul of any other statutory provisions. In so doing, these courts undertook an inquiry that was precisely parallel to the one followed by *Verizon v. FCC* with respect to section 706.

In this respect, two cases on ancillary jurisdiction are particularly instructive. In *Illinois Citizens Committee for Broadcasting v. FCC*, the U.S. Court of Appeals for the Seventh Circuit rejected the argument that the FCC had jurisdiction over all matters "affecting communications," concluding instead that the agency's authority was limited to the actual transmission of

121. *Verizon*, 740 F.3d at 643–49.
122. *Id.* at 640; 2010 *Open Internet Order*, *supra* note 258, at 17970 para. 121.

radio or television signals.[123] In other words, the FCC does not have regulatory authority over activities simply because they have a tangential impact on the transmission communications by wire or radio. In this sense, the FCC's authority is considerably narrower than Congress' commerce power, which has long been recognized to extend to activities that "affect" interstate commerce even when they are not themselves part of interstate commerce.[124]

Similarly, in *Motion Picture Association of America v. FCC*, the D.C. Circuit rejected arguments that the FCC possessed the authority to require that broadcasters include aural descriptions of a television program's key visual elements during pauses in the program dialogue.[125] The provision of the Communications Act giving the FCC jurisdiction over "all interstate and foreign communication by wire or radio" authorized the agency to impose regulations on transmissions that "incidentally and minimally affect[] program content."[126] It did not, however, give the agency authority to impose "a direct and significant regulation of program content" by requiring broadcasters to write scripts, select actors, decide what to describe and how, and choose the appropriate style and pace, all within "pauses that were not originally intended to be filled."[127] In short, the FCC's statutory authority over wire and radio communications does not give it the authority to regulate content directly.

The D.C. Circuit provided a more detailed discussion of this principle in *American Library Ass'n v. FCC*, in which the court ruled that the FCC lacked the authority to mandate that receivers recognize a code embedded in digital television programs that prevents their redistribution.[128] The statute gives the FCC authority over devices engaged in interstate "communication" by radio or wire; it does not give the agency authority over devices when they are not engaged in radio or wire transmission, including television receivers after the digital broadcast has been completed.[129]

Together, the courts' precedents establish a number of important limits on the FCC's ancillary authority. Although the FCC can impose regulations that have incidental and minimal effects on content, it lacks the authority to regulate content directly.[130] In addition, the FCC has the authority to regulate communications only when they are being transmitted by wire or radio; it lacks any authority to regulate those communications after they have arrived and presumably before they have been sent.[131]

---

123. 467 F.2d 1397, 1400 (7th Cir. 1972).
124. Wickard v. Filburn, 317 U.S. 111, 124 (1942); United States v. Wrightwood Dairy, 315 U.S. 110, 119 (1942); United States v. Darby, 312 U.S. 100, 118 (1941).
125. 309 F.3d 796, 803–07 (D.C. Cir. 2002).
126. *Id.* at 803.
127. *Id.*
128. 406 F.3d 689, 707 (D.C. Cir. 2005).
129. *Id.* at 700.
130. *Motion Picture Ass'n of Am.*, 309 F.3d at 803.
131. *Am. Library Ass'n*, 406 F.3d at 700.

That said, the power to regulate communications while they are being transmitted does give the FCC considerable power over the economic relationships between content providers and network providers. For example, in *National Broadcasting Co. v. United States*, the Supreme Court held that even though the FCC lacked the authority to regulate content directly, the FCC could restrict the terms of the contracts between broadcast stations and content providers in ways designed to reallocate the relative bargaining power between these entities.[132] Thus, the FCC may be able to follow a similar path with respect to the Internet.

B. Common Carriage as a Limit to Section 706 Authority

The statutory limitation that the *Verizon* court spent the most time analyzing was the prohibition of the imposition of common carriage obligations on information services—including broadband access providers.[133] The statute provides that "[a] telecommunications carrier shall be treated as a common carrier under this [Act] only to the extent that it is engaged in providing telecommunications services."[134] On six separate occasions since 1998, the FCC has reiterated that broadband access is an "information service," a category that is mutually exclusive with "telecommunications service."[135] Unless the agency revisits this conclusion, this provision prevents the FCC from using section 706 to impose common carriage obligations on broadband access providers.[136] In other words, the FCC cannot use section 706 to impose backdoor common carriage regulation on providers that are not subject to Title II.[137]

This prohibition of common carriage represents the most significant obstacle to using section 706 to impose a blanket nondiscrimination

132. 319 U.S. 190, 224 (1943); *see also* Mt. Mansfield Television, Inc. v. FCC, 442 F.2d 470 (2d Cir. 1971) (following similar reasoning to regulate the source of prime time programming and the financial terms of network programming).

133. *See* Verizon v. FCC, 740 F.3d 623, 649–60 (D.C. Cir. 2014).

134. 47 U.S.C. § 153(51) (2006).

135. Federal-State Joint Board on Universal Service, *Report to Congress*, 13 FCC Rcd. 11501, 11520–23 paras. 39–43, 11536–40 paras. 73–81 (1998); *see also* Appropriate Regulatory Treatment for Broadband Access to the Internet over Wireless Networks, *Declaratory Ruling*, 22 FCC Rcd. 5901, 5909–11 paras. 19–27 (2007); United Power Line Council's Petition for Declaratory Ruling Regarding the Classification of Broadband over Power Line Internet Access Service as an Information Service, *Memorandum Opinion and Order*, 21 FCC Rcd. 13281, 13285–86 paras. 8–10 (2006); Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, *Report and Order and Notice of Proposed Rulemaking*, 20 FCC Rcd. 14853, 14862–63 paras. 12–14, 14909–12 paras. 102–107 (2005); *Cable Modem Declaratory Ruling*, *supra* note 38, at 4820 para. 34, 4822–23 paras. 38–39, *aff'd sub nom.* Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 996–1000 (2005); Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, *Notice of Proposed Rulemaking*, 17 FCC Rcd. 3019, 3029–33 paras. 17–25 (2002).

136. *See Verizon*, 740 F.3d at 650–52.

137. *See id.*

requirement. The court's decision in *Verizon* offers guidance as to what constitutes common carriage. As an initial matter, the court held that "requiring broadband providers to serve all edge providers without 'unreasonable discrimination'" is the same thing as the common carriage requirement "compel[ling] those providers to hold themselves out 'to serve the public indiscriminately.'"[138] Furthermore, as the *Verizon* court noted, the FCC explicitly equated common carriage and the nondiscrimination rule imposed by the 2010 order when it told commenters to look to its common carriage precedents for guidance as to what forms of discrimination were reasonable.[139] Moreover, the 2010 Open Internet Order's prohibition of unreasonable discrimination accommodated none of the flexibility and individualized bargaining needed to take the regulation outside of common carriage. Instead of signaling flexibility, the Order warned that "it is unlikely that pay for priority would satisfy the 'no unreasonable discrimination' standard."[140] Preventing "broadband providers from charging edge providers for using their service" in effect would have "forc[ed] them to sell service to all who ask at a price of $0."[141] The prohibition of unreasonable discrimination would thus have admitted none of the individualized bargaining that the court had previously found necessary to take a restriction outside the realm of common carriage.[142]

In fact, even common carriers typically enjoy the ability to offer different classes of service and to charge different amounts for them. In one extreme case, AT&T created a separate class of service for a single customer; the FCC's attempt to prevent AT&T from doing so was overturned in the courts.[143] Ironically, in declaring prioritized service to be presumptively invalid, the nondiscrimination rule in the Open Internet Order would have forbidden a practice that common carriage would have explicitly permitted.[144]

At the same time, the *Verizon* court distinguished the Order's nondiscrimination rule from the data roaming rule that the D.C. Circuit upheld in *Cellco Partnership v. FCC*.[145] As the *Verizon* court noted, the rule at issue in *Cellco* required only that mobile telephone companies enter into data roaming agreements on "commercially reasonable" terms, with reasonableness determined by the "totality of the circumstances" governed

---

138. *See id.* at 655–56.
139. *Id.* at 657 (citing *2010 Open Internet Order*, *supra* note 2, at 17948–40 para. 77 & n.240).
140. *Id.*
141. *Id.*
142. *Id.*
143. AT&T Communications, Revisions to Tariff FCC No. 12, *Memorandum Opinion and Order*, 4 FCC Rcd. 4932, 4938 para. 57 (1989), *rev'd and remanded sub nom.* MCI Telecomms. Corp. v. FCC, 917 F.2d 30, 37 (D.C. Cir. 1990).
144. *See* Daniel A. Lyons, *Net Neutrality and Nondiscrimination Norms in Telecommunications*, 54 ARIZ. L. REV. 1029, 1058 (2012).
145. 700 F.3d 534 (D.C. Cir. 2012).

by sixteen nonexclusive factors.[146] These rules left "substantial room for individualized bargaining and discrimination in terms" and "expressly permit[ted] providers to adapt roaming agreements to 'individualized circumstances without having to hold themselves out to serve all comers indiscriminately on the same or standardized terms.'"[147] Moreover, the order at issue in *Cellco* contained language expressly indicating that its standard differed from the nondiscrimination standard applied to common carriers.[148] The *Cellco* court warned that if the FCC were to apply the "commercially reasonable" standard in a way that was tantamount to common carriage, it would likely be invalidated in as-applied challenges.[149]

It is hard to see how the FCC could implement a blanket nondiscrimination rule and still provide the "substantial room for individualized bargaining and discrimination in terms" and the ability to "adapt roaming agreements to 'individualized circumstances without having to hold themselves out to serve all comers indiscriminately on the same or standardized terms'" required to be a proper exercise of section 706 authority that does not constitute common carriage.[150] Both *Cellco* and the tradition of common carriage afford providers the latitude to create individualized bargains and different classes of service. But permitting different classes of service with different prices is precisely what the nondiscrimination rule was designed to foreclose.[151]

C. Commercial Reasonableness as an Alternative Standard

That said, a nondiscrimination rule is not the only way for the FCC to address concerns that broadband access providers might restrict access to their networks in ways that would inhibit future broadband deployment. The D.C. Circuit's *Cellco* decision, holding that the FCC's data roaming rules did not constitute common carriage, and the court's careful distinction of *Cellco* in *Verizon v. FCC* offered a clear blueprint for fashioning such a rule based on commercial reasonableness. Indeed, the law employs the commercial reasonableness standard in a wide range of contractual agreements.[152]

---

146. *Verizon*, 740 F.3d at 652, 657.
147. *Id.* at 652 (alteration in original).
148. *Id.* at 656.
149. *Id.* at 652; *see Cellco*, 700 F.3d at 548–59.
150. *Cellco*, 700 F.3d at 548 (citing Reexamination of Roaming Obligations of Commercial Mobile Radio Service Providers and Other Providers of Mobile Data Services, *Second Report and Order*, 26 FCC Rcd. 5411, 5433 para. 45 (2011)).
151. *See 2010 Open Internet Order*, *supra* note 2, at 17947 para. 76.
152. *See, e.g.*, Heller v. TriEnergy, Inc., 877 F. Supp. 2d 414, 430 (N.D.W. Va. 2012) (applying a commercial reasonableness standard to the concept of unconscionability); David B. Pursell, *Commercial Reasonableness: The New Target*, J. HEALTH CARE COMPLIANCE, Mar.-Apr. 2011, at 69 (applying a commercial reasonableness standard within the context of health care contracts).

The FCC's new rules proposed in its 2014 Open Internet NPRM appear to accept that invitation by embracing commercial reasonableness as the basis for a rule and proposing a totality-of-the-circumstances test guided by six nonexclusive factors plus a catchall:[153]

- Impact on present and future competition;
- Impact on consumers;
- Impact on speech and civic engagement;
- Technical characteristics;
- "Good faith" negotiation;
- Industry practices; and
- Other factors.[154]

If properly applied, such a rule could address the FCC's desire to promote innovation, competition, free expression, and investment in infrastructure without imposing the type of mandatory obligations associated with common carriage.[155]

1. Impact on Competition

Consider, for example, the factor focusing on the impact on competition. As noted earlier, the literature on GPTs recognizes that strategic alliances between content and network providers can enhance competition.[156] This is consistent with one of the major findings of the modern academic literature on competition policy: that vertical integration and exclusivity contracts are often procompetitive in a broad range of circumstances[157] and that these practices can harm competition only when practiced by a firm with significant market share.[158]

This factor would permit firms to engage in individualized bargaining and prioritized service when the relevant firms are too small to plausibly harm competition or when strategic alliances are likely to promote competition. A prime example of when such practices are unlikely to harm competition is the MetroPCS case discussed at greater length below.[159] Simply put, at 3% market share, any practice adopted by MetroPCS was unlikely to harm competition, and any practice that enhanced its ability to compete with the market leaders despite its severe disadvantage in spectrum holdings could only enhance competition. Permitting similarly situated firms

153. *See 2014 Open Internet NPRM*, *supra* note 7, at 5600–08 paras. 113–135.
154. *Id.* at 5605–10 paras. 124–141.
155. *Cf.* Yoo, *supra* note 53, at 570–72 (identifying affirmative obligations imposed on common carriers by Title II of the Communications Act).
156. *See* Bresnahan & Trajtenberg, *supra* note 118, at 95.
157. Christopher S. Yoo, *Vertical Integration and Media Regulation in the New Economy*, 19 YALE J. ON REG. 171, 192–200, 260–64 (2002).
158. *Id.* at 188–92, 253–59.
159. *See infra* Part V.C.1.

not to carry the content of certain providers under these circumstances helps take this rule outside the realm of obligatory carriage associated with common carriage.

2. Impact on Consumers

Focusing on consumer welfare provides another way that the FCC's proposed rule may fall short of mandating carriage of all content on equal terms. For example, some consumers place a greater emphasis on cost than flexibility. Indeed, this cost sensitivity explains the continued popularity of feature phones, which support only a handful of highly popular functions through a proprietary operating system that supports only a narrow range of third-party applications.[160]

Moreover, as I noted nearly a decade ago, the fact that different customers use the network differently provides an opportunity to enhance consumer welfare through network diversity.[161] Most customers disproportionately frequent only a handful of locations.[162] Consequently, they may prefer a network that gives them prioritized access to the locations that they use the most frequently and on which they place the highest value, such as email servers, remote desktop access to their office computers, or their cloud service providers.[163]

Indeed, recent developments in the United Kingdom illustrate this dynamic nicely. Plusnet employs application-specific traffic management that prioritizes VoIP and gaming.[164] O2 prioritizes a different cluster of services, including streaming and gaming.[165] Sky offers an unmanaged network as a selling point.[166] Rather than offering me-too services, these ISPs offer differentiated services designed to deliver a high-value product to customers with strong preferences for particular applications. Indeed, the proof of the pudding is in the eating: the ISP that manages its network most heavily, Plusnet, enjoys the highest customer satisfaction ratings in the UK.[167]

---

160. Christopher S. Yoo, *Network Neutrality and the Need for a Technological Turn in Internet Scholarship*, *in* ROUTLEDGE HANDBOOK OF MEDIA LAW 539, 552 (Monroe E. Price, Stefaan G. Verhulst & Libby Morgan eds., 2012).

161. Christopher S. Yoo, *Beyond Network Neutrality*, 19 HARV. J.L & TECH. 1 (2005).

162. Christopher S. Yoo, *When Antitrust Met Facebook*, 19 GEO. MASON L. REV. 1147, 1151–52 (2012).

163. Christopher S. Yoo, *Possible Paradigm Shifts in Broadband Policy*, 9 I/S: J.L. & POL'Y FOR INFO. SOC'Y 367, 371 (2014).

164. Alissa Cooper, *How Competition Drives Discrimination: An Analysis of Broadband Traffic Management in the UK* 10 (Aug. 2013) (paper presented at the 41st Research Conference on Communications, Information and Internet Policy (TPRC)), *available at* http://ssrn.com/abstract=2241562.

165. *Id.* at 22.

166. *Id.* at 25–26.

167. Plusnet, Which? Recommended Broadband Provider Plus Award-Winning Customer Service, http://www.plus.net/home-broadband/awards/ (last visited September 20, 2014).

Focusing on consumer welfare thus provides another way that the commercial reasonableness standard can deviate from the nondiscrimination mandate associated with common carriage. These examples underscore how differentiation of traffic can provide consumer benefits by giving the increasingly heterogeneous universe of consumers a broader array of options from which to choose.

3. Industry Practices

Another way in which the commercial reasonableness standard can deviate from common carriage and still take horizontal fairness considerations into account is by examining industry practices. This factor requires an examination of similar transactions with other industry participants, while affording a degree of latitude for variations based on individualized considerations.

An examination of industry practices reveals that many basic services, including VoIP, IP video, and voice over LTE, depend on prioritization or reserved bandwidth to provide the quality of service that consumers demand. The prevalence of these industry practices should be taken into account when assessing the commercial reasonableness of similar arrangements and when implementing the proposed exception for specialized services. Any concerns about whether the growth of specialized services might starve the best-efforts Internet of bandwidth are best addressed through the minimum quality standards established by the anti-blocking rule.

IV. TITLE II RECLASSIFICATION

Many network neutrality proponents regard the *Verizon* court's prohibition on using section 706 to impose common carriage obligations as an insuperable barrier to the type of nondiscrimination mandate that they regard as the most critical.[168] These advocates believe that the only way to achieve a blanket nondiscrimination mandate would be to reclassify broadband access services under Title II, thereby enabling the FCC to impose common carriage regulation.[169] However, the FCC has repeatedly ruled that broadband access services are information services that are exempt from common carriage regulation, rather than telecommunications services that are subject to common carriage regulations.[170] The Supreme Court upheld

168. *See, e.g.*, Press Release, Public Knowledge, FCC to Allow Commercial Discrimination on the Internet (Apr. 23, 2014) ("The very essence of a 'commercial reasonableness' standard is discrimination. And the core of net neutrality is non discrimination"), *available at* http://www.publicknowledge.org/news-blog/press-release/public-knowledge-statement-on-updated-net-neutrality-rules.

169. *See, e.g.*, Lance Ulanoff, *Is Making Broadband a Utility the Key to Saving the Internet?*, MASHABLE (May 15, 2014), http://mashable.com/2014/05/15/fcc-broadband-utility-net-neutrality/.

170. *See supra* note 135 and accompanying text.

this determination as a reasonable interpretation of the Communications Act in *Brand X*.[171] The FCC floated the possibility of reclassifying broadband access as a Title II service while considering the Open Internet Order, relying exclusively on Justice Scalia's dissent in *Brand X*.[172] The agency ultimately declined to pursue reclassification, but made it a point to leave the Title II option open.[173]

A. Legal Barriers to Reclassification

I have addressed at length the problems with Title II reclassification elsewhere and will only sketch my objections here. The FCC's construction of the statute is subject to *Chevron* deference. As *Brand X* made clear, *Chevron* does not preclude the FCC from changing its mind so long as it justifies its change in position.[174] The fact that the FCC has ruled on six separate occasions that broadband access is an information service and not a telecommunications service does not prevent it from revisiting that decision.

To say that the agency may reevaluate its construction, however, does not relieve it from satisfying *Chevron*'s standard of review. *Chevron* Step one requires that the statute's text not foreclose the proffered construction of the statute.[175] If Congress has directly addressed the issue, congressional intent controls.[176] The language of the statute forecloses classifying broadband access as a telecommunications service. The statute defines a "telecommunications service" as a provider that offers for a fee directly to the public "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."[177] The FCC has characterized this as "pure" transmission that does not involve computer processing or storage.[178]

The problem is that much of the world's web content is served by content delivery networks ("CDNs"), which store popular web content in thousands of locations around the world. For example, market leader Akamai

171. Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 968–69 (2005).

172. JULIUS GENACHOWSKI, THE THIRD WAY: A NARROWLY TAILORED BROADBAND FRAMEWORK 4 (2010), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-297944A1.pdf; AUSTIN SCHLICK, A THIRD-WAY LEGAL FRAMEWORK FOR ADDRESSING THE *COMCAST* DILEMMA 3 (2010), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-297945A1.pdf; *see also* Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 1005 (2005) (Scalia, J., dissenting).

173. *See* Framework for Broadband Internet Service, *Notice of Inquiry*, 25 FCC Rcd. 7866, 7867 para. 2, 7919 (2010) (statement of Michael Copps, Comm'r).

174. *Brand X*, 545 U.S. at 981.

175. *Id.* at 982.

176. *Id.*

177. 47 U.S.C. § 153(46) (2006).

178. *Verizon*, 740 F.3d at 630.

uses nearly 150,000 servers throughout the network to serve 30% of the world's web content and rely on the domain name system ("DNS") to determine from which cache it should serve any particular request.[179] The Supreme Court has upheld the conclusion that the DNS and caching functions associated with the typical broadband access service inevitably involve both computer processing and storage and thus take broadband access outside the scope of Title II.[180]

The statutory requirement that the transmission take place between points specified by the end user is even more problematic. On the Internet, physical locations are addressed by the numbers of an Internet Protocol (IP) address, which in the case of IP version 4 is usually represented by four numbers between 0 and 255 separated by dots (such as 128.91.34.233, which is one of the IP addresses assigned to the University of Pennsylvania).[181] Although the National Science Foundation is currently studying a proposal to restructure Internet addresses so that they refer to particular content rather than particular locations,[182] until such a proposal is adopted, the address architecture will continue to focus on physical addresses. End users and applications typically do not rely on IP addresses, however. Instead, they generally use domain names (such as upenn.edu) to access Internet resources, relying on the DNS to map domain names onto IP addresses.[183] When this is the case, the points of communication are specified by DNS, not the end user.[184] Moreover, as anyone who has attempted to access Google's website from another country recognizes, the mapping of domain names onto IP addresses is not simply mechanical.[185] On the contrary, the DNS often routes the same domain name to different locations based on its inference of which location is most likely to be the one the end user wants. In addition, content is frequently not stored in a single location.[186] CDNs, for instance, depend on the DNS to determine from which of their thousands of caches that any particular request should be served.[187] Thus, unless the user employs IP addresses instead of domain names or maintains his or her own DNS, it is a third-party DNS provider that selects the points of transmission, not the end user. As a result, it is impossible to see how broadband access can fit within the statutory definition of telecommunications service governed by Title II.

---

179. Press Release, NanoTech Entertainment, NanoTech's Nuvola NP-1 4K Streaming Media Player Demonstrated with Akamai Media & Delivery Solutions at NAB 2014 (Mar. 19, 2014), *available at* http://finance.yahoo.com/news/nanotech-nuvola-np-1-4k-204400686.html.

180. *Brand X*, 545 U.S. at 998–1000.

181. Yoo, *supra* note 53, at 565.

182. NAMED DATA NETWORKING, http://named-data.net/ (last visited May 23, 2014).

183. Yoo, *supra* note 53, at 565.

184. *Id.* at 564.

185. *Id.* at 567.

186. *Id.* at 566.

187. *Id.* at 567.

B. Overlooked Implications of Reclassification

Interestingly, many network neutrality proponents seem to be unfamiliar with the way that Title II regulation works in practice. Specifically, it has generally not been applied to benefit actors occupying the position of content and service providers, it has never barred prioritized service, and it has long been plagued by a series of implementation difficulties.

1. Common Carriage's Inapplicability to Complementary Services

Supporters of Title II reclassification believe it will enable rules that give edge providers nondiscriminatory access to broadband networks. The history of common carriage is to the contrary. The seminal decision is *Memphis & Little Rock Railroad Co. v Southern Express Co.* (*The Express Package Cases*), in which the Supreme Court held that the nondiscrimination obligations of common carriers applied only to end users and did not apply to express package companies who wanted to use the railroad as a conduit for delivering another service.[188] This is because the specialized needs of such services "must necessarily be a matter of bargain," the Court reasoned, and thus cannot always be provided to all express package companies.[189] The fact that express package services had become a "public necessity," was "used in almost every conceivable way, and for almost every conceivable purpose," and that "[a]ll have become accustomed to it, and it cannot be taken away without breaking up many of the long-settled habits of business, and interfering materially with the conveniences of social life" did not change the Court's analysis.[190] The courts have applied similar principles to the telecommunications industry.[191]

The *Verizon* court elided this distinction somewhat when it rejected the FCC's argument that the nondiscrimination rule's requirement that broadband access providers carry edge providers did not impose common carriage obligations because broadband access providers only served as carriers for end users, not for edge providers.[192] The issue presents the converse of the question presented in the *Express Package Cases*. In those cases, the question was whether common carriage entailed nondiscrimination towards edge providers.[193] In *Verizon*, the issue was whether nondiscrimination towards edge providers entailed common carriage.

---

188. 117 U.S. 1, 27 (1885).
189. *Id.* at 24.
190. *Id.* at 20.
191. PETER W. HUBER ET AL., FEDERAL TELECOMMUNICATIONS LAW § 1.3.1, at 14–16, § 5.1.1, at 407–08 (2d ed. 1999).
192. *Verizon*, 740 F.3d at 653.
193. 117 U.S. at 20.

In any event, the history of common carriage raises questions whether common carriage would give edge providers the benefit of a nondiscrimination mandate. If not, Title II reclassification would not create the benefits that many network neutrality proponents envisage.

2. The Permissibility of Prioritized Service

As noted above, common carriage does not restrict from creating different classes of service so long as it provides each class of service to all comers.[194] Thus, notwithstanding the claims of some network neutrality proponents, Title II reclassification would not necessarily prevent broadband access providers from offering premium services at premium prices.[195]

3. Difficulties Implementing Common Carriage

Finally, advocates of Title II reclassification must come to grips with how difficult nondiscrimination mandates have historically been to implement in practice. Any decision-maker confronted with a nondiscrimination claim would have to determine whether the price differentials were the result of differences in quality or cost or the desire to implement schemes such a Ramsey pricing that can make the allocation of high fixed costs goods more efficient.[196]

Title II would also require decision-makers to ensure that rates are just and reasonable.[197] The methodologies for evaluating the reasonableness of rates have long been criticized for providing insufficient incentives to economize on costs, discouraging innovation, and leading to interminable controversies over how to determine the proper rate base and rate of return, how to allocate common costs, and over the reasonableness of non-price terms and conditions.[198] Rate regulation also facilitates collusion by creating entry barriers, standardizing products and pricing, pooling information, providing advance notice of changes, and allowing the government to serve as the means for forcing parties to adhere to the agreed upon prices.[199] Moreover, with respect to traditional telephony, the increasingly specialized needs of business customers led them to request an ever-growing number of special access tariffs and waivers designed to tailor services to individual customers' particular needs. In light of the growing diversity of Internet applications, imposition of Title II regulation would likely deluge regulators with a similar range of requests.

---

194. *See supra* notes 194–207 and accompanying text.
195. Yoo, *supra* note 53, at 574 n.183.
196. *Id.* at 573–81.
197. 47 U.S.C. § 201(b) (2006).
198. Yoo, *supra* note 53, at 581–95.
199. *Id.* at 602–05.

4. Difficulties Implementing Forbearance

Finally, any solution based on Title II reclassification would require the FCC to forbear from a number of statutory provisions, as both the Commission[200] and several advocates of reclassification have noted.[201] Section 10 of the Communications Act requires the FCC to forbear from "applying any regulation or any provision of [Title II] to a telecommunications carrier" if the agency finds that a regulation is not needed to protect consumers or ensure just and reasonable practices and that forbearing from such regulation is "consistent with the public interest."[202] In practice, however, the agency's experience with forbearance has not been a happy one. Scholars have criticized the agency for failing to establish clear evidentiary standards,[203] for establishing a market power test based on marginal cost pricing that is impossible for any telecommunications network to satisfy,[204] and for ignoring intermodal competition.[205] Indeed, the courts have found the FCC's forbearance decisions to be so internally inconsistent as to be arbitrary and capricious.[206]

The net result of these considerations is that Title II reclassification may not prohibit the types of practices that concern network neutrality proponents the most. In addition, the looming implementation difficulties suggest that even if common carriage regulation were somehow directed towards those exact practices, it may not create the benefits that they envisage. And the prospect of relying on forbearance to ensure that regulation remains light may be illusory.

V. OTHER IMPLICATIONS OF THE *VERIZON* DECISION

Both Verizon and the FCC declined to appeal the *Verizon* court's decision to the Supreme Court, and the FCC has already published a new notice of proposed rulemaking that proposes rules that comport with the

---

200. *2014 Open Internet NPRM*, *supra* note 7, at 5615–16 paras. 153–155.

201. *See* Comments of the Open Tech. Inst. at the New Am. Found. and Benton Found. at 26, Protecting and Promoting the Open Internet, FCC GN Docket No. 14-28 (rel. May 15, 2014), *available at* http://newamerica.net/sites/newamerica.net/files/profiles/attachments/OTI_NN_Comments_FINAL.pdf.

202. 47 U.S.C. § 160(a) (2006).

203. Rob Frieden, *Case Studies in Abandoned Empiricism and the Lack of Peer Review at the Federal Communications Commission*, 8 J. ON TELECOMM. & HIGH TECH. L. 277, 292 (2010).

204. George S. Ford & Lawrence J. Spiwak, *The Impossible Dream: Forbearance After the Phoenix Order* (Phx. Ctr. for Advanced Legal & Econ. Pub. Pol'y Studs., Paper No. 10-08, 2010), *available at* http://ssrn.com/abstract=1740558.

205. Seth L. Cooper, *Forbearance Follies: What the FCC's New Framework Portends for the "Third Way"* 3–4 (Free State Found., Perspectives from FSF Scholars Vol. 5 No. 18, 2010), *available at* http://www.freestatefoundation.org/images/Forbearance_Follies_070810.pdf.

206. Verizon Tel. Cos. v. FCC, 570 F.3d 294, 301–05 (2009).

Verizon decision.[207] Nonetheless, the text of the *Verizon* decision and the early debates surrounding the FCC's proposed rules raise some tantalizing possibilities as to what might transpire next.

A. State Regulation

Section 706 applies equally to "[t]he Commission and each State commission with regulatory jurisdiction over telecommunications services."[208] The statute thus seems to accord to state public utility commissions (PUCs) the same regulatory authority that it accords to the FCC. Concerns that inconsistent state regulation would disrupt the deployment of the newly emerging information services led the FCC to preempt state regulation in both its Second and Third Computer Inquiries.[209] History has shown that state and local authorities might well be eager to exercise this authority. Prior to 2002, when the FCC refused to address the regulatory status of broadband access services,[210] state and local governments rushed to the void.[211] The resulting regulation and litigation threatened the broadband industry with a welter of inconsistent and burdensome regulatory mandates. The FCC's 2002 assertion of exclusive federal jurisdiction over broadband largely eliminated these disputes.[212]

The obvious way to avoid the inconsistency of concurrent state-federal regulation is for the FCC to preempt state action, but it is questionable whether preemption is permissible when section 706(a) also gives authority to the state PUCs *in pari materia*.[213] Indeed, the *Verizon* court saw nothing untoward in concurrent federal-state jurisdiction.[214]

Language included in both the Senate and Conference Reports accompanying the 1996 Act may provide sufficient basis to avoid this problem. The Senate report clearly provides that "[t]he FCC may pre-empt State commissions if they fail to act to ensure reasonable and timely

---

207. *See* Open Internet Remand, *Public Notice*, FCC GN Docket No. 14-28 (rel. Feb. 19, 2014); *see also* 2014 Open Internet NPRM, *supra* note 7.

208. 47 U.S.C. § 1302(a) (2006).

209. Amendment of Section 64.702 of the Commission's Rules & Regulations (Third Computer Inquiry), *Report and Order*, 104 F.C.C.2d 958, 1127–28 paras. 347–348 (1986), *vacated sub nom.* California v. FCC, 905 F.2d 1217 (9th Cir. 1990); Amendment of Section 64.702 of the Commission's Rules & Regulations (Second Computer Inquiry), *Memorandum Opinion and Order*, 84 F.C.C.2d 50, 103 para. 154 (1980), *aff'd sub nom.* Computer & Commc'ns Indus. Ass'n v. FCC, 693 F.2d 198, 214–18 (D.C. Cir. 1982).

210. *See* Nat'l Cable & Telecomms. Ass'n v. Gulf Power Co., 534 U.S. 327, 349–51 (2002) (Thomas, J., concurring in part and dissenting in part) (rebuking the FCC for failing to address the regulatory status of broadband).

211. *See, e.g.*, MediaOne Group, Inc. v. County of Henrico, 257 F.3d 356 (4th Cir. 2001); AT&T Corp. v. City of Portland, 216 F.3d 871 (9th Cir. 2000).

212. *See Cable Modem Declaratory Ruling*, *supra* note 38, at 4800–02 paras. 2–7.

213. *See* 2B SUTHERLAND ON STATUTORY CONSTRUCTION § 51:2 (7th ed. & Supp. 2014) ("Courts try to construe apparently conflicting statutes on the same subject harmoniously, and, if possible, give effect to every provision in both.").

214. Verizon v. FCC, 740 F.3d 623, 638 (D.C. Cir. 2014).

access."[215] The Conference Report includes identical language.[216] The legislative history thus clearly suggests that the federal government should be able to preempt state regulation notwithstanding the language of section 706(a).

B. The Applicability of Network Neutrality to Interconnection Agreements

Both the 2010 Open Internet Order and the 2014 Open Internet Notice of Proposed Rulemaking made clear that the rules were designed to ensure equal treatment of traffic *within* a broadband access provider's network. The rules were not meant to equalize the terms under which traffic *arrives* at a broadband provider's network.

As a result, the FCC has repeatedly clarified that the Open Internet rules do not apply to interconnection agreements between Internet service providers (ISPs).[217] Some voices have begun to call for bringing interconnection agreements within the scope of the network neutrality debate.

Attempting to equilibrate interconnection agreements would turn every bilateral negotiation between two ISPs into a regulatory matter. Indeed, in a network comprised of more than 30,000 networks interconnected through bilateral agreements, variations in price and latency are endemic.

1. The Mischaracterization of Peering as Zero-Price Interconnection

It is often said that the Internet is a network of networks.[218] What this means in practice is that traffic that originates on one network often terminates on another network.[219] To make this possible, ISPs enter into contracts with other Internet service providers ("ISPs") to exchange traffic. Because the terminating ISP also incurs costs,[220] the traditional rule was that the originating ISP would make what is known as a transit payment to

---

215. S. REP. NO. 104-23, at 50 (1995).
216. S. REP. NO. 104-230, at 210 (1996) (Conf. Rep.).
217. *See infra* notes 257-258 and accompanying text.
218. The discussion that follows is adapted from my testimony before the Senate Judiciary Committee on April 9, 2014. *Examining the Comcast-Time Warner Cable Merger and the Impact on Consumers: Hearing Before the S. Comm. on the Judiciary*, 113th Congress (2014), *available at* http://www.judiciary.senate.gov/imo/media/doc/04-09-14YooTestimony.pdf.
219. Michael Kende, *The Digital Handshake: Connecting Internet Backbones*, 11 COMMLAW CONSPECTUS 45, 51 & n.60 (2003) ("In a settlement arrangement . . . the carrier on which the traffic originates pays the other carrier to terminate the traffic.").
220. *Id.* at 47–52.

compensate the terminating ISP for providing services to the originating ISP's customers.[221]

If traffic is roughly symmetrical, ISPs can reduce costs by foregoing monitoring and billing for the exchange of traffic and instead calling it a wash, a practice commonly known as settlement-free peering.[222] Such arrangements make economic sense only if the traffic exchanged is symmetrical in terms of cost and value. If traffic becomes out of ratio, peering contracts typically call for transit-style payments.[223]

The fact that peering agreements include a symmetry requirement underscores that they are more properly regarded as a form of barter that is conditional on an even exchange.[224] Consider what would happen if one of the parties to a peering contract that was roughly in balance suddenly signed up a customer that caused a significant increase in the amount of traffic that it was handing off to the other party for termination. At this point, the traffic would likely be out of ratio, in which case the terminating ISP would have to incur significant costs to terminate the traffic and the peering contract would typically call for the originating ISP to make a payment to the terminating ISP. Insisting that all interconnection occur at a zero price regardless of the amount of traffic is inconsistent with the barter-based justification underlying peering arrangements.

Certainly, the originating ISP would like the terminating ISP to bear all of the costs of doing so. Conversely, the terminating ISP would like the originating ISP to pay for the costs, as required by the typical peering contract. Both parties benefit from delivering greater value to the end users. The usual solution would be for both parties to bear part of the costs based on their relative elasticities of demand.[225] Mandating zero-price interconnection would prevent this from occurring.

2. The Multiple Functions Performed by Prices

Insisting that interconnection always occur at a zero price would also ignore the important role that prices play in any market economy. In terms of Internet interconnection, prices perform three key functions.

First, prices allocate scarce resources and allow markets to clear while helping to ensure that those resources are employed only when the benefits

---

221. CHRISTOPHER S. YOO, THE DYNAMIC INTERNET 64, 94 (2012).

222. Kende, *supra* note 219, at 49.

223. YOO, *supra* note 221, at 64, 95–96.

224. Kende, *supra* note 219, at 52 ("[P]eering agreements are the result of commercial negotiations; each backbone bases its decisions on whether, how and where to peer by weighing the benefits and costs of entering into a particular interconnection agreement with another backbone.").

225. For a detailed discussino of Internet backbone competition in light of end user demand elasticity, see Jean-Jacques Laffont et al., *Internet Interconnection and the Off-Net-Cost Pricing Principle*, 34 RAND J. ECON. 370 (2003).

of doing so exceed the costs.[226] Second, they provide an incentive for interconnection partners to conserve on bandwidth. Third, if supracompetitive prices emerge, they signal to other actors that the market is in short-run disequilibrium and provide the incentive for others to enter the market. Entry by other players shifts the supply curve out until the market is once again in long-run equilibrium.[227]

Imagine what would happen if all interconnection prices were required to equal zero. First, because prices could not rise, markets could not clear, so they would end up in persistent shortage.[228] Second, interconnection partners would have no incentive to rationalize their consumption or to invest in technologies that consume less bandwidth.[229] Third, and worst of all, zero-price interconnection would prevent those who invest in value-creating activities from earning a return and thus risk inhibiting innovation.[230]

Internet companies are investing in their businesses in an attempt to gain an edge on the competition, and any advantage gained only serves to force competitors to make new investments of their own. Consider the impact that the cable industry's deployment of DOCSIS 3.0[231] and the advent of Google Fiber [232] have had on telephone companies. The higher investments by these companies are forcing AT&T to respond in kind. [233] Faced with competitors able to deliver significantly higher bandwidth, AT&T has begun deploying more advanced DSL technologies capable of delivering between 45–100 Mbps service.[234] Where these services have been

---

226. Christopher S. Yoo, *Network Neutrality and the Economics of Congestion*, 94 GEO. L.J. 1847, 1864 (2006).

227. Christopher S. Yoo, *Rethinking the Commitment to Free, Local Television*, 52 EMORY L.J. 1579, 1590–91 (2003).

228. *See, e.g.*, DANIEL F. SPULBER & CHRISTOPHER S. YOO, NETWORKS IN TELECOMMUNICATIONS: ECONOMICS AND LAW 78–83 (2009) (discussing the harmful economic consequences of price controls).

229. *See* Yoo, *supra* note 226, at 1864–65.

230. *See* Yoo, *supra* note 161, at 48–53; Christopher S. Yoo, *Network Neutrality, Consumers, and Innovation*, 2008 U. CHI. LEGAL F. 179, 235–37 [hereinafter Yoo, *Consumers*].

231. *See Eighth Broadband Progress Report*, *supra* note 68, at 10385 para. 92.

232. *See* John Brodkin, *Google Fiber Chooses Nine Metro Areas for Possible Expansion*, ARS TECHNICA (Feb. 19, 2014, 1:00 PM), http://arstechnica.com/business/2014/02/google-fiber-chooses-nine-metro-areas-for-possible-expansion/.

233. *See, e.g.*, Applications and Public Interest Statement of Comcast Corp. and Time Warner Cable Inc. at 42–52, Applications of Comcast Corp. and Time Warner Cable Inc. for Consent to Assign and Transfer Control of Licenses and Other Authorizations, FCC MB Docket No. 14-57 (rel. July 10, 2014), *available at* http://corporate.comcast.com/images/Comcast-Public-Interest-Statement-April-8.pdf (chronicling the virtuous cycle of investment by cable and telco broadband providers in infrastructure upgrades including FTTN and VDSL2 with pair bonding).

234. Press Release, AT&T, AT&T to Invest $14 Billion to Significantly Expand Wireless and Wireline Broadband Networks, Support Future IP Data Growth and New Services (Nov. 7, 2012), *available at* http://www.att.com/gen/press-room?pid=23506&cdvn=news&newsarticleid=35661&mapcode=.

deployed, AT&T is successfully taking customers from the cable companies with which it competes.[235]

This type of dynamic is not limited to horizontal competition. Service providers are providing high-value content and services with strong customer appeal. The desirability of these products in turn strengthens these companies' hand when negotiating interconnection agreements.

Indeed, this is exactly what appears to be occurring with Netflix. Netflix has been a spectacular success, largely because of the billions of dollars in forward contracts in content that it has undertaken.[236] These risks have paid off spectacularly, and Netflix has grown to more than one-third of all primetime Internet traffic in the U.S.[237] Like any for-profit company, Netflix would prefer it if the ISPs bore as much of the burden of the additional costs of carrying this traffic as possible. Indeed, that is the gist of its Open Connect program, which requires ISPs to terminate Netflix traffic for free.[238] The strong bargaining leverage created by Netflix's investments has led many ISPs to embrace Open Connect.[239]

Netflix must be permitted to exercise the bargaining power created by its investments if it is to be expected to continue to invest in the future. Other ISPs have resisted and have made investments of their own in an attempt to gain bargaining leverage.[240] This pattern of move and countermove in an attempt to reap economic benefit is what drives investment and innovation. This is the true virtuous circle of innovation.

All of this is a natural part of healthy bargaining process. As in the typical case, both sides reached an interconnection agreement that divides the costs. Applying network neutrality to such disputes would turn every garden-variety bargain over price that characterizes every arms-length economic transaction into a regulatory matter. To the extent that it deprives firms of returns that are the result of the entrepreneurial risks they have taken, it threatens to cause the virtuous circle to stall. Determining the price that appropriately divides the costs is greatly complicated by the fact that the

---

235. *See* Mark A. Israel, Econ. Analysis of the Effect of the Comcast-TWC Transaction on Broadband: Reply to Commenters at 71 para. 80, Applications of Comcast Corp. and Time Warner Cable Inc. for Consent to Assign and Transfer Control of Licenses and Other Authorizations, FCC MB Docket No. 14-57 (rel. July 10, 2014), *available at* http://corporate.comcast.com/images/2014-09-23-REDACTED-Comcast-TWC-Opposition-and-Response-Exhibit-1-Israel.pdf.

236. *See, e.g.*, Mark Sweney, *Netflix to Spend $3bn on TV and Film Content in 2014*, THE GUARDIAN (Feb. 5, 2014, 11:07 AM), http://www.theguardian.com/media/2014/feb/05/netflix-spend-3-billion-tv-film-content-2014.

237. SANDVINE, GLOBAL INTERNET PHENOMENA 1H2014, at 5–6(2014), *available at* https://www.sandvine.com/downloads/general/global-internet-phenomena/2014/1h-2014-global-internet-phenomena-report.pdf.

238. *See* Jon Brodkin, *Netflix's Many-Pronged Plan to Eliminate Video Playback Problems*, ARS TECHNICA (May 13, 2014, 11:15 AM), http://arstechnica.com/information-technology/2014/05/netflixs-many-pronged-plan-to-eliminate-video-playback-problems/.

239. *Id.*

240. *Id.*

Internet constitutes a two-sided market.[241] The economics of two-sided markets are somewhat complex.[242] Conventional economics has long recognized the existence of "network economic effects," which cause a network to increase in value as the number of users connected to it increases.[243] To use a classic example, the value of a telephone network to consumers is thus determined by more than just the price charged and the services provided, as is the case with most goods. It also depends on the number of other subscribers connected to the network. The more people each user can reach through the network, the more valuable it becomes to all users.

The telephone system is an example of a one-sided market, as the value to any particular caller is determined in no small part by the number of similarly situated callers. When a market is two-sided, instead of bringing together a single class of similarly situated users, networks bring together two completely different classes of users.[244] In those cases, the value is determined not by the number of users of the same class, but rather the number of users of the other class. To put it in terms of a concrete example, consider the economics of broadcast television, which generates revenue from advertisers based on the number of viewers the industry can deliver.[245] The value of the network for advertisers is not determined by the number of other advertisers. Instead, the value of the network increases with the number of a different class of network participants (i.e., television viewers).

The economics of two-sided markets indicate that it may be socially beneficial for content and application providers to subsidize the prices paid by end users.[246] The fact that the Internet has become increasingly dominated by advertising revenue paid to content and application providers rather than network providers makes this particularly likely to be true. An advertiser's willingness to pay for an ad on any particular website depends on the number of end users viewing that website. Under these circumstances, the optimal solution may be for the website owner to subsidize the total number of end users by making payments to the network provider to help defray their costs

---

241. The discussion that follows is adapted from Christopher S. Yoo, *Network Neutrality After* Comcast*: Toward a Case-by-Case Approach to Reasonable Network Management*, *in* NEW DIRECTIONS IN COMMUNICATIONS POLICY 55, 71–76 (Randolph J. May ed., 2009). For a more extended discussion of the implications of the economics of two-sided markets for network neutrality, see Yoo, *Consumers*, *supra* note 230, at 222–27.

242. For overviews of the economics of two-sided markets, see David S. Evans & Richard Schmalensee, *The Industrial Organization of Markets with Two-Sided Platforms*, 3 COMP. POL'Y INT'L 151 (2007), *available at* https://www.law.berkeley.edu/files/Evans_and_Schmalensee_-_Two_Sided_Markets.pdf; Jean-Charles Rochet & Jean Tirole, *Two-Sided Markets: A Progress Report*, 37 RAND J. ECON. 645 (2006); Roberto Roson, *Two-Sided Markets: A Tentative Survey*, 4 REV. NETWORK ECON. 142 (2005), http://www.bepress.com/rne/vol4/iss2/3.

243. *See* Yoo, *supra* note 161, at 33.

244. *See* Yoo, *Consumers*, *supra* note 230, at 223.

245. *Id.* at 237

246. *Id.* at 237–38.

of connection.[247] The costs of subsidizing more users would be more than offset by the additional revenue generated by the fact that advertisers can now reach more potential customers.[248]

These revenue-side pressures are reinforced by cost-side considerations. The cost of connecting content and application providers to the Internet is quite low, typically only requiring a single high-speed line to a small number of business locations.[249] The cost of connecting end users to the Internet is much higher, requiring the wiring and upgrading of equipment in entire neighborhoods. In an industry in which the primary revenue is flowing to content and application providers and the costs involved in connecting content and application providers are much smaller than the costs of connecting end users, one would expect some cash to flow from content and application providers to those who are providing connections to end users.[250]

These dynamics are again well-illustrated by broadcast television. In many ways, broadcast television and the Internet are analogous. The movie studios that create television programs play a similar role to content and application providers. Television networks aggregate programs and deliver them nationally in much the same manner as server-side network providers and backbone providers.[251] Local broadcast stations provide last-mile connectivity that is quite similar to the role played by DSL and cable modem providers. In addition, the revenue structure is quite comparable, in that television networks receive advertising revenue in much the same manner as content and application providers. Furthermore, the cost structure is somewhat similar in that connecting individual homes is much more costly than distributing programming nationally.

For decades, the standard business arrangement has been for television networks to subsidize the operations of local broadcast stations by paying them to be members of their television networks.[252] The industry's revenue and cost structure make such arrangements quite logical. The cost of paying these broadcast stations to affiliate with a network is more than offset by the increase in advertising revenue made possible by the fact that the network is now able to reach a larger audience.[253] Broadcast television thus represents a prime example of when firms operating on one side of the market find it

247. *Id.*
248. *Id.* at 225–26.
249. *Id.* at 237.
250. Peyman Faratin et al., *The Growing Complexity of Internet Interconnection*, COMM. & STRATEGIES, 4th Quarter 2008, at 51, 59.
251. JEFF ULIN, THE BUSINESS OF MEDIA DISTRIBUTION: MONETIZING FILM, TV, AND VIDEO CONTENT 224–25 (1st ed. 2010).
252. Annual Assessment of the Status of Competition in the Market for the Delivery of Video Programming, *Fifteenth Report*, 28 FCC Rcd. 10496, 10599 para. 208 (2013) [hereinafter *Fifteenth Video Competition Report*], *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-13-99A1.pdf.
253. *See* Yoo, *Consumers*, *supra* note 230, at 237.

economically beneficial to subsidize end users on the other side of the market.

Furthermore, the magnitude of the affiliation fees that the networks pay to broadcast stations is anything but uniform. The precise amount paid varies with the relative strength of the network and the relative strength of the broadcast station.[254] Stronger broadcast stations receive more, while weaker ones receive less. Equally interesting is the fact that in recent years, the cash flow has begun to vary in its direction as well as magnitude, with weaker stations having to pay rather than be paid to be part of the television network.[255] The dynamic nature of this pricing regime benefits consumers by providing incentives for networks to invest in better quality programming and by providing an incentive for stations to provide better carriage.

The core insight of two-sided market is that prices can vary widely in magnitude and direction. Sometimes money flows from content providers to network providers, and sometimes it naturally flows the other way. All of this underscores the difficulty of identifying the optimal price as well as the fact that requiring all interconnection occur at a zero price would be an economic anomaly. Prices are how market-based economies allocate goods, provide incentives to minimize costs, and signal producers that the market is in disequilibrium. Freezing those prices would dampen those signals and risk forestalling the quest for bargaining leverage that is the engine that drives the virtuous circle of innovation forward.

3. The Danger of Regulating Interconnection Agreements

Although some have suggested that such interconnection agreements represent network neutrality violations,[256] network neutrality only applies to how traffic is handled *within* an ISP's network. It does not apply to how the traffic arrives at an ISP, which inevitably travels by paths of different lengths and incurs different costs as it traverses a system composed of 47,000 separate networks tied together through arms-length interconnection agreements. Indeed, this is why the Open Internet Order specified that it does

---

254. *Id.*.

255. *Fifteenth Video Competition Report*, *supra* note 252, at 10599–600 paras. 208–209 ("Network compensation to television broadcast stations has all but disappeared, and today, television stations instead commonly pay compensation to networks in order to air their programming." (citations omitted)).

256. *See, e.g.*, Reed Hastings, *Internet Tolls and the Case for Strong Net Neutrality*, NETFLIX US & CANADA BLOG (Mar. 20, 2014, 2:00 PM), http://blog.netflix.com/2014/03/internet-tolls-and-case-for-strong-net.html; Stacey Higginbotham, *Paid Peering Is Not a Net Neutrality Issue But Level 3 Wants to Make It One*, GIGAOM (Mar. 18, 2014, 9:26 AM), https://gigaom.com/2014/03/18/level-3-gets-the-problems-of-peering-fights-so-right-and-then-so-wrong/; Mark Rogovsky, *Comcast-Netflix Didn't Violate Net Neutrality But It Wasn't Benevolent, It Was Business*, FORBES (Feb. 24, 2014, 9:07 AM), http://www.forbes.com/sites/markrogowsky/2014/02/24/comcast-netflix-didnt-violate-net-neutrality-but-it-wasnt-benevolent-it-was-business/

not apply to interconnection agreements,[257] why FCC Chairman Julius Genachowski made clear that the Open Internet Order does not apply to interconnection disputes,[258] and why Chairman Wheeler has indicated the same.[259] The proposed rule that the FCC adopted on May 15, 2014, tentatively reiterated the conclusion that the rules would apply only to a broadband access provider's own network and not to traffic exchanged between networks.[260]

The Comcast-Netflix interconnection agreement appears to be nothing more than a typical case of such bargaining. One advantage is that because it now is a direct customer of Comcast, it gains the benefit of the guaranteed service levels in Comcast's standard service-level agreement. Indeed, media reports indicate that Comcast customers are experiencing a quality enhancement in their Netflix experience.[261]

The agreement reduces Comcast's costs, while the impact on Netflix is ambiguous: while it now must pay Comcast to terminate its traffic, it no longer needs to pay the third-party ISP on which it previously relied to reach Comcast in a classic case of efficiencies through cutting out the middleman. Although some have suggested that this might lead to a net reduction in Netflix's costs, that information is confidential and cannot be verified. In any event, interconnection represents a trivial revenue stream for Comcast and a tiny portion of Netflix's cost structure, which is dominated by program acquisition costs, which means that the transaction is unlikely to have any material effect on Netflix subscription prices.[262]

In addition, interconnection in the Internet space is fundamentally different from carriage agreements in cable television. In cable television, the failure to come to an agreement means that subscribers cannot receive

---

257. *2010 Open Internet Order*, *supra* note 2, at 17933 para. 47 (noting the Open Internet Order's inapplicability to "Internet backbone services"); *id.* at 17944 n.209 (noting the Open Internet Order's inapplicability to interconnection).

258. *Network Neutrality and Internet Regulation: Warranted or More Economic Harm than Good?, Hearing before the Subcomm. on Communications and Technology, H. Comm. on Energy and Commerce*, 102d Cong., 1st Sess. 102 (2011), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg65940/pdf/CHRG-112hhrg65940.pdf.

259. Brendan Sasso, *Netflix's Net-Neutrality Plea Gets Rejected by the FCC*, NAT'L J. (Apr. 1, 2014), http://www.nationaljournal.com/tech/netflix-s-net-neutrality-plea-gets-rejected-by-the-fcc-20140401.

260. *2014 Open Internet NPRM*, *supra* note 7, at 5617 para. 59.

261. *See, e.g.*, Chloe Albanesius, *Netflix Speeds Jump 65 Percent on Comcast After Deal*, PC MAG. (Apr. 14, 2014, 5:37 PM), http://www.pcmag.com/article2/0,2817,2456553,00.asp.

262. Dan Rayburn, *Here's How the Comcast & Netflix Deal Is Structured, with Data & Numbers*, STREAMING MEDIA BLOG (Feb. 27, 2014, 12:14 PM), http://blog.streamingmedia.com/2014/02/heres-comcast-netflix-deal-structured-numbers.html; Joan E. Solsman, *Netflix vs. the Comcast-TWC Merger: Nothing to Lose*, CNET (Apr. 22, 2014, 5:54 AM), http://www.cnet.com/news/netflix-a-comcast-merger-nemesis-of-convenience/.

particular content.[263] With respect to the Internet, multiple ways to reach consumers always exist. In fact, Comcast maintains 40 settlement-free peering relationships and over 8,000 paid transit relationships.[264] That means that edge providers will always have some way to reach Comcast customers even if they are unable to reach a direct interconnection agreement.[265] The only bargaining advantage that Comcast would enjoy is the different between the interconnection terms and the cost of Netflix's next-best interconnection option.[266] Although some have speculated that Comcast might still be able to discriminate against Netflix traffic flowing over other paths, that traffic is mixed with the traffic of other end users, which would require Comcast to inspect all of the traffic coming through that connection,[267] which would be unrealistic and prohibited by Comcast's commitment to abide by the terms of the Open Internet Order.[268]

As an added benefit, absent the interconnection agreement, all of Comcast's customers would have had to bear the costs of Netflix's increase in traffic regardless if they used the service or not. The interconnection agreement promotes fairness by ensuring that those who derive the benefits are the ones who bear the costs. The elimination of zero-cost pricing also avoids the problems that arise when edge providers have no incentive to economize on the volume of traffic they send, as well as address the legal concerns raised by Judge David Tatel in his decision in *Verizon v. FCC*.[269]

Any remaining concerns should be eliminated by the fact that Comcast has committed to abide by the terms of the FCC's Open Internet Order even

---

263. For instance, in early 2014, after Viacom failed to reach a deal with Cable One, a small cable company, subscribers lost access to all Viacom channels, including Comedy Central and MTV. Alex Ben Block, *Viacom Blackout Continues as Small Cable Company Takes Stand in Retrans Fight*, HOLLYWOOD REPORTER (Apr. 2, 2014, 5:06 PM), http://www.hollywoodreporter.com/news/viacom-blackout-continues-as-small-693143.

264. *Competition in the Video and Broadband Markets: The Proposed Merger of Comcast and Time Warner Cable: Oversight Hearing Before the Subcomm. on Regulatory Reform, Commercial and Antitrust Law of the H. Comm. on the Judiciary*, 113th Cong. (May 8, 2014) (Joint Written Statement of David L. Cohen, Executive Vice President, Comcast Corp., and Robert D. Marcus, Chairman and Chief Executive Officer, Time Warner Cable), *available at* http://judiciary.house.gov/?a=Files.Serve&File_id=E55CD2D5-C965-4D7B-84E0-BFD386769F2C.

265. Christopher S. Yoo, *Innovations in the Internet's Architecture That Challenge the Status Quo*, 8 J. ON TELECOMM. & HIGH TECH. L. 79, 86 (2010).

266. Stanley M. Besen et al., *Advances in Routing Technologies and Internet Peering Agreements*, 91 AM. ECON. REV. (PAPERS & PROC.) 292, 295 (2001).

267. *Cf.* Timothy B. Lee, *The Durable Internet: Preserving Network Neutrality Without Regulation* 15–23 (Cato Inst., Policy Analysis No. 626, 2008), *available at* http://object.cato.org/sites/cato.org/files/pubs/pdf/pa-626.pdf (arguing that ISP efforts to degrade or discriminate against disfavored Internet traffic are unlikely to succeed for technical and economic reasons).

268. Applications of Comcast Corp., Gen. Elec. Co. & NBC Universal, Inc., *Memorandum Opinion and Order*, 26 FCC Rcd. 4238, 4275 para. 94 (2011) [hereinafter *Comcast-NBCU Order*] (barring Comcast from discriminating against unaffiliated Internet traffic and requiring Comcast to abide by the rules contained in the 2010 Open Internet Order).

269. Verizon v. FCC, 740 F.3d 623, 658 (D.C. Cir. 2014).

though it was struck down by the courts.[270] In fact, the merger would extend this benefit to all of Time Warner Cable's customers as well.

C. Case-by-Case Adjudication

The *Verizon* court's discussion of *Cellco* leaves open the possibility that the FCC could implement a regime based on case-by-case adjudication. *Cellco* upheld a requirement of commercial reasonableness in data roaming agreements as distinct from common carriage. There is much to recommend such an approach; indeed, I have advocated it for a long time.[271]

There are some legal constraints to adjudication. Under *Cellco*, if the FCC imposes a nondiscrimination mandate on a case-by-case basis, it would be invalid.[272] *Verizon* echoed this concern.[273] So although case-by-case adjudication is a viable option, the FCC cannot use it as a backdoor means for mandating nondiscrimination.

Ex post, case-by-case adjudication has a long legacy, with roots in the debate between rules and standards as well as the rejection of the codification movement during the Nineteenth Century.[274] Indeed, the distinction between ex ante rules and ex post adjudication may be somewhat overstated, in that rules are never as clear and standards are never as vague as people suggest. Both have their place, with standards being the preferred form of the legal rule when the nature of the problem is contextual and variegated.

As a policy matter, this regime should be exercised with great restraint. Content and applications are complements to broadband access. As such, contracts between content and applications providers and broadband access providers are properly regarded as vertical restraints. As a theoretical matter, the welfare implications of vertical restraints are ambiguous, as they may either benefit or harm consumers.[275] Economic theory suggests that consumer harm can arise only if the relevant markets are concentrated and protected by entry barriers; that is, if the participants have market power.[276] As noted above, the empirical literature indicates that vertical restraints are

---

270. *Comcast-NBCU Order*, *supra* note 268, 268, at 4275 para. 94 ("Comcast and Comcast-NBCU shall also comply with all relevant FCC rules . . . and, in the event of any judicial challenge affecting the latter, Comcast-NBCU's voluntary commitments concerning adherence to those rules will be in effect." (citations omitted)).

271. *See* YOO, *supra* note 221; Christopher S. Yoo, *Product Life Cycle Theory and the Maturation of the Internet*, 104 NW. U. L. REV. 641, 644, 669–70 (2010); Yoo, *supra* note 241, at 71–76; Yoo, *Consumers*, *supra* note 230, at 186; Yoo, *supra* note 226, at 1854–55, 1900, 1908; Yoo, *supra* note 161, at 7–8, 24, 75; Christopher S. Yoo, *Would Mandating Network Neutrality Help or Hurt Broadband Competition?: A Comment on the End-to-End Debate*, 3 J. ON TELECOMM. & HIGH TECH. L. 23, 44–47, 58–59 (2004).

272. Cellco P'ship v. FCC, 700 F.3d 534, 548–49 (D.C. Cir. 2012).

273. *Verizon*, 740 F.3d at 652.

274. *See* Andrew P. Morris, *Codification and Right Answers*, 74 CHI.-KENT L. REV. 355 (1999) (chronicling the rise of the codification movement and the opposition to it).

275. Yoo, *supra* note 157, at 180, 190, 282–85.

276. *Id.* at 196.

either neutral or welfare enhancing in the vast majority of cases.[277] Most importantly, case-by-case adjudication should be conducted based on empirical evidenced in the context of a concrete theory. Placing the burden of proof on the party challenging the practice will help promote experimentation with new products, services, and business models.

1. MetroPCS/YouTube

These facts counsel in favor of certain guidelines for case-by-case adjudication. First, we should impose a market-power screen to filter out cases unlikely to cause consumer harm. Contrary to the suggestion of the dissent in *Verizon*,[278] this would be a significant deviation from common carriage, which has historically not required market power.[279]

The point is illustrated by MetroPCS, which was the target of one of the first network neutrality complaints. MetroPCS is a regional wireless provider in the U.S.[280] Its 8.1 million subscribers as of the end of 2010 made it the fifth-largest provider in the U.S., although its customer base was less than one-tenth that of market leaders Verizon and AT&T.[281] It specializes in offering unlimited voice and text plans without long-term contracts and at monthly rates that are significantly lower than the prices charged by the top-four national providers.[282]

In the markets in which it operates, MetroPCS controls significantly less spectrum than its national rivals. In addition, unlike its national rivals, which provide broadband services through 3G platforms such as EV-DO and HSPA+, until September 2010 MetroPCS operated exclusively through a second-generation ("2G") technology known as 1xRTT CDMA.[283] Given its 2G roots, its network is based on the Binary Runtime Environment for

277. *See supra* notes 118–120 and accompanying text.

278. 740 F.3d at 664–66 (Silberman, J., dissenting).

279. Yoo, *supra* note 75, at 560; Herbert Hovenkamp, *Regulatory Conflict in the Gilded Age: Federalism and the Railroad Problem*, 97 YALE L.J. 1017, 1045 (1988) ("As early as the 17th century, the common law had derived the duty to charge reasonable rates from the common carrier's obligation to serve everyone . . . ."); Susan P. Crawford, *Transporting Communications*, 89 B.U. L. REV. 871, 882–84 (2009); Thomas B. Nachbar, *The Public Network*, 17 COMMLAW CONSPECTUS 67, 97–100 (2008).

280. MetroPCS has since been acquired by T-Mobile, although MetroPCS continues to do business under its own brand, pending the eventual migration of its customers onto T-Mobile's network. Marguerite Reardon, *T-Mobile to Shut Off MetroPCS Network in Three Cities in 2014*, CNET (Feb. 25, 2014 11:08 AM), http://www.cnet.com/news/t-mobile-to-shut-off-metropcs-network-in-three-cities-in-2014/.

281. Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, *Fifteenth Report*, 26 FCC Rcd. 9664, 9697 tbl.3 (2011) [hereinafter *Fifteenth CMRS Report*].

282. Scott Woolley, *The Upstart Company That Made the AT&T-Mobile Merger Possible*, FORTUNE (Mar. 22, 2011, 5:24 PM), http://fortune.com/2011/03/22/the-upstart-company-that-made-the-att-mobile-merger-possible/.

283. Mike Dano, *MetroPCS to Skip 3G With LTE Rollout?*, FIERCEWIRELESS (Aug. 3, 2010), http://www.fiercewireless.com/story/metropcs-skip-3g-lte-rollout/2010-08-03.

Wireless (BREW) platform, which was designed primarily for text rather than multimedia.[284] The inability to support popular video applications such a YouTube put MetroPCS at a competitive disadvantage. Because video delivered to mobile devices do not require the same resolution as full-sized television screens, MetroPCS was able to reduce the bandwidth needed by using Real Time Streaming Protocol (RTSP) to compress the video signal so that it would work effectively on its 2G network.[285] Its core 2G data plan was priced at $50 per month.[286]

On September 21, 2010, MetroPCS skipped deploying 3G altogether and became the first provider to offer service using the 4G technology known as Long Term Evolution (LTE).[287] Unable to offer service through a true smartphone, MetroPCS opted to deploy LTE through the Samsung Craft, a less expensive, but more limited device known as a feature phone that was able to support BREW.[288] Providers of many popular applications, including Flash and other web plug-ins, did not regard the platform as sufficiently widespread to create BREW-compatible versions.[289] MetroPCS was able to augment BREW to provide full-track music downloads and premium video content from NBC Universal, Black Entertainment Television, and Univision through its MetroSTUDIO service.[290] In this way, MetroPCS was able to offer limited data offerings in markets in which it possessed only 10 MHz of spectrum.[291] MetroPCS's initial LTE deployments offered two service plans: $55 per month for unlimited voice text and data access and $60 per month for the same services plus MetroSTUDIO.[292] The terms of service defining data access specified that it "may include, for example, multimedia steaming and video on demand services, as well as certain multimedia uploads, downloads and gaming services and applications" and

284. Mike Dano, *MetroPCS to Allow VoIP Over LTE*, FIERCEWIRELESS (Feb. 15, 2011), http://www.fiercewireless.com/story/metropcs-allow-voip-over-lte/2011-02-15.

285. *See id.*

286. *See, e.g.*, Chris Knape, *Metropcs Begins Offering Flat-Rate, Unlimited Calling Wireless Phone Service In West Michigan*, GRAND RAPIDS PRESS (May 8, 2009, 5:56 PM), http://www.mlive.com/news/grand-rapids/index.ssf/2009/05/metropcs_begins_offering_flatr.html.

287. *See Fifteenth CMRS Report*, *supra* note 281, at 9720 para. 70.

288. Chris Foresman, *Samsung Craft First LTE Handset, Launches on MetroPCS*, ARS TECHNICA (Sep. 21, 2010, 2:19 PM), http://arstechnica.com/gadgets/2010/09/samsung-craft-first-lte-handset-launches-on-metropcs/.

289. Paul Kapustka, *Samsung Craft: Hands On the First LTE 4G Phone*, PC WORLD (Sep. 22, 2010, 10:24 AM). http://www.pcworld.com/article/205988/ss.html.

290. Simon Chester, *MetroPCS Launches LTE in San Francisco, Still Only One Compatible Featurephone*, TECHCRUNCH (Dec. 1, 2010), http://techcrunch.com/2010/12/01/metropcs-launches-lte-in-san-francisco-still-only-one-compatible-featurephone/.

291. Letter from Carl W. Northrop, Paul Hastings, to Julius Genachowski, Chairman, FCC at 3 (Feb. 14, 2011) [hereinafter Northrop Letter], *available at* http://fjallfoss.fcc.gov/ecfs/document/view.action?id=7021029361.

292. *Id.*

may exclude data sessions from MetroSTUDIO, with MetroPCS retaining the sole discretion to determine what constitutes data access.[293]

On January 3, 2011, MetroPCS revised its 4G LTE service plans. It maintained its previous $60-per-month plan, while adding two lower-priced plans.[294] Its $40-per-month plan offered unlimited talk, text, and 4G Web browsing with unlimited YouTube access.[295] Its $50-per-month plan added additional features (international and premium text messaging, GPS, mobile instant messaging, corporate e-mail, caller identity screening, and MetroSTUDIO service via WiFi) as well as 1 GB of additional "data access."[296] Its $60-per-month plan offered unlimited data access and MetroSTUDIO through any connection.[297]

One week later, a group of advocacy groups—Free Press, Center for Media Justice, Media Access Project, New America Foundation, and Presente.org—submitted a letter calling for the FCC to investigate whether MetroPCS's proposed service plans violated the FCC's Open Internet Order.[298] Their primary complaint was that MetroPCS's $40 and $50 per month plans permitted unlimited access to YouTube, while potentially categorizing other voice and video services, such as Skype and Netflix, as data access subject to bandwidth limits.[299] Consumers Union followed eleven days later with a similar letter.[300]

MetroPCS responded on February 14, 2011. It emphasized its long legacy of being the only provider to offer low cost, unlimited service plans without long-term contracts or requiring deposits or credit checks. It also noted that it has access to significantly less spectrum than its leading competitors: "As a consequence, MetroPCS had to innovate to make maximum use of its relatively limited spectrum resources."[301] In addition, device manufacturers were focused on more spectrum-intensive deployments planned by Verizon and AT&T, which typically used 20 MHz

293. *See* John Bergmayer, *Not Unlimited. Unlimitedish.*, PUB. KNOWLEDGE BLOG (Jan. 3, 2011), https://www.publicknowledge.org/news-blog/blogs/not-unlimited-unlimitedish.

294. Northrop Letter, *supra* note 291, at 9–10.

295. *Id.*

296. *Id.*

297. Press Release, MetroPCS, MetroPCS' New 4G LTE Plans Offer Unprecedented Value and Choice with Prices Starting at Just $40 (Jan. 3, 2011), *available at* https://www.metropcs.com/press/news-releases/2011/mpcs-news-20110103.html.

298. Letter from M. Chris Riley, Counsel, Free Press, to Julius Genachowski, Chairman, FCC (Jan. 10, 2011), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7021025490.

299. *Id.*

300. Letter from Parul P. Desai, Policy Counsel, Consumers Union, and Mark Cooper, Director of Research, Consumer Federation of America, to Julius Genachowski, Chairman, FCC (Jan. 21, 2011), *available at* http://apps.fcc.gov/ecfs/document/view?id=7021026387. Some of these organizations also complained that MetroPCS's initial LTE deployments did not support VoIP because no VoIP clients were available for BREW. The arrival of an Android-based handset in early February 2011 allowed all MetroPCS 4G LTE customers to access VoIP so long as their handset was technically capable of doing so.

301. Northrop Letter, *supra* note 291, at 3.

of spectrum, whereas MetroPCS needed to develop LTE service on as little as 1.4 MHz of spectrum.[302]

Moreover, LTE adoptions were slowed by the fact that its initial $55-per-month and $60-per-month LTE plans were priced higher than its 2G data plans. At the same time, the arrival of Android handsets was causing data traffic in its 2G network to increase. MetroPCS's revised LTE plans were carefully designed to avoid having to invest capital to upgrade a 2G data network that was already in the process of becoming obsolete by encouraging wireless data users to migrate to the more spectrum-efficient LTE network without overburdening it in the process.[303] The primary mechanism for doing so was the $40-per-month LTE plan, which was cheaper than its $50-per-month 2G data plan.[304] Because subscribers to the $50-per-month 2G data plan already had access to unlimited YouTube downloads, MetroPCS felt it had to include this functionality in its $40-per-month LTE plan if it was to be able to encourage subscribers to migrate from 2G to LTE. The fact that the $50-per-month LTE plan allowed subscribers to download up to 1 GB of multimedia streaming also made it more attractive than the identically priced 2G plan. MetroPCS emphasized that it facilitated access to YouTube in response to customer demand. It lacked any financial arrangements that provide it with any incentive to favor YouTube, and that no other YouTube competitors had ever sought access to the MetroPCS network.[305]

As an initial matter, it is hard to see how any policy implemented by a firm of MetroPCS's size could hurt consumers or competition. It had less than 3% of all U.S. wireless subscribers as of the end of 2010.[306] In an era where creating greater competition in wireless networks remains a major policy goal,[307] network management remains an important tool for firms like MetroPCS to deploy competitive services notwithstanding the dearth of spectrum under their control. MetroPCS also clearly states that it specializes in offering low-cost plans that provide more limited features than its competitors. As Tom Keys, MetroPCS's chief operating officer, stated, "We didn't build this network or this device to be all things to all people."[308] Requiring that all of MetroPCS's service plans support all applications on

---

302. *Id.* at 7.

303. *Id.* at 10.

304. *See id.* at 8–9; Phil Goldstein, *MetroPCS Slashes Base LTE Smartphone Plan By $10, To $40/Month*, FIERCEWIRELESS (Feb. 2, 2012), http://www.fiercewireless.com/story/metropcs-slashes-base-lte-smartphone-plan-10-40month/2012-02-02.

305. Northrop Letter, *supra* note 291, at 11–12.

306. *Fifteenth CMRS Report*, *supra* note 281, at 9697 tbl.3.

307. *See, e.g.*, Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, *Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless*, 28 FCC Rcd. 3700, 3729 para. 3 (2013).

308. Kevin Fitchard, *LTE Launches in the U.S.—MetroPCS Style*, CONNECTED PLANET (Sept. 21, 2010, 10:08 AM), http://connectedplanetonline.com/3g4g/news/metropcs-launches-lte-092110/.

equal basis would have made it impossible for them to compete in this manner.

2. AT&T/Apple FaceTime

Apple's video chat application FaceTime initially operated only over WiFi connections. In late 2012, FaceTime began supporting video calls over cellular networks in late 2012. AT&T initially required users to pay for a "Mobile Share Plan" in order to use FaceTime over the carrier's 3G or 4G LTE data networks, although FaceTime over WiFi remained available to all AT&T customers.[309] The policy required consumers to pay for a more expensive data plan in order to access FaceTime over 3G or 4G LTE networks. The policy applied to mobile devices, including tablets with broadband access capabilities. Soon after announcing the policy, however, AT&T granted 3G and 4G FaceTime access to consumers who upgraded to the newest iPhone and switched to any metered data usage plan.[310]

AT&T's FaceTime policy drew criticism from network neutrality proponents, including public interest groups Free Press, Public Knowledge, and the New America Foundation's Open Technology Institute. Free Press claims that the network neutrality issues stem from AT&T's determination to block 3G and 4G accessible FaceTime "unless customers pay for a more expensive voice and data plan."[311] Critics of AT&T's FaceTime policy contend that it violates network neutrality rules because it differentiates FaceTime from similar, rival applications. They contend that AT&T's treatment of FaceTime is "a direct contradiction of the Commission's open internet rules for mobile providers" because it interferes with consumer choice between similar mobile applications.[312]

AT&T has defended its policy on its consumer blog by arguing that (1) its FaceTime policy is "fully transparent to all consumers" and (2) there is no blocking issue because the FCC's network neutrality rules do not regulate applications that are preloaded on the mobile device. AT&T has since revised its policy to make it more permissive, although it still restricts

309. Lynn La, *Only AT&T Mobile Share Plan Users Can FaceTime Over Its Cellular Network*, CNET (Aug. 17, 2012, 3:03 PM), http://www.cnet.com/8301-17918_1-57495717-85/only-at-t-mobile-share-plan-users-can-FaceTime-over-its-cellular-network/.

310. Amy Schatz, *AT&T Limits on Video-Chat App Spurs Complaint*, WALL ST. J. (Sept. 12, 2012, 1:27 PM), http://online.wsj.com/article/SB10000872396390443816804578004302003765548.html?mod=googlenews_wsj.

311. Josh Levy, *AT&T's FaceTime Blocking: There's a Complaint for That*, FREE PRESS (Sept. 18, 2012), http://www.freepress.net/blog/2012/09/18/atts-FaceTime-blocking-theres-complaint.

312. *AT&T's Plan to Restrict FaceTime Violates FCC Rules*, PUB. KNOWLEDGE (Aug. 17, 2012) http://web.archive.org/web/20120821204806/http://publicknowledge.org/att-facetime (accessed via Internet Archive).

usage by those subscribing to grandfathered unlimited data plans that the company no longer offers.[313]

Because Apple FaceTime is a feature of the Apple iOS operating system, not a user-installed application, it is unclear whether the Open Internet Order applies.[314] Indeed, applying the Order would effectively require network providers to provide open access to all operating systems as well as applications. In addition, because the relevant broadband network is a wireless network, the nondiscrimination mandate does not apply.[315] Moreover, the prohibition against blocking applies only to wireless applications that compete with AT&T's offerings.[316] Because AT&T does not offer video chat, a decisionmaker would have to conclude that voice services compete with video chat services.

Moreover, the practice may be upheld if it constitutes reasonable network management.[317] A leading member of the FCC's Open Internet Advisory Committee has shown that a single FaceTime user can consume between one third and one half of all of the bandwidth available on a single node.[318] FaceTime thus appears to be more likely to cause congestion or disrupt its network traffic than downloadable video chat applications. Moreover, the fact that FaceTime is preloaded to the most popular devices owned by AT&T customers may make it a bigger threat to network traffic management than other video chat applications.

3. Verizon/Google Tethering Apps

Tethering applications permit users to use mobile devices as wireless access points for connecting additional devices to the initial device's network.[319] Until recently, providers have been able to justify blocking tethering applications by citing the providers' right to reasonable network management.[320] Providers justify charging consumers an additional fee for

313. Adi Robertson, *AT&T Says "Any" Mobile Video Chat App Will Work on its Network by the End of 2013*, THE VERGE (May 20, 2013, 2:12 PM), http://www.theverge.com/2013/5/20/4348672/att-will-allow-all-video-chat-apps-on-its-network-by-end-of-2013.

314. Salvador Rodriguez, *AT&T Says Charging for FaceTime Doesn't Violate Net Neutrality*, L.A. TIMES (Aug. 22, 2012), *available at* http://articles.latimes.com/2012/aug/22/business/la-fi-tn-att-facetime-net-neutrality-20120822.

315. *See 2010 Open Internet Order*, *supra* note 2, at 17960 para. 99 (barring mobile broadband providers "from degrading a particular website or an application that competes with the provider's voice or video telephony services so as to render the website or application effectively unusable").

316. *Id.*

317. *Id.* at 17961 para. 103 ("[C]onditions in mobile broadband networks may necessitate network management practices that would not be necessary in most fixed networks.").

318. FCC Open Internet Advisory Comm., AT&T/FaceTime Case Study (Aug. 20, 2013), *available at* http://transition.fcc.gov/cgb/oiac/Mobile-Broadband-FaceTime.pdf.

319. Preserving the Open Internet, *Notice of Proposed Rulemaking*, 24 FCC Rcd. 13064, 13121 para. 164 (2009).

320. *See id.*

tethering because tethering enables consumers to attach multiple devices, many of which have higher data capacities than phones, which in turn increases data usage.[321] Google has granted mobile carriers' request to block wireless subscribers from accessing tethering applications unless they subscribe to a premium data service.[322] Google inadvertently made fourteen tethering apps available to all customers.[323] When Verizon reportedly asked that they be removed from the Google app store, Google complied without complaint.[324] An end user filed an informal complaint against Verizon claiming that this policy violated open access requirements imposed on C Block licensee holders.[325]

Verizon justified its additional tethering fee by arguing that tethered devices, such as laptops and tablets, have higher data capacities than phones, so customers who tethered use more data than customer who do not tether.[326] Under its tethering policy, Verizon charged both unlimited data plan subscribers as well as usage-based data subscribers an additional fee for tethering their Verizon mobile device to third party devices. Because of its determination to charge the latter, the additional fee seemed like an unnecessary distinction between the Verizon device and the third party device.

In July of 2012, Verizon entered a consent decree with the FCC, in which the company agreed to pay $1.25 million to the FCC for its failure to comply with C-Block conditions requiring the company to maintain open access to its network for all applications and devices.[327] Verizon failed to comply with this requirement by forcing customers to pay an additional cost in order to use tethering applications that connect third party devices to Verizon's network.[328] In addition to the fine, which amounts to little more than a slap on the wrist, Verizon agreed to implement a company-wide system to ensure compliance with the C-Block requirements of their LTE

---

321. *See, e.g.*, James Kendrick, *The Truth About Tethering: Pay Up or You Are a Thief*, ZDNET (Apr. 4, 2011, 4:30 AM), http://www.zdnet.com/blog/mobile-news/the-truth-about-tethering-pay-up-or-you-are-a-thief/1749.

322. Brian Chen, *F.C.C. Forces Verizon to Allow Android Tethering Apps*, N.Y. TIMES BITS BLOG (July 31, 2012, 6:01 PM), http://bits.blogs.nytimes.com/2012/07/31/fcc-verizon-tethering/?_php=true&_type=blogs&_r=0.

323. Ellis Hamburger, *Google Caves: Bans Free Wi-Fi Hotspots on Your Android Phone*, BUS. INSIDER (May 3, 2011, 11:07 AM), http://www.businessinsider.com/google-gives-in-kills-android-tethering-apps-at-carrier-request-2011-5.

324. *See* Chen, *supra* note 322.

325. Stephen Shankland, *Complaint to FCC: Verizon Mustn't Bar 4G Tethering*, CNET (June 7, 2011 2:46 AM), http://www.cnet.com/news/complaint-to-fcc-verizon-mustnt-bar-4g-tethering/.

326. Steven J. Vaughan-Nichols, *Verizon: No Free Tethering for Unlimited Data Plan Customers*, ZDNET (Aug. 1, 2012, 11:00 AM), http://www.zdnet.com/verizon-no-free-tethering-for-unlimited-data-plan-customers-7000001987/.

327. Cellco Partnership d/b/a Verizon Wireless, *Order*, 27 FCC Rcd. 8932, 8937–41 (2012).

328. *Id.*

network. [329] The system includes (1) training for employees on the requirements for licensees of C-Block spectrum, (2) legal review of all communications between Verizon and application store operators regarding availability of the application to Verizon customers, and (3) disclosure of all instances of noncompliance during the two-year implementation of the plan.[330] The fact that Verizon has now shifted all of its plans to usage-based billing has eliminated any incentive it may have to restrict tethering apps.

4. Verizon/Google Wallet

Google has developed a mobile payment application called Google Wallet, which it has built into the proprietary chip installed in certain phones.[331] Google Wallet permits consumers to secure digital transactions over a short distance using phones with a near field communication (NFC) chip.[332] NFC payment systems enable users to pay for items in physical retail stores by tapping an NFC-enabled device on a payment reader. In 2011, Verizon determined that it would not preload Google Wallet on its mobile devices and may prevent users from downloading the application to devices after-the-fact.[333] Verizon has expressed hesitance to embrace the application because it must ensure it is appropriately "integrated into a new, secure and proprietary hardware element" in the devices.[334]

Critics of Verizon's treatment of Google Wallet suggest that Verizon's decision on the issue is related to its potential to partner with other mobile carriers, AT&T and T-Mobile, to launch a mobile payment application called "Softcard." [335] Competition among mobile payment applications has increased as the application and e-commerce industry become more lucrative, as evidenced by the recent launch of Apple Pay.[336] Though it is "still unclear whether many consumers will want to use electronic wallets,"

---

329. *Id.*

330. *Id.*

331. Jason Del Rey, *New Google Wallet App Moves Past NFC and to All Major Carriers. iPhone Version on Tap?*. ALL THINGS D (Sep, 17, 2013, 7:35 AM), http://allthingsd.com/20130917/with-ios-version-on-tap-new-google-wallet-for-android-moves-past-nfc/.

332. *Id.*

333. Amir Efrati & Anton Troianovski, *War Over the Digital Wallet: Google, Verizon Wireless Spar in Race to Build Mobile-Payment Services*, WALL ST. J., Dec. 7, 2011, at B1, *available at* http://online.wsj.com/news/articles/SB10001424052970204770404577081610232043208.

334. *Id.*

335. Softcard was previously known as Isis, but changed its name in September 2014 to "avoid any potential association with the Islamic militant group bearing the same name." Brett Molina, *Wallet App Isis Changing Name to Softcard*, USA TODAY (Sep. 3, 2014, 12:29 PM), http://www.usatoday.com/story/tech/2014/09/03/isis-softcard/15018035/.

336. Mike Isaac, *As PayPal Spins Off, Apple Pay Signals New Era at Cash Register*, N.Y. TIMES, Oct. 1, 2014, at A1, *available at* http://www.nytimes.com/2014/10/01/technology/apple-pay-signals-new-era-at-cash-register.html.

carriers and developers hope "mobile-payment platforms create new revenue streams by training customers to use their phones to shop."[337]

Verizon may be able to overcome complaints regarding its potentially discriminatory treatment of Google Wallet if it can adequately show that Google Wallet may jeopardize security on its network. According to some sources, Google Wallet may raise security concerns. A security firm called Zvelo contended, "the Google Wallet PIN, which is required of users to confirm purchases made with their phones, can be cracked via an exhaustive numerical search."[338] In addition, some critics contend that NFC systems will compromise consumer privacy. Though Google "plans to require users to opt into any service that would use or store their purchase data," and even though "the current version of Google Wallet doesn't allow data to be stored," critics contend that NFC systems will not be consistent and anticipate breaches of consumer privacy.[339] Both of these concerns apply to all NFC systems and are not unique to Google Wallet.

A bigger threshold question is whether the fact that Google Wallet is a built-in feature of the chip instead of an application arguably takes it outside the purview of the Open Internet Order. As such, applying the Open Internet Order to Google Wallet would extend the Order's scope beyond content, services, and applications to hardware features as well.

5. Amazon Kindle/Zero Rating

Amazon's Kindle has raised a host of interesting issues as well. Originally, the Kindle was shipped with a proprietary network known as Whispernet that gave prioritized treatment to Amazon services.[340] More recently, the Kindle Fire accelerates content that accesses Amazon's cloud services through the Silk browser.[341]

---

337. Efrati & Troianovski, *supra* note 333.

338. Sarah Jacobsson Purewal, *Update: Google Wallet Security Concerns Raised*, TECHHIVE (Feb. 9, 2012, 12:30 PM), http://www.techhive.com/article/249599/google_wallet_security_concerns_raised.html.

339. Eliza Krigman, *Amazon's Fire May Rekindle Net Neutrality Debate*, POLITICO (Oct. 26, 2011, 11:22 PM), http://www.politico.com/news/stories/1011/66936.html; Michael Morisy, *Does the Amazon Kindle Violate Network Neutrality Principles?*, IT KNOWLEDGE EXCH. (Feb. 25, 2008, 4:48 PM), http://itknowledgeexchange.techtarget.com/networkhub/does-the-amazon-kindle-violate-network-neutrality-principles/.

340. *See* Suzanne Choney, *Amazon May Be Building a Wireless Network of its Own*, NBC NEWS (Aug. 23, 2013, 4:26 PM), http://www.nbcnews.com/tech/internet/amazon-may-be-building-wireless-network-its-own-f8C10989062.

341. Roslyn Layton, *IGF Highlights How Developing Countries Use Zero Rating Programs to Drive Internet Adoption*, TECHPOLICYDAILY.COM (Sept. 4, 2014, 6:00 AM), http://www.techpolicydaily.com/communications/igf-zero-rating-programs/; Alicia Levine, *Facebook and Google's Race to Zero: And the Real Opportunity for the Next 5 Billion*, MEDIUM (Mar. 22, 2014), https://medium.com/@alicialev/facebook-and-googles-race-to-zero-7136fc3e5925; Rob Pegoraro, *"Zero Rating": The Pros and Cons of Free Online Access*, YAHOO! TECH (Aug. 26, 2014), https://www.yahoo.com/tech/zero-rating-the-pros-and-cons-of-free-online-access-95775730069.html.

In addition, a growing number of content providers are partnering with network providers to ensure that their content does not count against mobile subscribers' bandwidth caps. Leading examples include T-Mobile's Music Freedom partnership with music streaming services, Facebook Zero, Twitter Zero, Wikipedia Zero, and the now defunct Google Free Zone, which are helping wireless broadband deploy in the developing world.[342] All of these practices raise interesting questions that are hard to anticipate in advance. They provide a strong justification for adopting a case-by-case approach.

VI. CONCLUSION

The pendency of court's decision in *Verizon* created a lull in which everyone was on good behavior and the focus shifted away from policy and towards law. The lull is over, and the renewed attention to network neutrality has just begun. What remains to be seen is how expansively the FCC will interpret its authority under section 706 and whether it will attempt to reclassify broadband access as a Title II service. Other issues to be resolved include the role of the states, the applicability of network neutrality to interconnection between ISPs, and how case-by-case adjudication will be conducted. What recent events have made clearest is that the *Verizon* decision was simply a way station in the debate over network neutrality and that the controversy is likely to continue for the foreseeable future.

342. Miriam Gottfried, *Mobile Banking Gets Riskier*, WALL ST. J., June 9, 2011, at B9, *available at* http://online.wsj.com/news/articles/SB10001424052702304887904576398220617110318.

Sender Side Transmission Rules for the Internet

Tejas N. Narechania*
Tim Wu**

TABLE OF CONTENTS

* Julius Silver Research Fellow, Columbia Law School.
** Isidor & Seville Sulzbacher Professor of Law, Columbia Law School.

I. INTRODUCTION

Since 1966, the Federal Communications Commission has, one way or another, protected businesses that deliver services over the nation's communications infrastructure. But in January 2014, the U.S. Court of Appeals for the D.C. Circuit struck down the FCC's net neutrality rules contained in its 2010 *Open Internet Order*.[1] FCC Chairman Tom Wheeler has since indicated that he will take up the D.C. Circuit's invitation to implement rules that, consistent with historic practice, "will meet the court's test for preventing improper blocking of and discrimination among Internet traffic."[2]

Chairman Wheeler's statement invites an obvious question: presuming that the FCC wants its rules to survive judicial scrutiny, what is the most prudent legal course? While the Commission has a variety of legal options, we focus here on two solutions that are almost certain to survive legal challenge, while not taking any position on the merits of possible alternatives.

We propose a novel option that relies on a partial return to the powers delegated to the FCC by Title II of the Communications Act.[3] In particular, we suggest that the Commission take seriously the asymmetric framework suggested by the D.C. Circuit based on the premise that two distinct transmissions comprise a single broadband transaction. Consider a common usage of a broadband connection: first, the subscriber—the consumer—*calls* an application, service, or other content provider using the carrier facilities for which she has purchased access. Second, the content provider *sends a response* to the consumer, which necessarily traverses the broadband carrier's facilities to reach the original consumer. This two-stage process is the framework adopted by the D.C. Circuit; as the court emphasized, it may be "logical to conclude that [a broadband provider] may be a common carrier with regard to some activities but not others."[4]

---

1. Preserving the Open Internet Broadband Indus. Practices, *Report and Order*, FCC 10-201, 25 FCC Rcd. 17905 (2010) [hereinafter *2010 Open Internet Order*], *aff'd in part, vacated in part sub nom.* Verizon v. FCC, 740 F.3d 623, 636–42 (D.C. Cir. 2014).

2. Tom Wheeler, Chairman, FCC, Statement on the FCC's Open Internet Rules (Feb. 19, 2014), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-325654A1.pdf; *see* Open Internet Remand, *Public Notice*, FCC GN Docket No. 14-28 (rel. Feb. 19, 2014); *see also* Protecting and Promoting the Open Internet, *Notice of Proposed Rulemaking*, GN Docket No. 14-28, FCC 14-61 (2014), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db0515/FCC-14-61A1.pdf.

3. 47 U.S.C. §§ 201-231 (2006).

4. *Verizon*, 740 F.3d at 653 (citing NARUC v. FCC, 533 F.2d 601, 608 (D.C. Cir. 1976)); *see also* FCC v. Midwest Video Corp., 440 U.S. 689, 701 n.9 (1979).

The FCC may therefore decide, as a matter of first impression, that *response* transactions are subject to common carrier rules against discrimination and blocking. Indeed, as we explain below, none of the arguments that the information service designation applies to a broadband connection's call service can be said to apply to the response transaction. Cabining the reach of the Commission's *Cable Modem Order*, which designated the call transaction an information service,[5] to *only* the first stage of the two-stage framework would restore the Commission's authority to enforce network neutrality rules over broadband-delivered content. In addition, because such sender-side regulation focuses on incoming traffic, it also provides a useful framework for addressing interconnection disputes between broadband carriers and content providers.

Alternatively, the FCC could simply examine whether changed circumstances have undermined its decade-old decision[6] to reclassify broadband transmissions from telecommunications services to information services. Our examination of the Commission's analysis shows that the factual premises underlying its 2002 conclusion are now largely obsolete. That decision relied on the outdated premise that broadband subscriptions were akin to dial-up services including AOL, all of which offered a bundle of services including email access, branded web browsers, newsgroups, chat rooms, and other Internet-based services. Today, the relevance of these bundled services is highly diminished, as broadband subscribers overwhelmingly rely on third-party services and products such as Gmail, Firefox, Google Groups, Facebook, Twitter, and Instagram.[7]

Thus, the FCC has at least two available paths. The first is predominantly legal: by adopting the two-stage framework articulated by the D.C. Circuit in *Verizon*, the Commission need only decide whether sender-side transmissions fit more comfortably within the statutory definition of a telecommunications service or an information service. The second path is predominantly factual: Is the Commission still swayed by its analysis, now well over a decade old, analogizing broadband subscription services to dial-up Internet access? Regardless of the path the Commission chooses, it will reach a similar destination. Either course allows the Commission to develop a regime that resembles its approach in the 1980s and 1990s—a period notable for the exponential growth of the telecommunications and Internet industries.

---

5. Inquiry Concerning High-Speed Access to the Internet Over Cable & Other Facilities, *Declaratory Ruling and Notice of Proposed Rulemaking*, FCC 02-77, 17 FCC Rcd. 4798, paras. 34–41 (2002) [hereinafter *Cable Modem Order*].

6. *Id.*

7. *See* discussion *infra* Part II.B.

II. BACKGROUND

For nearly fifty years, the FCC has enforced a regime whose basic purpose has been to foster the growth of network application providers and protect them from the owners of network facilities.[8] The most recent iteration of that regime, which attempted to enforce a form of basic network neutrality norms, was contained within the Commission's *Open Internet Order*,[9] but in fact the history of that effort stretches back into the 1960s.

A. The Original Antidiscrimination Regime

The relevant history of the net neutrality regime begins with the FCC's *Computer Inquiries* that began in 1966.[10] Context is important here. The late 1960s marked the beginning of a historic shift at the Commission and the White House away from support for a regulated monopoly and toward the encouragement of competitive markets—especially in new markets.[11] This shift was driven both by the FCC and the Office of Telecommunications Policy in the White House; its long-term effects were nothing short of monumental.[12]

The project began with selected segments of the communications industry, primarily long-distance telephony, satellite services, attachments, and what was then called "network data processing" (now known as Internet services).[13] In each of these areas, the FCC developed a new regulatory initiative with two overarching goals.[14]

First, given the long history of regulation resulting in barriers to entry, the FCC attempted to avoid overregulation of new markets to encourage competition.[15] Second, the Commission recognized that any new entrant in these markets would necessarily depend on monopoly carriers, and would therefore be exceptionably vulnerable to anticompetitive behavior.[16] Hence, the project's second goal was to prevent the carriers from undermining these

---

8. *See 2010 Open Internet Order*, *supra* note 1, at 18044–45 (2010) (Copps, Comm'r, concurring).

9. *See generally id.*

10. *See, e.g.*, *id.* at 18045 (Copps, Comm'r, concurring) (referring to the "Computer Inquiries"); Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, *Report and Order and Notice of Proposed Rulemaking*, FCC 05-150, 20 FCC Rcd. 14853, paras. 4 & n.9, 21 (2005) [hereinafter *DSL Reclassification Order*].

11. *See generally* TIM WU, THE MASTER SWITCH, chs. 7, 14 (2010) (tracing FCC regulatory action from Hush-A-Phone through the Bell divestiture).

12. *Id.* at 187.

13. *Id.* at 189.

14. *Id.*

15. *See 2010 Open Internet Order*, *supra* note 1, at para. 116.

16. *See id.* at para. 26.

new entrants.[17] These two goals underlay the Commission's *Carterfone* decision and the subsequent liberalization of network attachments, the various MCI and Execunet decisions,[18] which opened to competition the long-distance telephony market, the "Open Skies" policy for satellites,[19] and, most relevant to our purposes, the *Computer Inquiries*.[20] The combined effect of these policies was to create a communications economy that relied on common carriage services as the foundation for other markets, and eventually, entire industries. Indeed, the entire Internet economy may be understood as an unexpected byproduct of the policies pursued in the *Computer Inquiries*.[21]

This philosophy of opening markets on top of the network drove the FCC's *First Computer Inquiry*. The 1966 Notice of Inquiry that began the FCC's first foray into this space sought "information, views, and recommendations" regarding the vast "number of regulatory and policy questions" that had come to the fore through the "the growing convergence of computers and communications."[22] In the *Notice*, the Commission sought to determine "under what circumstances data processing, computer information, and message switching services . . . should be subject to the provisions of the Communications Act."[23]

While the technologies of this era were different, the basic architecture of the regulatory problem is familiar. Companies, such as Electronic Data Systems (founded by entrepreneur Ross Perot), located at the "ends" of the telephone network, were offering computer services that ran "over" AT&T's wires.[24] Conceptually, firms such as EDS occupied a position similar to

17. WU, *supra* note 11, at 189–90.

18. *See* Jim Chen, *The Legal Process and Political Economy of Telecommunications Reform*, 97 COLUM. L. REV. 835, 845–47 (1997) (discussing FCC rulemaking and litigation regarding MCI and Execunet).

19. *See* Establishment of Domestic Commc'ns-Satellite Facilities by Non-Governmental Entities, *Report and Order*, FCC 70-306, 22 F.C.C. 2d 86 (1970); Establishment of Domestic Commc'ns-Satellite Facilities by Non-Governmental Entities, *Second Report and Order*, FCC 72-531, 35 F.C.C. 2d 844 (1972), *recon. in part*, Establishment of Domestic Commc'ns-Satellite Facilities by Non-Governmental Entities, *Memorandum Opinion and Order*, FCC 72-1198, 38 F.C.C. 2d 665 (1972).

20. *See infra* notes 22–34 and accompanying text.

21. *See* WU, *supra* note 11, at 197–99.

22. Reg. & Policy Problems Presented by the Interdependence of Computer & Commc'n Servs. & Facilities, *Notice of Inquiry*, FCC 66-1004, 7 F.C.C. 2d 11, para. 2 (1966) [hereinafter *Computer I Notice*].

23. *Id.* at para. 18.

24. *See, e.g.*, Computer III Further Remand Proceedings: Bell Operating Co. Provision of Enhanced Servs., *Notice of Proposed Rulemaking*, FCC 95-48, 10 FCC Rcd. 8360, paras. 32, 33 n.81 (1995).

Netflix or Wikipedia today, while the role of AT&T is now played by such carriers as Comcast, Verizon, and AT&T.[25]

As noted, the FCC was motivated by an interest in avoiding overregulation in the new data processing market and protecting that nascent industry from the monopoly carrier. The *First Computer Inquiry* achieved the first goal by exempting data processing services from common carrier regulation.[26] The FCC accomplished its second goal with the *Inquiry*'s "maximum separation" rule, which required an incumbent carrier to form an entirely separate corporate entity if it wished to offer data processing or computer networking services.[27] The FCC believed that if AT&T was allowed to freely enter the market for network services, it could give itself unfair advantages to quickly eliminate competitors.[28] The Commission feared that the Bell companies would "favor their own data processing activities by discriminatory services, cross subsidization, [and] improper pricing," and therefore required that any carrier seeking to provide both transmission and processing capabilities segregate its offerings into "separate corporate entit[ies]."[29]

To address cases where the distinction between data "transmission" and "processing" was less clear, the FCC defined a category of "hybrid" services[30] that were regulated according to the regime that governed the "primary thrust" of the offering: Where transmission predominated, the service would be subject to regulation under the Communications Act; where data processing predominated, only the maximum separation rule applied.[31] Importantly, the Commission deferred further guidance on the distinction within hybrid services.[32] Instead, the FCC offered to conduct "ad hoc

25. In 2005, twenty-one years after AT&T's court-ordered divestiture, SBC—a Regional Bell Operating Company previously known as Southwestern Bell—acquired its former parent AT&T, thus creating the nation's largest unified telecommunications company. *See* WU, *supra* note 11, at 238–49.

26. Reg. & Policy Problems Presented by the Interdependence of Computer and Commc'n Servs. & Facilities, *Tentative Decision of the Commission*, 28 F.C.C. 2d 291, para. 24 (1970) [hereinafter *Computer I Initial Decision*].

27. *Id.* at para. 35.

28. *See id.* at paras. 25–26.

29. *Id.* at paras. 33, 36; *see also* Reg. & Policy Problems Presented by the Interdependence of Computer & Commc'n Servs. & Facilities, *Final Decision and Order*, FCC 71-255, 28 F.C.C. 2d 267, para. 12 (1971) [hereinafter *Computer I Final Decision*] (maintaining decision reached in *Computer I Initial Decision*); 47 C.F.R. § 64.702(c) (2013).

30. *Computer I Initial Decision*, *supra* note 26, at para. 39; *Computer I Final Decision*, *supra* note 29, at para. 31.

31. *Computer I Initial Decision*, *supra* note 26, at paras. 41–42; *Computer I Final Decision*, *supra* note 29, at paras. 31–32.

32. *See generally Computer I Initial Decision*, *supra* note 26.

evaluations . . . to determine whether a particular package offering was essentially data processing or communication."[33]

In 1979, the FCC's *Second Computer Inquiry* eliminated the confusing "hybrid" service and established a regime with just two layers: basic and enhanced services.[34] The new taxonomy created the first clear horizontal regulatory model in FCC history,[35] with its rough recognition of a transport layer and an application layer. *Computer II* put all firms offering services over the network into the enhanced category[36] and exempted them from most regulation.[37] At the same time, it maintained the common carriage rules for the underlying transport services that supported this growing industry.[38]

The *Computer II* approach was the governing regulatory regime during the period of the exponential growth during the 1980s and 1990s in the computer networking and Internet industries.[39] Notably, the explosion in network services during this time casts serious doubt on the claims that any regulation under Title II is necessarily inconsistent with economic growth.[40] To the contrary, the clever design of *Computer II*, which avoided overregulation of application-layer industries while simultaneously protecting them from carrier threats of blocking or discrimination, actually fueled growth in application-layer services.[41] Thus, the *Computer II* model can be understood as a great boon to firms like AOL and MSN, which

---

33. *Computer I Final Decision*, *supra* note 29, at para. 27.

34. Amendment of Section 64.702 of the Comm'n's Rules & Regs., *Final Decision*, 77 F.C.C. 2d 384, paras. 88–102 (1980) [hereinafter *Computer II Final Decision*].

35. *See* Richard S. Whitt, *A Horizontal Leap Forward: Formulating a New Communications Public Policy Framework Based on the Network Layers Model*, 56 FED. COMM. L.J. 587, 615 (2004).

36. *Computer II Final Decision*, *supra* note 34, at para. 114 (There is "no regulatory distinction between enhanced services."); *see id.* at paras. 5, 96, 109.

37. *Id.* at paras. 107, 119–120.

38. *Id.* at paras. 7, 12. Basic services included voice services. The revised rules also limited the application of the "maximum separation" rule to only AT&T and GTE (now known as Verizon).

39. *See* Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925, 930 (2001) ("The Internet is the fastest growing network in history. In its thirty years of existence, its population has grown a million times over.").

40. *See, e.g.*, Christopher S. Yoo, *Is There a Role for Common Carriage in an Internet-Based World?*, 51 HOUS. L. REV. 545, 557 (2013) ("[T]o the extent that the Internet generates positive externalities, imposing regulation would represent the opposite policy, systematically causing the systematic bias toward underproduction to worsen.").

41. *See* Robert Cannon, *The Legacy of the Federal Communications Commission's Computer Inquiries*, 55 FED. COMM. L.J. 167, 169 (2003); Jonathan Weinberg, *The Internet and "Telecommunications Services," Universal Service Mechanisms, Access Charges, and Other Flotsam of the Regulatory System*, 16 YALE J. ON REG. 211, 222 (1999).

provided low-cost network services simply by buying volumes of telephone numbers, as well as to the first wave of "dot-com" firms, such as Netscape and Yahoo!, which were able to reach users without paying costly termination fees to carriers.

The *Computer II* model survived until the early 2000s. Congress codified it in the Telecommunications Act of 1996, merely changing its nomenclature: an "enhanced service" was effectively renamed an "information service," and "basic service" became "telecommunications service."[42] Although *Computer II* was largely codified in statute, some details of the regime were modified by the Commission's lengthy *Third*

42. The Act's definition of a "telecommunications service"—the commercial offering of the transmission of user information between two points without any change to the information—mirrored the FCC's understanding of a "basic service" under *Computer II*. *Compare* 47 U.S.C. § 153(50), (53), *with Computer II Final Decision*, *supra* note 34, at para. 96 (basic service "offers a pure transmission capability over a communications path that is virtually transparent in terms of its interaction with customer supplied information."). *See also Computer II Final Decision*, *supra* note 34, at para. 5.Similarly, the Act's definition of "information service"—"the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications"—sounds in Computer II's "enhanced service" definition. *Compare* 47 U.S.C. § 153(24) *with Computer II Final Decision*, *supra* note 34, at para. 97 (in enhanced service, for example, "applications are used to act on the content, code, protocol, and other aspects of the subscriber's information."). *See also Computer II Final Decision*, *supra* note 34, at para. 5.
For more on the similarities between Computer II and the Telecommunications Act of 1996, see Fed.-State Joint Bd. on Universal Serv., *Report to Congress*, FCC 98-67, 13 FCC Rcd. 11501, para. 21 (1998) ("[W]e find that Congress intended the categories of 'telecommunications service' and 'information service' to parallel the definitions of 'basic service' and 'enhanced service' developed in our Computer II proceeding . . . ."). *See also* Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 977 (2005) ("The definitions of the terms telecommunications service and information service established by the 1996 Act are similar to the *Computer II* basic- and enhanced-service classifications." (internal quotation marks omitted)); Framework for Broadband Internet Serv., *Notice of Inquiry*, FCC 10-114, 25 FCC Rcd. 7866, para. 13 (2010) (the Telecommunications Act of 1996 "codif[ied] the Commission's distinction" from the *Computer Inquiries*); Kevin Werbach, *The Network Utility*, 60 DUKE L.J. 1761, 1774–75 (2011) (noting subtle difference in definitions).

Computer Inquiry,[43] which, most notably, eliminated the "maximum separation" rule.[44]

B. From Computer II to Information Service

Until the turn of the millennium, the Internet industry—that is, the set of application-layer data businesses that depended on networked telecommunications infrastructure—blossomed under a regime that both deregulated its services and protected them from carrier interference under Title II of the Communications Act of 1934. Shortly thereafter, the FCC sought to preserve these critical goals under a new regulatory structure. It moved to an alternative regime that reclassified all Internet services—including the underlying carrier services—as "information services,"[45] while still preventing carrier abuses through the enforcement of net neutrality norms.[46]

In 1998, the Commission began considering how to appropriately classify broadband services, beginning with the puzzle posed by cable Internet service providers.[47] Cable broadband providers vertically integrated many of the functions that were sold separately by "enhanced service" providers like AOL. In fact, one of the justifications for the AOL-Time

---

43. Amendment of Section 64.702 of the Comm'n's Rules & Regs (Third Computer Inquiry), *Notice of Proposed Rulemaking*, FCC 85-397, 50 Fed. Reg. 33581 (1985). This final proceeding in the trilogy of *Inquiries* lasted over a decade, spawning a plethora of orders and related litigation. *E.g.*, Amendment of Sections 64.702 of the Comm'n's Rules & Regs (Third Computer Inquiry), *Report and Order*, FCC 86-252, 104 F.C.C. 2d 958 (1986), *vacated sub nom.* California v. FCC, 905 F.2d 1217 (9th Cir. 1990); California v. FCC, 4 F.3d 1505 (9th Cir. 1993); California v. FCC, 39 F.3d 919 (9th Cir. 1994). In the end, *Computer III* replaced the "maximum separation" rule with a variety of technical rules mandating interconnection and a series of accounting safeguards to prevent cross-subsidization and potentially anticompetitive pricing practices. *See generally* Computer III Remand Proceedings: Bell Operating Co. Safeguards and Tier 1 Local Exchange Co. Safeguards, *Report and Order*, FCC 91-381, 6 FCC Rcd. 7571 (1991), *vacated in part sub nom.* California v. FCC, 39 F.3d 919 (9th Cir. 1994).

44. The motivation to remove the maximum separation rule was driven, in part, by a Chicago School-based understanding of the benefits of vertical integration. But as we explain further, such an understanding of vertical integration understates the possibility for network platforms to make anticompetitive use of vertical agreements by, for example, exclusion.

45. *See Cable Modem Order*, *supra* note 5; *DSL Reclassification Order*, *supra* note 10.

46. Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, *Policy Statement*, FCC 05-151, 20 FCC Rcd. 14986, para. 4 (2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf.

47. *See* Inquiry Concerning the Deployment of Advanced Telecomms. Capability to All Ams. in a Reasonable & Timely Fashion, *Notice of Inquiry*, FCC 98-187, 13 FCC Rcd. 15280, paras. 77–82 (1998).

Warner merger in 2000 was facilitating such integration.[48] Cable providers therefore seemed to be offering what, under the *Computer Inquiries* model, would have been two services: a telecommunications service and an information service.[49] Consequently, based on the statutory text of the Telecommunications Act—which, as we have noted, codified the *Computer II* regime—the Ninth Circuit concluded that cable operators were clearly offering both services.[50]

In 2002, the FCC departed from the interpretation derived from its *Computer Inquiries* by reclassifying all of the layers of cable modem service as one single "information service."[51] This designation had the critical effect of exempting it from the regulatory structure of Title II.[52] The Commission's reclassification rested on a few critical facts. First, the Commission compared the commercial offering of a cable modem service provider with the predominant alternative at the time: a dial-up internet connection offered by an independent provider like Earthlink or AOL (before its merger).[53] Such Internet service providers typically offered a bundle of Internet services that were not themselves separable and had no separate legal status: a subscription to AOL came with access to an aol.com email address, to AOL-based newsgroups, as well as to the domain name system ("DNS").[54] So too with cable modem service: A cable modem subscriber had access, for example, to a [provider].net email address, a DNS, and other related services.[55] Thus, because dial-up Internet services were considered information services,[56] the Commission reasoned that cable modem service must also be an information service.[57]

Critical to the FCC's decision was its enigmatic conclusion that the "telecommunications component is not . . . separable from the data-processing capabilities of the [cable modem] service."[58] Dial-up Internet access providers, such as AOL, sold only data processing capabilities; the transmission component was separately sold and provided by each subscriber's respective phone company.[59] By contrast, the Commission noted that, at the time, no "cable modem service provider ha[d] made a stand-

48. WU, *supra* note 11, at 264–65.
49. *See* discussion *supra* Part II.A.
50. AT&T Corp. v. City of Portland, 216 F.3d 871 (9th Cir. 2000).
51. *Cable Modem Order*, *supra* note 5, at para. 7.
52. *See* 47 U.S.C. § 153(51) ("A telecommunications carrier shall be treated as a common carrier under this [Act] only to the extent that it is engaged in providing telecommunications services.").
53. *Cable Modem Order*, *supra* note 5, at para. 10.
54. *Id.*
55. *Id.* at para. 17.
56. *Id.* at para. 38.
57. *Id.*
58. *Id.* at para. 39.
59. *Id.* at para. 9, n.19.

alone offering of transmission for a fee directly to the public."[60] Hence, the Commission found that "the telecommunications is part and parcel of cable modem service and is integral to its other capabilities" such as email and newsgroups. [61] The Commission's conclusion that this transmission capability was inseparable from the rest of the commercial offering was questionable in 2002; today, as we discuss below, it seems clearly erroneous given the widespread demand for independent services that compete with a provider's bundled offering. [62]

The Supreme Court ultimately reviewed the FCC's *Cable Modem Order* in *National Cable & Telecommunications Association v. Brand X Internet Services*.[63] Although *Brand X* is a favorite of administrative law aficionados for its discussion of judicial deference to administrative agencies under *Chevron*,[64] the decision is, at its core, about telecommunications law. The majority in *Brand X* found sufficient ambiguity in the Telecommunications Act's definition of "telecommunications service"—"the offering of telecommunications for a fee directly to the public"[65]—that the Court deferred to the Commission's conclusion that cable modem service fell outside of its ambit.[66] In particular, the Court noted that the critical question for the *Cable Modem Order* was whether "from the consumer's point of view" the data transmission service is used "always in connection with the information-processing capabilities."[67] The Court concluded that it was: The transmission component, after all, was in the Commission's view "part and parcel" of the rest of the service.[68] Because the Court determined that "offering can reasonably be read to mean a 'stand-alone' offering," it held that the Commission need not treat "the underlying telecommunications used to transmit that service" as a separate "offer" under the Telecommunications Act's regime.[69]

Although the Court deferred to the Commission's conclusion in the *Cable Modem Order*, some members were doubtful. Justice Breyer noted that the Commission's interpretation "just barely" fell within the "scope of the [FCC's] statutorily delegated authority." [70] Three justices dissented,

---

60. *Id.* at paras. 39–40.
61. *Id.* at para. 40.
62. See discussion *infra* Part III.A.
63. Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 973–74 (2005).
64. Chevron, USA, Inc. v. Natural Res. Def. Council, 467 U.S. 837 (1984); *see also Brand X*, 545 U.S. at 982–83 (under *Chevron*, an agency interpretation of an ambiguous statute can override prior judicial interpretation).
65. 47 U.S.C. § 153 (2010).
66. *Brand X*, 545 U.S. at 993.
67. *Id.* at 988.
68. *Id.* (quoting *Cable Modem Order*, *supra* note 5, at para. 39).
69. *Brand X*, 545 U.S. at 989.
70. *Id.* at 1003 (Breyer, J., concurring).

writing that "the telecommunications component of the cable-modem service retains such an ample independent identity that it *must* be regarded as being on offer."[71] Despite this skepticism from four justices, the Court upheld the Commission's *Cable Modem Order*. Propelled by its victory in *Brand X*, the Commission extended the "information service" designation to Internet access via DSL (digital subscriber lines)[72] and to other physical platforms,[73] including wireless networks.[74]

These various reclassification orders threatened to undermine the FCC's long-held regulatory aim of protecting application layer companies from the threat of discrimination and blocking by carriers.[75] Former FCC Chairman Michael Powell proposed that some behavior once prohibited by Title II would still be punished under a net neutrality regime that could be enforced even under the new classification. In a 2004 speech, Powell proposed four "Internet Freedoms,"[76] which the Commission later codified as a policy statement,[77] and which served as a baseline for the *Open Internet Order*.[78] Notably, in 2005, the Commission seemed to assume that it retained authority to enforce its policy statement under its Title II powers. Faced with the first major complaint regarding the blocking of Internet traffic, the Commission settled with Madison River Communications to resolve the claim that the company was blocking Voice over Internet Protocol applications in violation of Section 201 of the Telecommunications Act of 1996.[79] Since reaching that settlement, however, the Commission has faced

---

71. *Id.* at 1008 (Scalia, J., dissenting) (emphasis added). Justices Souter and Ginsburg joined Justice Scalia's dissent.

72. *DSL Reclassification Order*, *supra* note 10.

73. United Power Line Council's Petition for Declaratory Ruling Regarding the Classification of Broadband over Power Line Internet Access Serv. as an Info. Serv., *Memorandum Opinion and Order*, FCC 06-165, 21 FCC Rcd. 13281 (2006).

74. Appropriate Regulatory Treatment for Broadband Access to the Internet Over Wireless Networks, *Declaratory Ruling*, FCC 07-30, 22 FCC Rcd. 5901 (2007).

75. *See supra* notes 36–41 and accompanying text.

76. Michael K. Powell, Chairman, FCC, Remarks at the Silicon Flatirons Symposium on "The Digital Broadband Migration: Toward a Regulatory Regime for the Internet Age," (Feb. 8, 2004), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-243556A1.pdf.

77. Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, *Policy Statement*, FCC 05-151, 20 FCC Rcd. 14986, para. 4 (2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf.

78. *2010 Open Internet Order*, supra note 1, at para. 5.

79. Madison River Communications, LLC and Affiliated Companies, *Consent Decree*, DA 05-543, 20 FCC Rcd. 4295, paras. 4 & 6 (2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-543A2.pdf. The Consent Decree notes that the FCC was investigating "Madison River's compliance with section 201(b) . . . with respect to the blocking of ports used for Voice over Internet Protocol ("VoIP") applications." *Id.* at para. 1. Section 201(b) provides that "[a]ll charges, practices, classifications, and regulations for and in connection with such

formidable legal challenges to its authority to enforce these principles, losing before the D.C. Circuit in 2010[80] and again in 2014.[81]

III. PRESENT OPTIONS

For half a century, the FCC has maintained some system for policing the power of carriers to block or discriminate against application layer businesses attempting to reach customers over carrier wires.[82] The recent invalidation of the Commission's *Open Internet Order* in *Verizon*[83] casts that basic premise into doubt for the first time in the history of modern computer networking. Unsurprisingly, the Commission has responded by indicating that it will seek to reinforce its authority by whatever means necessary.[84] The operative question, then, is how the Commission can most easily accomplish this goal.

The FCC's decision to sweep the transmission of Internet traffic outside of the definitional scope of "telecommunications service" has significantly affected its ability to regulate such traffic. [85] The Telecommunications Act of 1996 explicitly provides that a "carrier shall be treated as a common carrier under this chapter *only to the extent that it is engaged in providing telecommunications services.*" [86] Thus, where a facilities owner—a carrier—is providing a service other than "telecommunications" (as the term is statutorily defined[87]), the Commission

---

communication service, shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful." 47 U.S.C. § 201(b) (2006).

80. Comcast Corp. v. FCC, 600 F.3d 642, 661 (D.C. Cir. 2010).

81. Verizon v. FCC, 740 F.3d 623, 628 (D.C. Cir. 2014).

82. *See* discussion *supra* Part II (chronicling the FCC's Computer Inquiries and the Open Internet Order).

83. *Verizon*, 740 F.3d at 659.

84. Protecting & Promoting the Open Internet, *Notice of Proposed Rulemaking*, FCC 14-61, 29 FCC Rcd. 5561 (2014) [hereinafter *2014 Open Internet NPRM*]; *see also* New Docket Established to Address Open Internet Remand, *Public Notice*, DA 14-211 (Feb. 19, 2014), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DA-14-211A1.pdf (establishing a new docket to consider path forward based on "authority under section 706 and *all other available sources of Commission authority*" (emphasis added)).

85. *2014 Open Internet NPRM*, *supra* note 84, at para. 149.

86. 47 U.S.C. § 153(51); *see also* Nat'l Cable & Telecomms. Ass'n v. Brand X. Internet Servs., 545 U.S. 967, 975 (2005) ("The Act regulates telecommunications carriers, but not information-service providers, as common carriers.").The provision was originally codified at 47 U.S.C. § 153(49), and was moved to subsection 51 following subsequent amendments to the Telecommunications Act of 1996. *See* Pub. L. No. 105-33, § 3001(b) (1997) (adding new (49) and renumbering) and Pub. L. No. 111-260, § 101 (2010) (renumbering).

87. 47 U.S.C. § 153(50) (2006).

has disabled itself from regulating that service as a common carrier.[88] The Commission has twice sought alternative ways of regulating Internet traffic. Both attempts were squarely rejected by the D.C. Circuit. First, the Commission's attempt to rely on its ancillary authority was rejected in *Comcast*;[89] more recently, in *Verizon*, the court held that the Commission's *Open Internet Order* imposed on broadband providers rules tantamount to common carrier regulation in violation of the Communications Act's "specific prohibition[s]" described above.[90]

Some have suggested that section 706 of the Telecommunications Act can provide the FCC with the authority to enforce basic network neutrality norms with some limitations.[91] We do not express any opinion on this hypothesis. Our present focus, instead, is on the Commission's traditional power to regulate carriers. Some have called for the Commission to overturn its 2002 reclassification decision.[92] As explained in more detail below, we agree that the *Cable Modem Order*'s conclusions no longer have a substantial basis in fact.[93] However, we begin with a more modest solution: a narrow application of the Commission's strongest and most secure grant of congressional power: Title II of the Telecommunications Act.[94]

A. Sender Side Transmission Rules

Over the course of Verizon's challenge to the *Open Internet Order*, the FCC and Verizon articulated distinct and competing visions of the nature of the relationship between broadband carriers and content providers. The Commission argued that content providers were not, in any meaningful sense, "customers" of a broadband carrier; to the contrary, the Commission argued that broadband subscribers are the *only* necessary customers, and the relationship between a content provider and the carrier is simply *derivative*

---

88. What it means to be "treated as a common carrier" remains unclear and fiercely contested. *See, e.g.*, Cellco P'ship v. FCC, 700 F.3d 534, 538 (D.C. Cir. 2012) ("The Act's definition of 'common carrier' is unsatisfyingly circular . . . .").

89. *See* Comcast Corp. v. FCC, 600 F.3d 642 (D.C. Cir. 2010).

90. Verizon v. FCC, 740 F.3d 623, 649–50 (D.C. Cir. 2014).

91. *E.g.*, Tom Wheeler, Chairman, FCC, Prepared Remarks at Silicon Flatirons, Univ. Colo. Law School (Feb. 10, 2014), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-325531A1.pdf; Tejas N. Narechania, *Federal and State Authority for Network Neutrality and Broadband Regulation*, STAN. TECH. L. REV. (forthcoming 2014), *available at* http://ssrn.com/abstract=2404996.

92. *See, e.g.*, Comments of Pub. Knowledge & Common Cause at 11–12, Open Internet Remand, FCC GN Docket No. 14-28 (rel. Mar. 24, 2014), *available at* http://www.publicknowledge.org/assets/uploads/documents/Public_Knowledge_Common_Cause_Open_Internet_706_Public_Notice_Comments.pdf.

93. *See* discussion *infra* Part III.B.

94. *See generally* 47 U.S.C. §§ 201–221.

of any request by that customer to view specified content.[95] The D.C. Circuit rejected this construction.[96] Instead, it adopted the view proffered by Verizon, which argued that there were two distinct, separable, and equally important commercial relationships at issue: (1) the broadband provider's contract with "retail end-users" as well as (2) its relationship with "other providers that seek to deliver their own services over the common carrier's facilities."[97] The D.C. Circuit agreed that these were better treated as distinct relationships.[98] But in so doing, the court stated that it would be "logical to conclude that [a broadband provider] may be a common carrier with regard to some activities but not others."[99] In other words, by individuating these two commercial relationships, the court suggested the possibility for the distinct regulatory treatment of these separable transactions.

Therefore, rather than treat *all* Internet traffic as a monolithic entity subject to the same regulatory treatment, the FCC can split the facilities-based services offered by broadband carriers into two discrete transactions: first, a *call* by a broadband subscriber to request data from a third-party content provider; and second, a content provider's *response* to the subscriber. Imposing this two-stage call-and-response framework on the structure of Internet traffic—a framework derived from the D.C. Circuit's recent decision in *Verizon*—would allow the Commission to separately consider the appropriate regulatory treatment for each type of transaction.

This creates an obvious opportunity for the FCC to classify—in the first instance—one of these relationships as subject to some form of regulation under Title II. In particular, the Commission should consider the appropriate regulatory treatment of traffic that is sent by content providers in response to requests from retail end-users.[100] One important reason to

---

95. Brief for Appellee/Respondents at 60–63, Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014) (No. 11-1355) [hereinafter FCC Brief].

96. Verizon v. FCC, 740 F.3d 623, 653 (D.C. Cir. 2014); *but see* City of Arlington v. FCC, 133 S. Ct. 1863, 1869 (2013) (under a hypothetical statute, a court must defer to agency's definition of "common carrier").

97. Joint Reply Brief for Verizon & MetroPCS at 1, 6–8, Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014) (No. 11-1355) [hereinafter Verizon Reply Brief].

98. *Verizon*, 740 F.3d at 653.

99. *Id.* (citing NARUC v. FCC, 533 F.2d 601, 608 (D.C. Cir. 1976)); *see also* FCC v. Midwest Video Corp., 440 U.S. 689, 701 n.9 (1979).

100. Here, we use the term "response" somewhat loosely. We do not mean to cabin the applicability of our proposed framework to only particularized sorts of real-time "dialogues" between a user and a content provider. The framework is equally applicable to asynchronous communications (e.g., a user, who hosts her own email service, who receives an email days after an offline communication with an acquaintance). Rather, the point is that the commercial offer to deliver *incoming* traffic (incoming from the perspective of the access network) is distinguishable from the offer to the consumer for a broadband subscription. Happily, the offer to deliver *unwanted* incoming traffic, such as spam or malware, is also distinguishable,

consider distinct regulatory treatment for this aspect of the broadband transaction is that the broadband carrier is endowed with a terminating monopoly.[101] That is, the content provider has no alternative to the carrier to complete its response to the calling consumer. Such terminating monopolies have traditionally been subject to enhanced regulatory scrutiny, and the Commission's policies have, in recent years, strongly disfavored "access charges" imposed by terminating monopolists.

Classifying "sender-side" traffic as a telecommunications service is also, perhaps surprisingly, consistent with the *Cable Modem Order*. As we described above, [102] the Commission's analysis in that *Order* focused squarely on the broadband provider's relationship with the end user. In considering the "business relationships" between "cable operators" and "consumers," the Commission examined only *retail* subscribers to broadband service.[103] Indeed, even the Supreme Court agreed that the critical question addressed in the *Cable Modem Order* was what a broadband subscription looked like "from the consumer's point of view."[104] Thus, this specific focus on the set of bundled services that broadband providers sold their subscribers excluded any analysis of the opposing offer to charge for the delivery of traffic in the second stage of the two-stage framework described above.[105]

Despite this exclusion, both the D.C. Circuit and the FCC have proceeded on the assumption that the conclusion reached in the *Cable Modem Order* applies equally across both the call and the response transactions.[106] But the decision in *Verizon* makes clear that this need not be so. Indeed, the Commission has a long history of regulating a carrier in its

---

creating space for the FCC to create narrow exceptions for *reasonable network management*, as it had in the Open Internet Order.

101. *See 2014 Open Internet NPRM*, *supra* note 84, at para. 42 (finding that broadband providers are "terminating monopolies" for content providers needing to reach end users, because "most residential customers have only one or two options for wireline broadband Internet access service.").

102. *See* discussion *supra* Part II.B.

103. *Cable Modem Order*, *supra* note 5, at para. 30.

104. Nat'l Cable & Telecomms. Ass'n v. Brand X. Internet Servs., 545 U.S. 967, 988 (2005).

105. Even to the extent that the *Cable Modem Order* considered content offered through internet service providers, it emphasized that this content is typically bundled—from the consumer's perspective—with the broadband service. *See Cable Modem Order*, *supra* note 5, at paras. 52–53 (arrangements with unaffiliated ISPs offer an integrated service for which both the provider and the ISP take dual responsibility). The same cannot be said for YouTube or Netflix content that is delivered by Comcast. *Cf. The ISP Speed Index From Netflix*, NETFLIX, http://ispspeedindex.netflix.com/ (last visited April 2014) (Netflix reporting on differences among facilities owners over which it sends content).

106. Verizon v. FCC, 740 F.3d 623, 654–655 (D.C. Cir. 2014) (noting classification decision as applicable).

capacity as a terminating monopolist differently than in its capacity as a vendor of retail, end-user services.[107]

A closer analysis of the service that a broadband provider, in its capacity as a terminating monopolist, offers to a content provider in sender-side response transactions bears none of the hallmarks of an information service as described by the *Cable Modem Order*.[108] When Verizon delivers Netflix content to Verizon subscribers, it does not also offer Netflix "e-mail, newsgroups, and the ability to create a web page . . . ."[109] Instead, Verizon provides a discrete transmission service: It delivers traffic from the point of interconnection to a specified subscriber.

Verizon now wants to charge some content providers for this delivery.[110] Notably, the *Cable Modem Order*'s conclusion rested in part on the observation that no broadband "provider ha[d] made a stand-alone offering of transmission for a fee."[111] But Verizon's new proposal is exactly that:[112] It is a stand-alone offer of "transmission" "between . . . points" that Netflix (for example) has "specified." [113] This is paradigmatic "telecommunications service" that may be subject to regulation under Title II.[114] That is, the transmission of data from the Internet *to* an individual subscriber not only retains an "independent identity that it must be regarded as being on offer"—it seems to be the *only* identity that can be regarded as on offer.[115] Thus, relying on the distinction drawn by Verizon in its challenge to the *Open Internet Order*, the Commission can classify commercial offers to deliver sender-side traffic, beginning at the point of interconnection, as a telecommunications service under the 1996 Act.[116]

B. Changed Circumstances

As an alternative to the limited classification of sender-side traffic, the FCC could return to its original position that the transmission of all Internet traffic is a "telecommunications service."[117] That is, rather than simply

---

107. *See*, *e.g.*, Verizon Reply Brief, *supra* note 97, at 6–7.

108. *See Cable Modem Order*, *supra* note 5, at paras. 34–37.

109. *See id.* at para. 37.

110. *See Verizon*, 740 F.3d at 645–46.

111. *Cable Modem Order*, *supra* note 5, at paras. 39–40.

112. *Verizon*, 740 F.3d at 646 ("[B]ut for the Open Internet Order [Verizon] would be exploring . . . commercial arrangements" to charge for the delivery of sender-side traffic).

113. 47 U.S.C. § 153(50) (2006). Here, the "user" is Netflix, and "points . . . specified" are the point of interconnection and the "calling" subscriber.

114. *See* 47 U.S.C. § 153(53) (2006).

115. Nat'l Cable & Telecomms. Ass'n v. Brand X. Internet Servs., 545 U.S. 967, 1008 (2005) (Scalia, J., dissenting).

116. *See* Verizon Reply Brief, *supra* note 97, at 1.

117. There is one further wrinkle with regard to mobile Internet service. Section 332 of the Telecommunications Act states that providers of "commercial mobile

cabining the reach of *Cable Modem Order* to its original context—the call transaction—the Commission could undertake to address both stages of traffic by revisiting its conclusions in the *Cable Modem Order*.[118]

On this point, it is important to emphasize that no legal bar prevents the FCC from undoing its decision in the *Cable Modem Order*. Indeed, the Supreme Court has repeatedly recognized that agencies have "ample latitude to 'adapt their rules and policies to the demands of changing circumstances.'"[119] Indeed, changed circumstances seem to have invalidated many of the factual premises underlying the Commission's 2002 *Cable Modem Order*. That decision rests on a now-outdated understanding of cable-based broadband offerings: subscribers then "d[id] not need to contract separately" for "discrete services or applications."[120] Not only were these integrated applications "part and parcel" of the subscription package, [121] but—in the view of the *Cable Modem Order*—they formed a critical part of the *value* of the service to consumers.[122]

Today, it is no longer clear that these additional services add measurable value to broadband subscriptions. To be sure, the *Cable Modem Order* acknowledged the existence of competing content at the time it was adopted; it noted that, "by 'click-through' access," cable modem service offers "many functions from companies with whom the cable operator has not even a contractual relationship. For example, a subscriber . . . is free to download and use . . . a web browser from Netscape, content from Fox

---

services" are common carriers, whereas providers of other mobile services are exempt from common carrier regulation. 47 U.S.C. § 332 (2006). The FCC has concluded that wireless transmission of Internet traffic both "*is* an 'information service' and *is not* a 'commercial mobile service.'" Cellco P'ship v. FCC, 700 F.3d 534, 538 (D.C. Cir. 2012). Thus, "mobile-data providers are statutorily immune, perhaps twice over, from treatment as common carriers." *Id.*

Reclassification for wireless broadband would require undoing both layers of protection. *See id.* For present purposes we focus on the question that is common to all physical platforms for the transmission of Internet traffic: the information service designation. For now, it suffices to note that the FCC would have to also address the "commercial mobile service" finding of the *Wireless Classification Order*. 22 FCC Rcd. 5901, para. 37 (2007). That would require the FCC to conclude that wireless internet service is "for profit," is an "interconnected service," and is available "to the public or . . . to a substantial portion of the public," as those terms are defined in the Telecommunication Act. 47 U.S.C. § 332(d)(1) (2006).

118. *See generally Cable Modem Order*, *supra* note 5.

119. *See, e.g.*, Motor Vehicles Mfrs. Ass'n of the U.S. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 42 (1983) (quoting Permian Basin Area Rate Cases, 390 U.S. 747, 784 (1968)).

120. *See Cable Modem Order*, *supra* note 5, at para. 11.

121. *Id.* at paras. 11, 39.

122. *Id*. at para. 11 (accessing "unaffiliated" content "may require the subscriber to pay those entities an additional fee"); *see also* Nat'l Cable & Telecomms. Ass'n v. Brand X. Internet Servs., 545 U.S. 967, 988 (2005).

News, and e-mail in the form of Microsoft's 'Hotmail.'"[123] The *Cable Modem Order*, however, de-emphasized the import of these options, suggesting that they were simply redundant because such "functions currently are all [also] included in the standard cable modem service offering."[124]

The FCC did, however, wisely note the inchoate nature of the broadband business and conceded that "[c]ustomers, for their part, are still learning the capabilities of cable modem service and deciding which applications they prefer."[125] The intervening decade of experience has provided the Commission with vast data regarding actual consumer preferences between those affiliated applications that were critical to its determination that broadband access was properly classified an information service and other unaffiliated options. These data indicate that independent email services, such as Gmail and Outlook.com (formerly Hotmail), dominate comparable services that are supplied by broadband providers.[126] And the majority of Internet traffic is for content outside of the "services or applications" that are provisioned through the broadband subscription.[127]

Furthermore, while the FCC once expressed concern that "additional fee[s]" might deter a broadband subscriber from accessing "unaffiliated" content, the recent proliferation of paid broadband-based services, such as Netflix, suggests that such a concern is no longer well-founded.[128] That is, consumers are not only willing to access unaffiliated advertisement-supported content, they are also willing to pay to access content outside of that which is built into a broadband carrier's offering.[129]

---

123. *Cable Modem Order*, *supra* note 5, at para. 25.

124. *Id.*

125. *Id.* at para. 30.

126. *See* MARK GAYNOR, NETWORK SERVICES INVESTMENT GUIDE 124–125 (2002) ("By 1999, more Web-based email boxes existed in the United States and internationally than the total number of ISP-based email accounts . . . ."); *see also What Does Your ISP Say About You?*, MAILCHIMP (Nov. 26, 2013), http://blog.mailchimp.com/what-does-your-isp-say-about-you/ (data from an web-based email service provider showing that web-based email services outpace the popularity of ISP-based services); *Cable Modem Order*, *supra* note 5, at para. 25 (contrast between outside service providers and affiliated services).

127. *See* SANDVINE, GLOBAL INTERNET PHENOMENA REPORT 5-6 (2H 2013) (28% of traffic associated with Netflix, 17% with YouTube, 7% with BitTorrent, 3% with iTunes, 1% each for Amazon Video, Hulu, and Facebook, for a total of 58%).

128. Netflix has 33 million U.S. members, as compared to an estimated 115 million households in the U.S. Without controlling for household broadband access, Netflix *alone* has achieved 29% market penetration. *Compare* Letter from Reed Hastings, CEO, Netflix, Inc., to Shareholders (Jan. 22, 2014), *with* Daphne Lofquist et al., U.S. Census Bureau, *Households and Families: 2010*, *in* 2010 U.S. CENSUS BRIEFS (Apr. 2012).

129. *See* SANDVINE, *supra* note 127, at 6 (28% traffic for Netflix, 17% for YouTube).

Taken together, this evidence suggests a consumer preference to use the provider's transmission service to connect to third-party content services. Unlike the conclusions reached in the *Cable Modem Order*, end users do not use broadband transmission capabilities "always in connection" with the services offered by the provider.[130] To the contrary, end users increasingly view broadband service as providing predominantly a transmission service that connects them to content services provided by other entities, rather than as an integrated information service.[131] Viewed on the terms of *Cable Modem Order*—which emphasized the retail subscriber's view of the commercial "offer"[132]—the information service designation based on bundled services now seems quaint.

One bundled service bears special attention. Of critical importance to practically every broadband subscriber is the Domain Name System ("DNS") service. Stated simply, DNS service allows a web user to reach a particular website; www.fcc.gov, for example, is a signifier for a unique numerical address—an IP address—such as 192.104.54.5. A DNS service acts as an automated phone book, translating between the easily-remembered website name and its unique address. Standard web traffic, which still comprises roughly ten percent of all Internet traffic in North America,[133] depends on accurate DNS service. End users, then, seem to contract for DNS service when they subscribe for broadband access.[134]

That broadband subscribers contract for DNS service, however, need not mean that they are purchasing an information service. Indeed, even the *Cable Modem Order* itself provides no clear guidance as to whether DNS services are categorized as "data processing" or "transmission" services.[135] Turning to the statute, "telecommunications" is defined to mean "the

---

130. Nat'l Cable & Telecomms. Ass'n v. Brand X. Internet Servs., 545 U.S. 967, 988 (2005).

131. For a list of capabilities that even the *Cable Modem Order* considers to be within the "basic level" transmission functions, see *Cable Modem Order*, *supra* note 5, at para. 17 ("physical connection between the cable system and the Internet by operating or interconnecting with Internet backbone facilities . . . . protocol conversion, IP address number assignment, domain name resolution through a domain name system (DNS), network security, and caching").

132. *See Brand X*, 545 U.S. at 988; *see also Cable Modem Order*, *supra* note 5, at para. 35 (examining "the functions that cable modem service makes available to its end users").

133. SANDVINE, *supra* note 127, at 5 (HTTP traffic comprises 9% of internet traffic).

134. Although most DNS service comes with broadband service, it is increasingly offered on a stand-alone basis by independent entities (e.g., OpenDNS, Google DNS).

135. *Compare Cable Modem Order*, *supra* note 5, at para. 17 ("[B]asic" "functions" to "transmit data" include "domain name resolution through a domain name system (DNS)"), *with id.* at para. 37 ("DNS constitutes a general purpose information processing . . . capability").

transmission, between or among points specified by the user, of information of the user's choosing." [136] DNS service, then, merely enables telecommunications: In seeking to visit a website, the user identifies the information they want (the website) and the location from which they want it (www.fcc.gov), and requests that it be transmitted back to them. Any intermediate action to translate the website name to a particular address[137] is no more than a functional step carried out in service of that transmission.

Other policy considerations undercut the prevailing "information service" designation. The *DSL Reclassification Order*—one of the proceedings that followed soon after the *Cable Modem Order*—concluded that an "access requirement impedes deployment of innovative wireline broadband services."[138] The Commission has since rejected this reasoning, stating in its *Open Internet Order* that "openness is critical to . . . increased end-user demand for broadband, which drives network improvements."[139] That is, the Commission now believes that the statutory aims of the Telecommunications Act are more easily met through regulated access rules rather than deregulated access.

"Regulatory agencies do not establish rules of conduct to last forever," the Supreme Court has explained; the "forces of change do not always or necessarily point in the direction of deregulation."[140] The FCC retains the ability to re-examine the conclusions it reached in the *Cable Modem Order*

---

136. 47 U.S.C. § 153 (50) (2006).

137. The fact that either the address or the content might be cached, that different DNS services might point to two distinct but identical copies of the same website, or even that a single DNS might dynamically cycle through different locations for the same content need not change this conclusion. The instruction is best understood as a command to retrieve information from *any* of the available end points that matches www.fcc.gov. This is a reasonable construction of the phrase "points specified by the user;" the statute does not require that user command be so specific as to identify the IP address with particularity. *But see* Christopher Yoo, *supra* note 40, at 567 ("The fact that DNS determines from which of the multiple available endpoints a particular query will be served makes it hard to characterize Internet communications as being between "points specified by the user" as required by the definition of telecommunications service."). The FCC can permissibly construe the "*points* specified by the user" as simply "my computer" and "FCC," and allow the user to defer to the network's best judgment as to how to deliver that content. The point is further illustrated by a call forwarding service. Telephone service subscribers can request that incoming calls to them be forwarded to an alternate number even before reaching the end point (that is, the call forwarding is carried out by the network, not by the handset). In such cases, the network will dynamically reroute the call to an appropriate location in order to effectuate the intent of the caller. Yet the use of call forwarding does not mean that the telephone call is no longer a telecommunications service.

138. *DSL Reclassification Order*, *supra* note 10, at para. 97.

139. *2010 Open Internet Order*, *supra* note 1, at para. 14.

140. Motor Vehicles Mfrs. Ass'n of the U.S. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 37, 42 (1983) (alterations and citations omitted).

and its subsequent related decisions. A number of "chang[ed] circumstances" support the decision to treat broadband access as a telecommunications service. For one, consumer behavior suggests the users increasingly view broadband as a transmission service providing access to independent content providers and other subscription services, rather than as a bundle of applications that rely on an underlying faster-than-dial-up transmission service. That is, the "offer," which has always been capacious enough to *include* a telecommunications service, [141] is increasingly seen as *predominantly* a telecommunications service. [142] Furthermore, the Commission's view of how to best promote the statutory aims of the Telecommunications Act has fundamentally shifted: [143] where the Commission once thought that a nondiscrimination rule would deter network investment, it now believes that such rules will "increase incentives to invest in broadband infrastructure." [144] Given these "chang[ed] circumstances," including the shift in the "agency's view of what is in the public interest," the Commission can provide an amply reasoned analysis for reinstituting its classification of the transmission of Internet traffic as a telecommunications service.[145]

C. Proceeding by Adjudication

So far we have examined two routes for the FCC to consider as it forges a path forward from *Verizon*. But there are more permutations to consider; the Commission has a variety of procedural options, regardless of the substantive path it chooses.

Consider, for example, section 208 of the Communications Act,[146] which gives the Commission the adjudicatory authority to investigate and resolve complaints against common carriers.[147] In particular, it allows the

---

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

142. *Cf. Computer I Final Decision*, *supra* note 29, at para. 1.

143. *See* 47 U.S.C. § 1302(a) (2006) ("The Commission . . . shall encourage the deployment on a reasonable and timely basis of advanced telecommunications [broadband] capability to all Americans.").

144. *2010 Open Internet Order*, *supra* note 1, at para. 40.

145. *State Farm*, 463 U.S. at 57.

146. 47 U.S.C. § 208 (2006). Although we briefly discuss Section 208 here, we do not mean to opine on the proper scope of the rules that the FCC should impose under Title II. We note only that the FCC has, in the past, noted that it could "forbear . . . from all but a small handful of provisions necessary for effective implementation" of its policy goals. Framework for Broadband Internet Serv., *Notice of Inquiry*, FCC 10-114, 25 FCC Rcd. 7866, para. 28 (2010). We do not comment on which provisions of Title II are ripe for such forbearance.

147. Section 403 offers similar authority, but allows the FCC to act *sua sponte*. 47 U.S.C. § 403 (2006) ("The Commission shall have full authority and power at

FCC to initiate an inquiry into conduct that is inconsistent with the Commission's long-held goal of protecting application layer services from untoward carrier behavior.[148] If, for example, broadband carriers were to begin to discriminate against unaffiliated competing content, the Commission might reconsider its classification decisions through a series of adjudicatory proceedings. One such proceeding might address only sender-side traffic if the alleged violation affects only incoming traffic, or if it involves an interconnection dispute. A subsequent adjudication might expand the scope of inquiry as necessary.

The Commission, of course, retains the discretion to choose the mode of policymaking that it believes best serves the public interest.[149] So long as the Commission's "adjudicative procedures . . . produce the relevant information to mature and fair consideration of the issues," it is entitled to "proceed with caution, developing its standards in a case-by-case manner . . . ."[150]

In other words, the FCC can establish by adjudication that an offer to transmit data sent by a content provider to a subscriber is a "telecommunications service" subject to regulation under Title II.[151] And the Commission can then make an individual determination as to whether the particular practice at issue is "unjust" or an "unreasonable discrimination" against an application-layer service, [152] and enjoin the practice as necessary. [153] This approach has the notable benefit of allowing the Commission to operate on a case-by-case basis,[154] thereby creating room for the flexible administration of policy in a still-evolving technological space.[155]

---

any time to institute an inquiry, on its own motion, in any case and as to any matter or thing concerning which complaint is authorized to be made . . . .").

148. *See supra* notes 36–41 and accompanying text.

149. NLRB v. Bell Aerospace Co., 416 U.S. 267 (1974); *see also* Verizon Tel. Cos. v. FCC, 269 F.3d 1098 (D.C. Cir. 2001).

150. *Bell Aerospace*, 416 U.S. at 268; *see generally* Benjamin Kapnik, *Affirming the Status Quo?: The FCC, ALJs, and Agency Adjudications*, 80 GEO. WASH. L. REV. 1527 (2012) (reviewing quality of FCC adjudicatory process).

151. *See supra* Part III.A.

152. 47 U.S.C. § 202 (2006).

153. We note, for the sake of completeness, that the FCC would likely be unable to impose retrospective fines in cases that present first-of-their-kind departures from governing standards (including settled expectations regarding the reach of various classification decisions). *See generally* Verizon Tel. Cos., 269 F.3d at 1098. Nevertheless, the FCC can clearly order injunctive relief, which is the more important—and more practical—remedy.

154. Wheeler, *supra* note 91.

155. *See* Formal Complaint of Free Press & Pub. Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer Applications, *Memorandum Opinion and Order*, FCC 08-183, 23 FCC Rcd. 13028, paras. 30–32 (2008) (arguments in favor

IV. CONCLUSION

For nearly a half-century, the FCC has attempted to nurture the growth of the various application-layer industries by protecting them from the potential for owners of basic network infrastructure to block their content and discriminate against their services. The D.C. Circuit's decision in *Verizon v. FCC* to strike down the Commission's *Open Internet Order* has undermined the agency's ability to continue its efforts in service of that goal.

The FCC, however, is hardly helpless in the face of this setback. As we have explained, the Commission might follow a previously unconsidered option under Title II of the Communications Act. As Verizon itself argued, a broadband transaction can be understood as occurring in two-stages: a call and a response. This framework, which was adopted by the D.C. Circuit, allows the Commission to correctly characterize the response as no more than a telecommunications service. Such a conclusion would return the scope of the *Cable Modem Order* to its original context, while giving the Commission the ability to protect application service providers from anticompetitive carrier conduct.

Alternatively, the Commission could expand its frame of inquiry to both the call and response, and hold a proceeding to examine whether changed circumstances have undermined the Commission's 2002 classification of broadband services. As described above, we are confident that the factual premises underlying that decision are now obsolete.

As a legal matter, either possibility is less novel than it first appears. Both resemble the approach the FCC took in its *Computer Inquiries*. Furthermore, the Commission's regulatory authority under Title II is not subject to serious doubt, but is naturally cabined to the context of telecommunications. Most recently, the D.C. Circuit mentioned that, in enacting the Telecommunications Act of 1996, "Congress clearly contemplated that the Commission would continue regulating internet providers in the manner it had previously."[156] In short, we believe that the proposals described here represent the most straightforward and legally secure measures for ensuring the continued growth of the application industries that have blossomed while they remained insulated from the anticompetitive carrier conduct.

---

of an adjudicatory approach), *vacated sub nom.* Comcast Corp. v. FCC, 600 F.3d 642, 661 (D.C. Cir. 2010).

156. Verizon v. FCC, 740 F.3d 623, 639 (D.C. Cir. 2014) (citing Deployment of Wireline Services Offering Advanced Telecomms. Capability, *Memorandum Opinion and Order, and Notice of Proposed Rulemaking*, FCC 98-188, 13 F.C.C.R. at 24029–30 para. 35 (1998) ("We conclude that advanced services are telecommunications services.")).

Unintentional Antitrust: The FCC's Only (and Better) Way Forward with Net Neutrality after the Mess of *Verizon v. FCC*

James B. Speta*

TABLE OF CONTENTS

* Professor, Northwestern University School of Law.

I. INTRODUCTION

The principal, alternative vision to network neutrality rules has always been antitrust. Opponents of the Federal Communications Commission's use of Communications Act regulatory authority (if any it had) to create nondiscrimination rules have long argued that competition law is both an adequate and a superior way to address any concerns over ISP actions against content and applications providers. On the other hand, network neutrality advocates have argued that antitrust is neither doctrinally nor institutionally adequate for the task. In adopting its *Open Internet Rules*,[1] the FCC expressly rejected antitrust as well.

The recent decision of the U.S. Court of Appeals for the D.C. Circuit in *Verizon v. FCC*[2] somewhat ironically puts the FCC in the position of turning to antitrust. After the court granted a partial win to the FCC, recognizing its authority to regulate Internet carriers even if they do not provide "telecommunications services," the court also held that such regulation must stop short of "common carrier" regulation.[3] The FCC's quest, therefore, is how to address nondiscrimination without going so far as to impose common carriage. Indeed, although the court's opinion does not expressly state that conclusion, I believe that, short of reclassifying broadband services as telecommunications services, the FCC's only path forward is to adopt antitrust-like rules. It is the only way to make sense of the court's holding that the FCC has "some" authority under section 706.[4] Moreover, I believe that such an approach is preferable to any of the other alternatives the FCC might consider. Doctrinally, a competition law-based rule would better fit with the D.C. Circuit's explanation of the FCC's section 706 authority and would fall short of the forbidden zone of common carrier rules. As a policy matter, the FCC could address the core concern of net neutrality arguments: that ISPs would alter content or distribution markets by discriminating among content providers. And this approach would be better than reclassification, a scenario that would require the FCC to begin a lengthy process of calibrating numerous, outdated regulatory rules.

---

1. Preserving the Open Internet, *Report and Order*, FCC 10-201, 25 FCC Rcd. 17905 (2010) [hereinafter *2010 Open Internet Order*], *aff'd in part, vacated in part sub nom.* Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014).

2. 740 F.3d 623 (D.C. Cir. 2014).

3. *Id.* at 649.

4. To be clear, I have previously written (and still believe) that section 706 does not create any affirmative authority in the Commission to regulate broadband markets, except through the limited regulatory tools identified in the section. *See generally* James B. Speta, *The Shaky Foundations of the Regulated Internet*, 8 J. ON TELECOMM. & HIGH TECH. L. 101 (2010); James B. Speta, *FCC Authority to Regulate the Internet: Creating It and Limiting It*, 35 LOY. U. CHI. L.J. 15 (2003). That is, I think Judge Silberman's dissent adopted the better reading of the statute. Verizon, 740 F.3d at 659 (Silberman, J., dissenting).

The FCC in fact does seem to be moving in the path of a competition-law like standard, although as we go to press, its final path has not been decided.

If the foregoing reasoning is right, and the FCC has the authority to address discrimination by ISPs but the FCC's rules must mimic antitrust principles, then the remaining question is whether the FCC should bother with this path. The FCC could decide to leave such a scheme to the Department of Justice ("DOJ") or the Federal Trade Commission ("FTC"). After all, those agencies have long-standing, principal expertise in competition law. FCC action would likely be duplicative and perhaps not as competent as an approach led by the antitrust agencies. I think this challenge is wrong. The FCC likely has relevant technical and industry expertise that the antitrust agencies may not possess. More importantly, as an administrative agency, the FCC is empowered to make rules based on predictive judgments.[5] Though I am no defender of some of the FCC's more fanciful theories of the past, I do think, given the likelihood that broadband access markets will remain significantly concentrated, that a specialized agency should have the authority to impose certain behavioral requirements on the basis of predicted competitive effects.

Although all of this may be an acceptable policy result, *Verizon* also reveals the very serious dysfunction that plagues telecommunications policy. Flowing from the Supreme Court's willingness to permit FCC regulation of cable systems at a time when the Communications Act said nothing about them, the courts have long accommodated Congress' absence from communications policy. Even if Congress cannot or will not act, the Telecommunications Act of 1996 should have pointed toward common carrier regulation plus forbearance, not toward the building of a new edifice of uncertain regulatory powers.

II. NET NEUTRALITY REJECTS ANTITRUST

The fault line between net neutrality rules and antitrust is well-established. Net neutrality rules focus on nondiscrimination—that is, they make the act of discriminatory treatment illegal, absent any particularized showing that specific acts of discrimination have caused particular harms.[6] By contrast, an antitrust rule condemns discrimination only in instances in which discrimination has a particular effect: the likely foreclosure of competition.[7]

---

5. Rural Cellular Ass'n v. FCC, 588 F.3d 1095, 1105 (D.C. Cir. 2009) ("The 'arbitrary and capricious' standard is particularly deferential in matters implicating predictive judgments and interim regulations.").

6. *Verizon*, 740 F.3d at 633 (The "*Order* imposes an anti-discrimination requirement").

7. Brown Shoe Co. v. United States, 370 U.S. 294, 320 (1962) (antitrust laws are designed to protect "competition, not competitors").

The FCC's *Open Internet Order* quite explicitly stated that an antitrust rule would not serve the Commission's purposes: "We also reject the argument that only 'anticompetitive' discrimination yielding 'substantial consumer harm' should be prohibited by our rules."[8] The Commission explained that its purpose of maintaining an open Internet ecosystem "cannot be achieved by preventing only those practices that are demonstrably anticompetitive or harmful to consumers."[9] Applications and content providers needed assurance that "broadband providers [w]ould not pick winners and losers on the Internet – even for reasons that may be independent of providers' competitive interests or that may not immediately or demonstrably cause substantial consumer harm."[10]

To be sure, a particular rule can occupy the space between the substantive poles of nondiscrimination and antitrust. The *Open Internet Rules* forbade only "unreasonable discrimination,"[11] as do the common carrier provisions of the Communications Act.[12] Indeed, as discussed below, the Communications Act hardly forbade all discrimination.[13] Common carriers were permitted to offer different services to different customers; indeed, sometimes carriers were required to discriminate to advance other goals (such as universal service). The more that the "unreasonableness" of any discrimination is based on notions of competitive markets, the more such a rule resembles antitrust as a conceptual matter.

If a nondiscrimination rule were based on antitrust thinking, then its principal difference from antitrust enforcement would be institutional, a point to which I will return below. For now, however, note that institutional differences were also one of the FCC's grounds for rejecting antitrust as the best mode. When the FCC expressed its concern that an antitrust rule would not control behaviors that "may not immediately or demonstrably cause substantial consumer harm,"[14] it meant that it wanted more ex ante assurance than a more antitrust-like rule—one that relied on ex post determinations—might provide.

III. THE D.C. CIRCUIT REJECTS COMMON CARRIER NONDISCRIMINATION

The D.C. Circuit's decision in *Verizon v. FCC* puts the Commission on a Goldilocks-like quest to find broadband regulation that is "just right." The D.C. Circuit ruled that section 706 gave the FCC significant authority to regulate broadband markets, just so long as the FCC stopped short of

8. *2010 Open Internet Order*, *supra* note 1, at para. 78.
9. *Id.*
10. *Id.*
11. *Id.* at paras. 77–79.
12. 47 U.S.C. § 202(a) (2006).
13. *See infra* notes 53-55 and accompanying text.
14. *2010 Open Internet Order*, *supra* note 1, at para. 78.

requiring common carrier rules.[15] In its *Order*, the FCC had rejected two narrower interpretations of section 706. First, it rejected its earlier view that section 706 was merely hortatory, that the FCC should use whatever authority it otherwise had to "encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans."[16] Second, it rejected the view that section 706 was limited to the narrow list of regulatory tools set forth in the end of the section, including "price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market, or other regulating methods that remove barriers to infrastructure investment."[17] Instead, the FCC said that section 706 authorized it to take any measure that could increase infrastructure investment (by forbidding anything that might serve as a barrier to investment).[18] Given the recent breadth of the Supreme Court's *Chevron* cases,[19] the D.C. Circuit was more or less compelled to approve.[20]

But while the court recognized the FCC's regulatory authority over ISPs, it also said that the FCC could not—so long as it classifies ISPs as information service providers—subject them to common carrier regulation.[21] The court leaned heavily on *Midwest Video II*,[22] a 1979 opinion in which the Supreme Court held that FCC cable access rules improperly imposed common carriage regulation on cable television companies.[23]

---

15. Verizon v. FCC, 740 F.3d 623, 628 (D.C. Cir. 2014) ("Even though the Commission has general authority in this area, it may not impose requirements that contravene express statutory mandates. Given that the Commission has chosen to classify broadband providers in a manner that exempts them from treatment as common carriers, the Communications Act expressly prohibits the Commission from nonetheless regulating them as such.").

16. *2010 Open Internet Order*, *supra* note 1, at para. 120 (quoting Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, § 706(a) (codified at 47 U.S.C. § 1302(a))).

17. *2010 Open Internet Order*, *supra* note 1, at paras. 120-121. This view of course treated the concluding clause as meaning only those tools functionally equivalent to those specifically listed, *ejusdem generis*.

18. *Id.*

19. *See* City of Arlington, Tex. v. FCC, 133 S. Ct. 1863 (2013) (holding that the FCC was entitled to *Chevron* deference even on jurisdiction-expanding interpretations of the Communications Act); *see also* Thomas W. Merrill, *Rethinking Article I, Section 1: From Nondelegation to Exclusive Delegation*, 104 COLUM. L. REV. 2097 (2004) (arguing that agency jurisdictional decisions should receive only lesser *Skidmore* deference).

20. *Verizon*, 740 F.3d at 635 ("As the Supreme Court recently made clear, *Chevron* deference is warranted even if the Commission has interpreted a statutory provision that could be said to delineate the scope of the agency's jurisdiction.").

21. *Id.* at 628.

22. *See generally* FCC v. Midwest Video Corp., 440 U.S. 689 (1979).

23. Verizon v. FCC, 740 F.3d 623, 651 (D.C. Cir. 2014) ("For our purposes, perhaps the seminal case applying this notion of common carriage is *Midwest Video II*."); *id.* at 654 ("The Commission advances several grounds for distinguishing *Midwest Video II*. None is convincing.").

IV. REJECTING THE IDEA OF NONDISCRIMINATION WITHOUT COMMON CARRIAGE

The core of the D.C. Circuit's decision was that the FCC's actions under section 706 could not impose "common carrier" regulation; the important extension was its holding that the Open Internet Order's nondiscrimination and no-blocking rules constituted such forbidden common carrier regulation. In the face of such a decision, one standard administrative law move would be to ask whether the FCC could take another bite at the apple—that is, could the FCC attempt to explain further why the nondiscrimination rules it had adopted were not actually common carrier regulation, but rather something else short of it? The D.C. Circuit left this sort of path open in the *Comcast* case. Although the court rejected the FCC's attempt to regulate Comcast, it invited the FCC to better explain its authority for regulating broadband.[24]

In this case, although the history of common carrier regulation could support an argument that the FCC's nondiscrimination rules stopped short of "common carrier" regulation, the D.C. Circuit's decision appears to effectively foreclose that argument. The argument that nondiscrimination rules alone might not be common carriage requires first stepping back to definitional principles. The statutory language at issue forbids the treatment of non-common carriers as common carriers, and of course the FCC has classified broadband as a non-common carrier service.[25] One interpretive difficulty arises from distinguishing the oft-noted circularity of the definition of a common carrier with the obligations of common carriers. The first issue is one of status: is the carrier or the service common carriage? Then, the second issue addresses the regulatory treatment that attends such status.

Status as a common carrier service (or telecommunications service) arises principally (but not exclusively as discussed below) from "an undertaking to carry for all people indifferently."[26] The D.C. Circuit decided that the nondiscrimination and no-blocking rules required Internet providers to offer service indifferently, and therefore treated them as common carriers. In so doing, the court leaned on *Midwest Video II*, which similarly held that the FCC had gone too far in regulating cable television companies when

24. Comcast Corp. v. FCC, 600 F.3d 642, 658–61 (D.C. Cir. 2010).

25. *See* 47 U.S.C. § 153(51) (2006) ("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" (emphasis added)).

26. NARUC v. FCC, 533 F.2d 601, 608–09 (D.C. Cir. 1976) ("[T]he primary sine qua non of common carrier status is a quasi-public character, which arises out of the undertaking to carry for all people indifferently. This does not mean that the particular services offered must practically be available to the entire public; a specialized carrier whose service is of possible use to only a fraction of the population may nonetheless be a common carrier if he holds himself out to serve indifferently all potential users.").

those companies were similarly granted statutory protection from being subject to common carrier regulation.[27]

But in so holding, the D.C. Circuit seemed to ignore both the second test for status as common carriage and the FCC's decisions holding that Internet providers were not common carriers. In addition to serving the public generally, the controlling case law holds that "[a] second prerequisite to common carrier status [is] . . . that the system be such that customers 'transmit intelligence of their own design and choosing.'"[28] The FCC relied on this characteristic in holding that Internet providers' offering of general services such as DNS and caching meant that Internet service was not common carrier service—and the courts have upheld the FCC's decision.[29] The FCC's reliance on DNS service as a mode of transforming user inputs as opposed to merely providing transport service is somewhat suspect, but the D.C. Circuit could not, given *Brand X*, forbid the classification.[30]

Given that the D.C. Circuit did not confront the definitional issue head-on, it seems more likely that the court was saying that the nondiscrimination and no-blocking rules amounted to the application of common carrier obligations to non-common carriers and were therefore impermissible. This seems to be the better reading of section 153(51) in all events, for the section states that "[a] telecommunications carrier shall be treated as a common carrier . . . *only* to the extent that it is engaged in providing telecommunications services."[31] Moreover, if the FCC may not apply common carriage regulation to a telecommunications company's non-telecommunications activities, surely it cannot regulate as a common carrier a company that provides no telecommunications services whatsoever. But this then raises the question of whether it would be possible to treat a nondiscrimination and no-blocking requirement as a regulatory regime short of common carriage.

The history of common carriage and the history of the Communications Act support an argument that common carriage involves more than just nondiscrimination requirements. The Communications Act's scheme—borrowed of course from the Interstate Commerce Act's regulation of railroads[32]—required common carriers to provide service upon request, to charge only just and reasonable rates (along with just and reasonable terms and conditions), and not to engage in unreasonable discrimination.[33] In support of these substantive requirements, Congress created "an

27. *See generally* FCC v. Midwest Video Corp., 440 U.S. 689 (1979).
28. *NARUC*, 533 F.2d at 609.
29. NCTA v. Brand X Internet Servs., Inc., 545 U.S. 967, 974, 977–78, 987 (2005).
30. *See Id.*
31. 47 U.S.C. § 153(51) (2006).
32. James B. Speta, *A Common Carrier Approach to Internet Interconnection*, 54 FED. COMM. L.J. 225, 262–64 (2002).
33. 47 U.S.C. §§ 201-203 (2006).

administrative agency whose task was to oversee an industry."[34] Privately owned common carriers were required to file tariffs describing all of their rates, terms, and conditions, and the agency was empowered to suspend, investigate, and cancel tariffed offerings.[35]

The FCC might have argued that only this complete ecosystem—incorporating tariff-filing, rate control, and nondiscrimination—constitutes "treat[ment] as a common carrier under this chapter."[36] Tariff filing and ex ante rate control would, of course, be the most significant differences, for the Open Internet Order's nondiscrimination rules were meant to echo section 202's ban on "unreasonable discrimination."[37] But these are significant differences. Tariff filing was the central tool of the regulated industries regime under the Interstate Commerce Act and the Communications Act. "The duty to file rates with the Commission . . . and the obligation to charge only those rates . . . have always been considered essential to preventing price discrimination and stabilizing rates."[38] Tariff filing provided not only the means by which the expert agency could superintend the carriers, but tariffs became the inflexible contract between the carriers and the public: carriers were forbidden to deviate from the tariffs and even intended deviations were illegal and unenforceable. "This extraordinarily strict rule, which would eventually be called the 'filed rate doctrine,' was deemed necessary" to achieve the goals of nondiscrimination and rate regulation.[39] Although the Open Internet Order required transparency, this rule is distinct from tariff filing, for it does not afford the agency an opportunity to review carriers' terms and conditions before they become effective.[40] Similarly, the Order does not contemplate any review of rates to ensure they are "just and reasonable"[41] or any ex ante review of rates. To be sure, nondiscrimination

---

34. Joseph D. Kearney & Thomas W. Merrill, *The Great Transformation of Regulated Industries Law*, 98 COLUM. L. REV. 1323, 1325 (1998).

35. 47 U.S.C. §§ 204-205 (2006).

36. 47 U.S.C. § 153(51) (2006).

37. *2010 Open Internet Order*, *supra* note 1, at para. 77.

38. Maislin Indus., U.S., Inc. v. Primary Steel, Inc., 497 U.S. 116, 126 (1990) (citations omitted); *see also* Ariz. Grocery Co. v. Atchison, T. & S. F. Ry. Co., 284 U.S. 370, 384 (1932) ("In order to render rates definite and certain, and to prevent discrimination and other abuses, the statute require[s] the filing and publishing of tariffs specifying the rates adopted by the carrier, and [makes] these the legal rates; that is, those which must be charged to all shippers alike."); Kearney & Merrill, *supra* note 34, at 1331–32 (discussing importance of tariffing).

39. Kearney & Merrill, *supra* note 34, at 1331–32; *see also Maislin*, 497 U.S. at 126–27 ("Given the close interplay between the duties imposed by §§ 10761-10762 and the statutory prohibition on discrimination, this Court has read the statute to create strict filed rate requirements and to forbid equitable defenses to collection of the filed tariff." (citations omitted)).

40. The Communications Act does not require the FCC to approve tariffs before they become effective; rather, carriers must file them and the FCC has the authority to suspend or deny them. If the FCC does not act, the tariff goes into effect. 47 U.S.C. §§ 203-205.

41. As compared to 47 U.S.C. § 201(b).

rules can affect rates by eliminating rate differentials.[42] But the Order did not contemplate the cost-of-service regulation that so dominated the traditional model of common carrier regulation.

The FCC might even have found support in *Midwest Video II*, even though the D.C. Circuit relied on it in deciding that the Open Internet Rules constituted impermissible common carrier regulation. In *Midwest Video II*, the Supreme Court held that the FCC had improperly attempted to impose common carrier regulation on cable companies.[43] The opinion undoubtedly focused on the nondiscrimination requirement there: "With its access rules, however, the Commission has transferred control of the content of access cable channels from cable operators to members of the public who wish to communicate by the cable medium. Effectively, the Commission has relegated cable systems, *pro tanto*, to common-carrier status."[44] However, the FCC's actual decision imposed not only nondiscrimination rules, but also service rules and rate regulation:

> The access rules plainly impose common-carrier obligations on cable operators. Under the rules, cable systems are required to hold out dedicated channels on a first-come, nondiscriminatory basis. Operators are prohibited from determining or influencing the content of access programming. And the rules delimit what operators may charge for access and use of equipment.[45]

Most importantly, the Court made clear it was proceeding on a case-by-case basis: "Whether less intrusive access regulation might fall within the Commission's jurisdiction . . . is not presently before the Court."[46]

In the *Open Internet Order*, the FCC actually said very little about why its rules did not constitute common carriage.[47] The agency focused on the consumer end users and said that "with respect to those customers, a broadband provider may make individualized decisions."[48] As such, it said, section 153(51) was "not relevant to the Commission's action here."[49] The court easily dismissed this rationale, noting that as in *Midwest Video II*, a nondiscrimination rule with respect to content and applications providers would forbid the carrier's choice of carriage.[50]

---

42. The FCC said as much. *2010 Open Internet Order*, *supra* note 1, at para. 5. *See also* C. Scott Hemphill, *Network Neutrality and the False Promise of Zero-Price Regulation*, 25 YALE J. ON REG. 135, 142 (2008).
43. *See* FCC v. Midwest Video Corp., 440 U.S. 689 (1979) ("Midwest Video II").
44. *Id.* at 700–01.
45. *Id.* at 701–02 (citations omitted).
46. *Id.* at 705 n.14.
47. *See generally 2010 Open Internet Order*, *supra* note 1.
48. *Id.* at para. 79.
49. *Id.*
50. Verizon v. FCC, 740 F.3d 623, 652–54 (D.C. Cir. 2014).

Because the FCC said so little about common carriage, and because courts have frequently noted the difficulty of applying the definition of common carriage, the FCC might, as a matter of administrative law, have been given the opportunity to further explain its rules; only if a statute is unambiguous does the agency lose interpretive primacy under the *Chevron* doctrine.[51] The D.C. Circuit did not make clear whether its holding came under step one or step two of *Chevron*. The presence of *Midwest Video II* allowed it to avoid using the *Chevron* analysis, given that Supreme Court interpretations of statutes made pre-*Chevron* are binding on agencies post-*Chevron*.[52] But if the D.C. Circuit had treated *Midwest Video II* as less controlling (as I have suggested it might have), then the agency both should have received *Chevron* deference and should now have an additional chance to explain itself.

Setting aside these seeming technicalities of administrative law and the debate over the breadth of *Midwest Video II*, the broader context of the Communications Act suggests that the FCC should have been able to define its rules as non-common carriage for two reasons. First, even the traditional regime of common carrier regulation under the 1934 Act had a very context-specific definition of nondiscrimination.[53] The statute outlawed only "*unreasonable discrimination*," and regulators frequently allowed common carriers to engage in value-of-service pricing to ensure universal service and the coverage of the carrier's capital costs.[54] In fact, regulators frequently *required* discrimination in order to provide universal service (or, perhaps more accurately, to provide cheap residential service).[55] As competition came to telecommunications markets, the FCC allowed contract-like tariffs to be developed, under which the carriers could define customer characteristics in such a way as to effectively discriminate among classes of customers. The technical requirement of nondiscrimination was met because

51. *See, e.g.*, NCTA v. Brand X Internet Servs., Inc., 545 U.S. 967, 982 (2005) ("A court's prior judicial construction of a statute trumps an agency construction otherwise entitled to *Chevron* deference only if the prior court decision holds that its construction follows from the unambiguous terms of the statute and thus leaves no room for agency discretion. This principle follows from *Chevron* itself. *Chevron* established a 'presumption that Congress, when it left ambiguity in a statute meant for implementation by an agency, understood that the ambiguity would be resolved, first and foremost, by the agency, and desired the agency (rather than the courts) to possess whatever degree of discretion the ambiguity allows.'") (quoting Smiley v. Citibank (South Dakota), N.A., 517 U.S. 735, 740–41 (1996)).

52. *See* United States v. Home Concrete & Supply, LLC, 132 S. Ct. 1836, 1843–44 (2012).

53. *See* James B. Speta, *Supervising Discrimination: Reflections of the Interstate Commerce Act in the Broadband Debate*, 95 MARQ. L. REV. 1195, 1200 (2012).

54. *Id.* at 1198 (emphasis added).

55. *Id.* at 1196.

each package was open to any customer that could meet the described characteristics.[56]

Second, and more fundamentally, the Telecommunications Act of 1996 gave the FCC the authority to eliminate the mandatory provisions of common carrier regulation, even as to those carriers that are unambiguously common carriers. The forbearance authority, now codified in section 10 of the Act,[57] means that Congress has given the agency the broad authority to determine the content of common carrier regulation. In fact, the Telecommunications Act of 1996 included this provision in part because the Supreme Court had held that tariffing was mandatory under the common carrier provision, notwithstanding that the FCC had found that competition meant that tariffing was no longer required.[58] To be sure, the FCC must make specific findings when granting forbearance,[59] but the authority to forbear further blurs the line between regulation that is common carriage and regulation that is not.

To be clear, I think all of the foregoing is relevant *only* after the court decides that the FCC has affirmative authority to regulate the Internet under section 706 and that the only effective limit on that authority is that the FCC may not impose common carrier regulation. I think, in fact, that the foregoing reveals that the court is and will be engaged in the same sort of ad hoc analysis that would inhere in recognizing FCC "ancillary" authority over the Internet—where the agency is given substantial authority subject only to a judgment by the court that particular actions are "too much." Either *Chevron* will be ignored as necessary, or the court will soon get out of the business of trying to limit the FCC's authority over Internet and information services providers. As I said above, all of this confirms to me that Congress cannot have intended to give the FCC authority to regulate the Internet at all—that is, so long as the FCC maintains the notion that Internet service is not telecommunications service.

V. WHY THE FCC MUST NOW BE AN ANTITRUSTER—AND WHY THAT'S NOT A BAD THING

Given that the FCC probably cannot attempt to define nondiscrimination rules as less-than-common-carriage, the FCC's best way forward to address the concerns that it cited as the basis for the Open Internet Order[60] is to adopt an antitrust-like framework. This framework would forbid Internet carrier actions that foreclosed competition. Because the focus would

56. *See* Competitive Telecomm. Ass'n v. FCC, 998 F.2d 1058, 1063–64 (D.C. Cir. 1993) (upholding these tariff packages).

57. 47 U.S.C. § 160 (2006).

58. MCI Telecomm. Corp. v. AT&T Co., 512 U.S. 218 (1994) (holding that the FCC did not have authority to waive tariffing requirements on common carriers).

59. 47 U.S.C. § 160(a) (2006).

60. *2010 Open Internet Order*, *supra* note 1.

be on competitive effects and not on discrimination itself, an antitrust-like framework would differ from a nondiscrimination rule while addressing the FCC's underlying concerns. Moreover, such rules would more clearly fall within the D.C. Circuit's holding that FCC rules must remove "barriers to investment."[61] The FCC is an appropriate institution for such rules, even though we already have two antitrust agencies (the DOJ and the FTC), because the FCC can use its expertise and agency standing to conduct appropriate inquiries and adopt appropriate (albeit hopefully limited) prophylactic rules.

The heart of the FCC's justification for the *Open Internet Rules* was the concern that ISPs could use discrimination to foreclose competition in two markets.[62] The Commission's principal focus, of course, was on ISP actions that reduced "openness" and competitive opportunities for "content, applications, services, and devices access over or connected to broadband access service ('edge' products and services)."[63] The Commission also emphasized (as was important to the court affirming the rules) that discrimination had the potential to stifle overall investment in Internet infrastructure and limit competition in telecommunications markets.[64]

Antitrust-like rules can address these concerns; indeed, foreclosure of competition is the touchstone of competition law.[65] Apart from the limited scope of the per se rules, antitrust requires the showing of anticompetitive effect: under the rule of reason used in section 1 cases, the first requirement is that the plaintiff show an anticompetitive effect.[66] Monopolization cases similarly require a demonstration that competition has been foreclosed.[67] Several examples from antitrust cases in utility industries show that antitrust can address these concerns. For example, the antitrust litigation against the integrated Bell System contended that AT&T used its control over local access monopolies to stifle entry in the related markets of long distance and customer premises equipment.[68] This parallels the FCC's allegations that ISPs might use their control over local distribution to reduce entry into

---

61. Verizon v. FCC, 740 F.3d 623, 661–62 (D.C. Cir. 2014).
62. *2010 Open Internet Order*, *supra* note 1, at paras. 5-6.
63. *Id.*
64. *Id.*
65. *See, e.g.*, Nat'l Soc. of Prof'l Eng'rs v. United States, 435 U.S. 679, 691 (1978) ("The true test of legality is whether the restraint imposed is such as merely regulates and perhaps thereby promotes competition or whether it is such as may suppress or even destroy competition." (citations omitted)).
66. *See, e.g.*, United States v. Brown Univ., 5 F.3d 658, 668 (3d Cir. 1993) ("The rule of reason requires the fact-finder to weigh[] all of the circumstances of a case in deciding whether a restrictive practice should be prohibited as imposing an unreasonable restraint on competition. The plaintiff bears an initial burden under the rule of reason of showing that the alleged combination or agreement produced adverse, anti-competitive effects within the relevant product and geographic markets." (internal quotations omitted)).
67. *See, e.g.*, United States v. Microsoft Corp., 253 F.3d 34, 58 (D.C. Cir. 2001) (discussing burden to show anticompetitive effect in monopolization cases).
68. United States v. AT&T Co., 552 F. Supp. 131, 135–36 (D.D.C. 1982).

content and applications markets. Similarly, the Bell System consent decree imposed equal access conditions—essentially nondiscrimination requirements—both in the hope of inducing entry into the long distance market and that such entry would eventually contribute to competition in local markets.[69] This last rationale parallels the FCC's expectation that ISP nondiscrimination would enhance demand for broadband and infrastructure investment. Similarly, in the famous *Otter Tail*[70] and *Terminal Bridge*[71] cases, antitrust was used to open bottlenecks to enable competition in the electricity and railroad markets. Today, antitrust doctrine might not embrace the results of those cases, given the Supreme Court's reluctance in *Trinko*[72] to embrace antitrust supervision of interconnection arrangements.[73] But even if antitrust litigation could not impose the *Otter Tail* and *Terminal Bridge* results, the competition-law reasoning of those cases remains.

Antitrust, however, is classically an ex post remedy, so any antitrust-like framework employed by the FCC will differ. The FCC expressed concern that the new enterprises that are key to the Internet's innovative ecosystem needed assurance that their entry would be unrestricted,[74] and a strong, ex ante nondiscrimination rule certainly provides more assurance in that regard. Many network neutrality advocates, in fact, thought the FCC's rules were not strong enough, given the focus on "unreasonable" discrimination.[75] But an antitrust approach is not necessarily inconsistent with rules, so long as the agency employs competition-law reasoning to determine their content. Moreover, as Phil Weiser has argued, case-by-case steps in this area can also help to preserve the flexibility needed as new network technologies and business models develop.[76]

The focus on foreclosure also seems more consistent with the D.C. Circuit's clear holding that "any regulations [adopted pursuant to section 706] must be designed to achieve a particular purpose: to 'encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans.'"[77] The FCC's theory was that the regulations would "remove barriers to infrastructure investment."[78] These are market-oriented measures, and antitrust law's focus on eliminating

---

69. *Id.* at 194–95.
70. Otter Tail Power Co. v. United States, 410 U.S. 366 (1973).
71. United States v. Terminal R.R. Ass'n, 224 U.S. 383 (1912).
72. Verizon Commc'ns, Inc. v. Law Offices of Curtis V. Trinko, 540 U.S. 398 (2004).
73. *See, e.g.*, Daniel F. Spulber & Christopher S. Yoo, *Mandating Access to Telecom and the Hidden Side of* Trinko, 107 COLUM. L. REV. 1822, 1825 (2007).
74. *See supra* notes 60-64 and accompanying text.
75. *See, e.g.*, Adam Candeub & Daniel McCartney, *Law and the Open Internet*, 64 FED. COMM. L.J. 493, 496–97 (2012) (arguing that the "normative principle of 'reasonable discrimination' as the legal standard for Internet regulation" is a "fatally narrow" regulatory approach).
76. Philip J. Weiser, *Towards a Next Generation Regulatory Strategy*, 35 LOY. U. CHI. L.J. 41 (2003).
77. *Verizon* v. FCC, 740 F.3d 623, 640 (D.C. Cir. 2014).
78. *2010 Open Internet Order*, *supra* note 1, at para. 117.

market-foreclosing activities directly furthers these goals. Indeed, although it opted for nondiscrimination rules, the FCC's rationale was almost entirely about competitive effects.[79]

Finally, the FCC is an appropriate focus for competition-law based rules, even though both the DOJ and the FTC are the principal antitrust enforcers. The DOJ only has the authority of an enforcement agency—apart from mergers—to attack market foreclosing activities after the damage has been done.[80] This role is important: strongly punishing foreclosures gives additional assurance and perhaps compensation to entrants that actions taken by market incumbents will be contained. But ex post remedies will only be part of the solution, especially as markets continue to be characterized by concentration. The FTC, for its part, does have rulemaking authority, but that authority has been cabined by statute and judicial decision.[81] The FTC's more general authority[82] does give comfort that it might not be as captured by industry-specific politics, but may also suggest less attention to broadband markets.

The FCC, by contrast, will be entitled to adopt ex ante rules and make "predictive judgments" concerning practices that might result in foreclosure.[83] The FCC might also experiment with the shape of competition law, for example, by borrowing the "abuse of dominance" notion from European Competition laws.[84] In that domain, a dominant firm has a "special responsibility . . . not to allow its conduct to impair genuine undistorted competition."[85] While the focus remains on competitive effects, E.U. law does not require as strict a showing of foreclosure as U.S. antitrust. The point is that the FCC, as an administrative agency pursuing its authority under

---

79. *See supra* notes 53-60 and accompanying text. The FCC also contended that Internet openness would further free speech and other noneconomic values, but the threat to those values generally arose from ISPs' possible anticompetitive actions. *2010 Open Internet Order*, *supra* note 1, at paras. 15-22.

80. *See generally* EINER ELHAUGE, UNITED STATES ANTITRUST LAW AND ECONOMICS 10–14 (2d ed. 2011) (providing an overview of the United States' antitrust laws and remedial structure).

81. *See id.* at 11, n.11 (noting that "[t]he only substantive rule related to competition that the FTC ever enacted was pursuant to its special authority to define price discrimination under 15 U.S.C. §13(a), and has since been rescinded.").

82. 15 U.S.C. § 45 (2012).

83. *See* Verizon v. FCC, 740 F.3d 623, 644 (D.C. Cir. 2014) ("When assessing the reasonableness of the Commission's conclusions, we must be careful not to simply 'substitute [our] judgment for that of the agency,' especially when the 'agency's predictive judgments about the likely economic effects of a rule' are at issue.") (quoting NTCA v. FCC, 563 F.3d 536, 541 (D.C. Cir. 2009) (quoting Motor Vehicle Mfrs. Ass'n v. State Farm Ins. Co., 463 U.S. 29, 43 (1983))); FCC v. Fox Television Stations, Inc., 556 U.S. 502, 521 (2009) ("the agency's predictive judgment . . . merits deference").

84. *See* Consolidated Version of the Treaty on the Functioning of the European Union art. 102, Oct. 26, 2012, 2012 O.J. (C 326) 47.

85. Pierre LaRouche, *Continental Drift in the Treatment of Dominant Firms: Article 102 TFEU in Contrast to Section 2 of the Sherman Act*, 45 LOY. U. CHI. L.J. (forthcoming 2014).

section 706,[86] will be free to consider competition in a broader context. The danger, of course, is that the FCC will not use competition law, but will revert to a public interest standard. Nothing in *Verizon*[87] prevents that. But, given the structure of the Open Internet Order,[88] one has hope that competition law is the most appealing approach.

In short, a competition-law approach to the underlying concerns of network neutrality is likely the FCC's best way forward. It is likely the only way open to the agency, given the D.C. Circuit's decision, and it will address many of the same concerns.

In fact, the FCC appears to be pointed in this direction to a degree, in its post-*Verizon* Notice of Proposed Rulemaking in the Open Internet Docket.[89] The Commission's revised proposal, however, introduces a requirement that any individualized agreements between carriers and edge providers be "commercially reasonable."[90] In its first formulation, the rule appears not to move beyond "openness" or "nondiscrimination," as the FCC says that "[i]t would prohibit as commercially unreasonable those broadband providers' practices that, based on the totality of the circumstances, threaten to harm Internet openness and all that it protects."[91] But the FCC has also said that the principle should be fleshed out by several factors, and the lead factor (proposed, to be sure, not yet adopted) is the "impact on present and future competition."[92]

The FCC believes that "this competition inquiry [would] extend beyond an application of antitrust principles to include, for example, the predicted impact on future competition."[93] This makes too much of the difference: as discussed above, an FCC analysis guided by competition law and economics could make predictive judgments. The FCC points at other factors that would be considered in a competition analysis: vertical integration[94] and effects on consumer choice.[95] To be sure, the FCC also identifies considerations that are not typical of antitrust analysis, such as free speech effects.[96] But the important point is that the FCC does seem more focused on finding a rule that is grounded in a more nuanced effects-based analysis than the "nondiscrimination" focus of the rejected rules—and this is more like antitrust analysis.

---

86. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, § 706 (codified at 47 U.S.C. §1302(a)).
87. 740 F.3d 623 (D.C. Cir. 2014).
88. *2010 Open Internet Order*, *supra* note 1.
89. Protecting & Promoting the Open Internet, *Notice of Proposed Rulemaking*, FCC 14-61, 29 FCC Rcd. 5561 (2014).
90. *Id.* at para. 116.
91. *Id.*
92. *Id.* at para. 124.
93. *Id.*
94. *Id.* at para. 126.
95. *Id.* at para. 129.
96. *Id.* at para. 131.

VI. CODA: WHERE I REJECT THIS WHOLE BUSINESS

At bottom, this entire business is a mess. That we find ourselves in this position as a matter of making rational telecommunications policy is entirely regrettable. To my mind, each of the government players bears some responsibility. As the Internet developed, the FCC was faced with a regime of fairly stringent common-carrier regulation, and as a policy matter it chose to classify Internet services under the information services construct to avoid those strict rules (even if the technical and statutory rationales for doing so were rather unconvincing).[97] The FCC believed that it would have some regulatory authority to address any serious problems that arose, and this belief was reasonable given the history of the Supreme Court's permitting the agency to have "ancillary jurisdiction" over communications services not directly addressed in the Act.[98]

Indeed, in some regards, *Verizon* feels like a replay of the Supreme Court's recognition of the FCC's ancillary jurisdiction as cable television came to be an important service.[99] There was a growing communications service, an important one in its own right, and one that was likely to affect the services at the core of the Communications Act (which Congress had clearly indicated should be regulated). And yet Congress was not updating the Act to account for cable television. So the Court found a way to give the FCC authority, subject to judicial review at the boundaries.[100] The same seems to have been the D.C. Circuit's intent in *Verizon*.[101] Forcing the FCC to treat the Internet as a common carrier service (by revisiting its classification decision) was foreclosed by the Supreme Court's own permissive approach to that question in *Brand X*.[102] Conversely, holding that the FCC had no authority to superintend this important communications market also seemed untenable. Section 706 was at hand. I do not think the players necessarily evaluated the case in these meta-terms; I do think this was an honest (if incorrect) exercise in statutory interpretation. But everyone understood the stakes.

If one were writing on a blank slate, granting the FCC authority to regulate the Internet but cabining that authority to something short of full-blown common-carrier regulation is not a bad place to be, especially if the result is that the FCC's regulation of the Internet is based strongly on competition law. But I doubt that the courts will be able to find a competition-law limit in the current Act, and I suspect the court's vigor in

97. *See* Verizon v. FCC, 740 F.3d 623, 631 (D.C. Cir. 2014) (summarizing the FCC's approach to classifying internet service providers as information services).

98. *See, e.g.*, United States v. Sw. Cable Co., 392 U.S. 157 (1968); United States v. Midwest Video Corp., 406 U.S. 649 (1972).

99. 740 F.3d 623.

100. *Midwest Video Corp.*, 406 U.S. at 649.

101. 740 F.3d 623.

102. NCTA v. Brand X Internet Servs., Inc., 545 U.S. 967 (2005).

challenging the agency's choice of regulatory tools will wane. Thus, I think it likely we end up with the FCC regulating the Internet "in the public interest, convenience, and necessity."[103]

Congress needs to act. The FCC's classification decision—and the courts' accommodation of it and of the FCC's regulatory authority over information services—have taken the legislature off the hook. One can worry about whether Congress can or will make rational communications policy, for Congress has a history of poorly-timed and politically-expedient interventions in the Act. But the rule of law envisions that Congress will act in making these very fundamental decisions.

Short of new congressional action, the Telecommunications Act of 1996—Congress's last major intervention—actually pointed to the better way forward. Verizon argued to the D.C. Circuit that regulating the Internet was a fairly significant policy decision, one which Congress would have made more clearly if it had intended to grant the FCC expansive authority.[104] As part of its response, the court said that Congress probably did intend the FCC to continue to superintend broadband carriers—but under the common carrier rules of Title II.[105] If that is right, then Congress gave the FCC the authority to regulate broadband, but in a different way than common carriage—through the forbearance authority.

In sum, *Verizon v. FCC* is decidedly a mixed bag. Out of its tortured statutory interpretation may come a reasonable policy approach—that the FCC has some authority to regulate Internet carriers, but it must do so under a competition-law approach. But it is another example of the courts empowering the FCC to be a regulator of "all communications" without clear direction from Congress.

103. NBC v. United States, 319 U.S. 190, 204 (1943).

104. *See* Verizon, 740 F.3d 623, 638–39 (D.C. Cir. 2014).

105. *Id.* at 638–39 ("Indeed, one might have thought, as the Commission originally concluded, that Congress clearly contemplated that the Commission would continue regulated Internet providers in the manner it had previously.").

35573-fcl_66-3 Sheet No. 53 Side B 10/21/2014 10:02:02

Net Neutrality 10 Years Later: A Still Unconvinced Commissioner

Deborah Taylor Tate*

TABLE OF CONTENTS

* Former Commissioner, Federal Communications Commission; Special Envoy to the International Telecommunication Union.

"Some men see things as they are and say, 'Why?'. . . I dream things that never were and say, 'Why not?'"

-Robert F. Kennedy, 1966[1]

I. INTRODUCTION

From the moment I first heard the words "net neutrality," I marveled at the absolute brilliance of coining such a phrase[2]—one that evokes such a democratic, neutral value proposition, yet threatens disastrous results for our economy. Interestingly, although net neutrality seemingly endorses the free and open nature of the Internet ecosystem,[3] its impact would actually be burdensome and onerous. In fact, this so-called net neutrality goes directly against most American consumers' values, such as competition, freedom of choice, and less government regulation.

At the end of the FCC's first and only investigation on the subject, which involved the slowing of BitTorrent traffic by Comcast,[4] I suggested that we change the dialogue to be much more concerned about whether the Internet is "safe and secure."[5] Those fears have, sadly, come to fruition, as illustrated by recent data breaches afflicting the National Security Agency,[6] the Internal Revenue Service,[7] and the Target Corporation,[8] among many

---

1. *CBS News: Edward M. Kennedy's Eulogy of Sen. Robert F. Kennedy* (CBS television broadcast Aug. 26, 2009), *available at* http://www.youtube.com/watch?v=dvo-7YrMoK0 (quoting GEORGE BERNARD SHAW, BACK TO METHUSELAH act 1, *in* GEORGE BERNARD SHAW, SELECTED PLAYS WITH PREFACES 7 (1949)).

2. The phrase was popularized by Tim Wu in *Network Neutrality, Broadband Discrimination*, 2 J. ON TELECOMM. & HIGH TECH. L. 141, 145 (2003) (defining a "neutral network" as one that does not "favor one application . . . over others").

3. *Id.*

4. *See* Formal Complaint of Free Press & Pub. Knowledge Against Comcast Corp., *Memorandum Opinion and Order*, FCC 08-183, 23 FCC Rcd. 13028, 13031, para. 8 (2008) [hereinafter *Comcast Order*] ("Following [Associated Press] tests, Comcast . . . admitted that it target[ed] peer-to-peer traffic for interference."), *vacated sub nom.* Comcast Corp. v. FCC, 600 F.3d 642, 644 (D.C. Cir. 2010); *see also* Peter Svensson, *Comcast Blocks Some Internet Traffic*, ASSOCIATED PRESS, Oct 19, 2007, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/10/19/AR2007101900842.html (describing Comcast's degradation of certain "uploads of complete files" transferred using the BitTorrent protocol).

5. Deborah Taylor Tate, *A Tangled Web: Moving from "Open and Free" to "Safe and Secure"*, (The Free State Found., Perspectives from FSF Scholars Vol. 5 No. 13, 2010), *available at* http://www.freestatefoundation.org/images/A_Tangled_Web.pdf.

6. David E. Sanger & Eric Schmitt, *Snowden Used Low-Cost Tool to Best N.S.A.*, N.Y. TIMES, Feb. 8, 2014, http://www.nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa.html?_r=0 (discussing Edward Snowden gaining access to many highly classified documents from the National Security Agency's networks).

7. *See*, *e.g.*, Brian Fung, *The IRS Mistakenly Exposed Thousands of Social Security Numbers*, NAT'L J., July 8, 2013, http://www.nationaljournal.com/tech/the-irs-mistakenly-exposed-thousands-of-social-security-numbers-20130708; Jeremy Kirk, *IRS Blamed in Massive South Carolina Data Breach*, PC WORLD (Nov. 21, 2012, 6:01 AM),

others. Nevertheless, net neutrality seems to still hold the attention of policymakers in Washington, D.C.[9]

The FCC in 2005 issued a seemingly benign "Internet policy statement"[10] under former Chairman Kevin Martin. Then, in 2010, the FCC plowed forward with a newly expanded list of "net neutrality principles."[11] Both forays into regulation of the Internet were held to exceed the legal authority of the FCC by the U.S. Court of Appeals for the D.C. Circuit.[12]

Many scholars have discussed the regulatory and legal history of the latest ruling by the D.C. Circuit in *Verizon v. FCC*.[13] As a former FCC Commissioner, I would be remiss to minimize the longstanding legal principle of *Chevron* deference that the judiciary affords federal expert agencies such as the FCC.[14] At the same time, I believe it is equally

---

http://www.pcworld.com/article/2015543/irs-blamed-in-massive-south-carolina-data-breach.html.

8. Jia Lynn Yang & Amrita Jayakumar, *Target Says up to 70 Million More Customers Were Hit by December Data Breach*, WASH. POST, Jan. 10, 2014, http://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html.

9. *See* Marguerite Reardon, *New Senate, House Bills Would Restore Net Neutrality*, CNET (Feb. 3, 2014, 3:52 PM), http://news.cnet.com/8301-13578_3-57618273-38/new-senate-house-bills-would-restore-net-neutrality/ (following the *Verizon* opinion, Senate and House Democrats introduced legislation to temporarily restore the FCC's net neutrality rules); *but see* Press Release, Sen. John Thune, Statement on Chairman Wheeler's Announcement (Feb. 19, 2014), *available at* http://www.commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=a7c131bc-afcb-4665-a3ff-d5aad5d28331&ContentType_id=77eb43da-aa94-497d-a73f-5c951ff72372&Group_id=4b968841-f3e8-49da-a529-7b18e32fd69d&MonthDisplay=2&YearDisplay=2014 (criticizing FCC's planned third attempt to impose net neutrality rules).

10. Appropriate Framework for Broadband Access to the Internet, *Policy Statement*, FCC 05-151, 20 FCC Rcd. 14986, 14987–88, para. 4 (2005) [hereinafter *Broadband Policy Statement*] (adopting four principles regarding broadband practices of Internet service providers).

11. Preserving the Open Internet, *Report and Order*, FCC 10-201, 25 FCC Rcd. 17905, 17906, para. 1 (2010) [hereinafter *2010 Open Internet Order*], *aff'd in part, vacated and remanded in part sub nom*. Verizon v. FCC, 740 F.3d 623, 628 (D.C. Cir. 2014).

12. *Verizon*, 740 F.3d at 628; Comcast Corp. v. FCC, 600 F.3d 642, 644 (D.C. Cir. 2010).

13. *See e.g.*, Christopher S. Yoo, *Some Initial Reflections on the D.C. Circuit's* Verizon v. FCC *Net Neutrality Decision*, (The Free State Found., Perspectives from FSF Scholars Vol. 9 No. 5, 2014), *available at* http://www.freestatefoundation.org/images/Some_Initial_-Reflections_on_the_D.C._Circuit_s_Verizon_v._FCC_Net_Neutrality_Decision_011614.pdf; Berin Szoka & Geoffrey Manne, *The Feds Lost on Net Neutrality, But Won Control of the Internet*, WIRED (Jan. 16, 2014, 6:30 AM), http://www.wired.com/opinion/2014/01/one-talking-comes-net-neutrality/.

14. Chevron U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 843–45 (1984) (holding that courts should afford considerable deference to a federal agency's construction of a statutory scheme it is entrusted to administer).

important that the FCC—indeed, any agency or arm of our government—acts completely within its legal authority.[15]

In *Verizon*, the FCC defended its net neutrality rules as a permissible exercise of the Commission's "ancillary jurisdiction," which supposedly emerged from a tapestry of other authorities within the broader Communications Act.[16] The FCC also relied on its authority under section 706 of the Telecommunications Act,[17] which tasks the FCC with encouraging the "deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans" by using, among other tools, "regulating methods that remove barriers to infrastructure investment."[18] Although the *Verizon* court recognized section 706 as a standalone fount of regulatory authority for the FCC,[19] the court nonetheless vacated the net neutrality rules' core provisions on the grounds that they impermissibly imposed common carriage status on fixed broadband providers.[20]

Despite its duo of losses, the FCC is now developing a *third* version of net neutrality rules.[21] I cannot imagine it manages to find the authority to promulgate similar rules this time around. As a skeptic of net neutrality regulation, I believe this outcome will be for the best.

II. TELECOM REGULATION AND THE ROLE OF GOVERNMENT

Whenever the government acts, interestingly, it is often in *reaction* to a real or perceived problem that, if left unattended or unregulated, might

---

15. *See* La. Pub. Serv. Comm'n v. FCC, 476 U.S. 355, 374 (1986) ("[A]n agency literally has *no power to act* . . . unless and until Congress confers power upon it.") (emphasis added); City of Arlington v. FCC, 133 S. Ct. 1863, 1880 (2013) (Roberts, C.J., dissenting) ("[B]efore a court may grant [*Chevron*] deference, it must on its own decide whether Congress—the branch vested with lawmaking authority under the Constitution—has in fact delegated to the agency lawmaking power over the ambiguity at issue.").

16. *See* Brief for Appellee-Respondents at 49, Verizon v. FCC, 740 F.3d 623, 628 (D.C. Cir. 2014) (No. 11–1355) (arguing the FCC may have "ancillary" authority over "communications matters even where Congress granted 'no express authority'" to the agency) (citing Comcast Corp. v. FCC, 600 F.3d 642, 646 (D.C. Cir. 2010)).

17. *Id.* at 68 ("[T]he Commission has sufficient authority to adopt [open Internet] rules under Section 706 alone, without relying on any other authority.").

18. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended at 47 U.S.C. § 1302 (2011)).

19. *Verizon*, 740 F.3d at 635 ("[S]ection 706 of the 1996 Telecommunications Act . . . furnishes the Commission with the requisite affirmative authority to adopt the [open Internet] regulations.").

20. *Id.* at 655 ("We have little hesitation in concluding that the anti-discrimination obligation imposed on fixed broadband providers has 'relegated [those providers], *pro tanto*, to common carrier status.'" (alteration in original) (citing FCC v. Midwest Video Corp., 440 U.S. 689, 700–01 (1979))).

21. New Docket Established to Address Open Internet Remand, *Public Notice*, GN Docket No. 14–28 (rel. Feb. 19, 2014), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DA-14-211A1.pdf.

cause harm.[22] New regulations often emerge after a specific incident, perhaps involving toxic substances, dangerous medications, tainted food, or misleading product advertisements.[23] Where perceived risk exists, government officials worry about political liability of they do nothing; to avert this prospect, they frequently resort to regulation.[24]

The resulting government is far larger than that envisioned by the founding fathers, who established the United States as a constitutionally limited government.[25] Today, the founders would probably struggle to recognize the nation's capital, which houses vast bureaucracies that span the city and sprawl into the surrounding states, and employs millions of federal workers and contractors.[26] As the Chief Justice of the United States recently observed, the "administrative state wields vast power and touches almost every aspect of daily life."[27] Indeed, the "overreach" of these federal agencies has never been more apparent, as demonstrated by the recent spate of congressional investigations of agencies acting outside their legal authority.[28]

One such agency is the Federal Communications Commission ("FCC"), which Congress tasked with overseeing a sector that accounts for

---

22. Technology policy researcher Adam Thierer explains this phenomenon as follows:

> [I]n a public policy setting, the precautionary principle holds that since every technology and technological advance could pose some theoretical danger or risk, public policies should prevent people from using innovations until their developers can prove that they won't cause any harms. In other words, the law should mandate "play it safe" as the default policy toward technological progress.

Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J.L. SCI. & TECH. 309, 352–53 (2013) (footnotes omitted).

23. *See, e.g.*, Henry I. Miller & Gregory Conko, *Precaution Without Principle*, 19 NATURE BIOTECHNOLOGY 302, 302 (2001).

24. *See* AARON WILDAVSKY, SEARCHING FOR SAFETY 38 (1988) (arguing that human progress is unattainable unless some nonzero level of risk is accepted).

25. City of Arlington v. FCC, 133 S. Ct. 1863, 1878 (2013) (Roberts, C.J., dissenting) ("The Framers could hardly have envisioned today's vast and varied federal bureaucracy and the authority administrative agencies now hold over our economic, social, and political activities.") (citing Free Enter. Fund v. Pub. Co. Accounting Oversight Bd., 130 S.Ct. 3138, 3156 (2010)); *id.* ("The administrative state with its reams of regulations would leave [the Framers] rubbing their eyes.") (citing Alden v. Maine, 527 U.S. 706, 807 (1999) (Souter, J., dissenting)).

26. *See* Haley Barbour & Ed Rogers, *The Lobbyists' Lament*, POLITICO MAG. (Dec. 17, 2013), http://www.politico.com/magazine/story/2013/12/the-lobbyists-lament-101252.html#.UyeaBJyP1I0 (discussing how "ever-expanding government and the perpetual nature of bureaucracy" have spurred rapid growth in "the lawyer and lobbyist business").

27. *City of Arlington*, 133 S. Ct. at 1878 (internal quotation marks omitted).

28. *Cf.* Molly K. Hooper, *Rep. Darrell Issa's Agenda in 2014: IRS, Benghazi and Fast and Furious*, THE HILL (Jan. 12, 2014, 6:00 AM), http://thehill.com/homenews/house/195169-issas-2014-agenda-irs-benghazi-and-fast-and-furious (chronicling the many congressional probes launched by Rep. Darrell Issa, the Chairman of the U.S. House Committee on Oversight and Government Reform from 2011 to 2014).

approximately one-sixth of nation's economy.[29] Created, in part, as a response to the sinking of the *RMS Titanic*,[30] to coordinate domestic and international radio communications, the FCC eventually took on a broad role in the telecommunications and media sectors.[31] Approving new gadgets—now devices—and negotiating with global players in the satellite sector further broadened the FCC's purview.[32] Yet, in my experience, most citizens have no idea how far the FCC's reach extends. Instead, many Americans think the Commission watches television all day in hopes of keeping "wardrobe malfunctions" and dirty words off the airwaves.

Whenever I speak to a civic club, I often explain the FCC's breadth by depicting a day in the life of an ordinary American. From the moment you turn on the news, open your garage door, use your remote control, switch radio stations, and listen to SiriusXM on your drive to work, you have probably spent more time with the FCC than your family. Much of the FCC's work aims to ensure all of these technologies operate so that consumers have the best possible experience, unimpeded by interference.[33]

To be sure, preconceptions of the FCC's activities are not uncommon. Some people relate to the FCC as the federal overseer of our nation's emergency response systems, such as 911.[34] Others are familiar with the FCC's placement of satellites for global telecommunications.[35]

---

29. *Oversight of the Federal Communications Commission: Hearing Before the Subcomm. on Commc'ns and Tech. of the H. Comm. on Energy and Commerce*, 113th Cong. 1 (2013) (statement of Jessica Rosenworcel, Comm'r, FCC), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-324628A1.pdf.

30. *See* John F. Duffy, *The FCC and the Patent System: Progressive Ideals, Jacksonian Realism, and the Technology of Regulation*, 71 U. COLO. L. REV. 1071, 1097 n.98 (2000).

31. *See* Kevin Ryan, *Communications Regulation—Ripe for Reform*, 17 COMMLAW CONSPECTUS 771, 780 (2009).

32. Kevin Werbach, *The Federal Computer Commission*, 84 N.C. L. REV. 1, 3–4 (2005) ("The FCC was regulating end-user computing devices plugged into the phone network for nearly a decade before the personal computer ('PC') was introduced. The FCC began regulating wireless equipment forty years before that, and it did not stop regulating end-user hardware when the PC came along.") (footnotes omitted); *see also* John H. Harwood II et al., *Competition in International Telecommunications Services*, 97 COLUM. L. REV. 874, 896 (1997) (discussing FCC regulation of international satellite services).

33. Comm'n Staff Clarifies FCC's Role Regarding Radio Interference Matters & Its Rules Governing Customer Antennas and Other Unlicensed Equip., *Public Notice*, DA 04-1844, 19 FCC Rcd. 11300, 11300 (2004) ("Section 302 [of the Communications Act] has granted the Commission express authority to adopt regulations 'governing the interference potential of devices which in their operation are capable of emitting radio frequency energy by radiation . . . in sufficient degree to cause harmful interference to radio communications.'") (citing 47 U.S.C. § 302a(a)(1) (2011)).

34. *See, e.g.*, U.S. Cellular Corp. v. FCC, 254 F.3d 78, 80 (D.C. Cir. 2001) (upholding FCC regulation promoting enhanced 911 services for wireless phones by requiring wireless carriers to bear implementation costs).

35. *See* Harwood II et al., *supra* note 32, at 896.

Some even relate to the Commission's role in national security.[36] And many parents whose children attend public schools have heard of the E-Rate program, which has connected almost every public school and library across this vast nation to the Internet.[37]

I am quite honored to have had the opportunity to serve the American people at the FCC, especially to the extent that our work saved lives and enhanced economic investment in the next dazzling innovation. However, in a few instances during my tenure, the FCC ventured outside of its legal bounds. The issue of net neutrality was—and is—one such instance.

III. A COMMISSIONER'S EXPERIENCE WITH NET NEUTRALITY

As one of the two original Commissioners to take issue with the entire premise of net neutrality,[38] I could never quite fathom that we were spending countless man-hours at the FCC on it, holding public "hearings" around the country and attempting to create regulations out of whole cloth—all basically because of one lone complaint regarding an ISP that had slowed down some consumers' Internet speeds.[39]

Similarly, in the second complaint—which involved the degradation, rather than the blocking, of Internet traffic[40]—broadband provider Comcast voluntarily resolved the issue and promised the FCC it would not happen again.[41] As my former colleague and FCC Commissioner Robert McDowell argued in his dissent from the *Open Internet Order*, "in the almost nine years since those fears were first sewn, net regulation lobbyists can point to fewer than a handful of cases of alleged misconduct, out of an

---

36. *See Homeland Security Policy Council Highlights FCC Actions Promoting Homeland Security*, FCC NEWS (Aug. 4, 2004), http://transition.fcc.gov/eb/News_Releases/DOC-250521A1.html.

37. Modernizing the E-Rate Program for Schools & Libraries, *Notice of Proposed Rulemaking*, FCC 13-100, 28 FCC Rcd. 11304, 11308, paras. 7–11 (2013), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-13-100A1_Rcd.pdf (proposing E-rate reform to better serve schools and libraries with broadband Internet connectivity).

38. Formal Complaint of Free Press & Pub. Knowledge Against Comcast Corp., *Memorandum Opinion and Order*, FCC 08-183, 23 FCC Rcd. 13028, 13085 (2008) (Tate, Comm'r, dissenting); *see also id.* at 13088 (McDowell, Comm'r, dissenting).

39. *See* Madison River Commc'ns, LLC, *Order*, DA 05-543, 20 FCC Rcd. 4295, paras. 3–5 (2005) (FCC Enforcement Bureau entered into consent decree with Madison River Communication, a broadband provider that blocked its customers' ability to use certain VoIP applications). Previously, a "blocking" complaint arose when Verizon Wireless began rejecting text messages sent to its mobile subscribers by a pro-choice organization. Dawn C. Nunziato, *The First Amendment Issue of Our Time*, 29 YALE L. & POL'Y REV. 1, 17 (2010) (citing Adam Liptak, *Verizon Blocks Messages of Abortion Rights Group*, N.Y. TIMES, (Sept. 27, 2007), http://www.nytimes.com/2007/09/27/us/27verizon.html). After receiving intense criticism for its actions, Verizon Wireless soon reversed its decision. *Id.*

40. *Comcast Order*, *supra* note 4, at para. 44.

41. *See* Julia Boorstin, *Comcast and BitTorrent: Enemies Become "Net-Neutral" Friends*, CNBC (Mar. 27, 2008, 3:21 PM), http://www.cnbc.com/id/23831261/.

infinite number of Internet communications. *All* of those cases were resolved in favor of consumers under *current* law."[42]

Indeed, while the FCC has found that ninety-four percent of households have access to fixed broadband Internet, meeting the Commission's speed benchmark,[43] the aforementioned formal complaints were the only two filed with the FCC alleging discrimination by a broadband provider. Juxtaposed against those two complaints are the 1.5 million indecency complaints[44]—many of which are still pending[45]—and many other consumer complaints clearly within the legal authority of the Commission, all of which remain unaddressed.

Informally designated "the Children's Commissioner"[46] during my time at the FCC, I was and continue to be outspoken on issues regarding illegal online activities, such as child pornography and online predatory behavior targeting minors. In addition, as a Music City native, I often speak about the harms caused by online infringement of intellectual property rights. These problems hurt individuals, especially children,[47] and the music industry.[48] However, despite my ardent desire to crack down on these illegal, unethical, and economically harmful online activities, I could not embrace FCC net neutrality regulation, as it clearly exceeded the Commission's legal authority.

My first question to attorneys and government relations officials who frequented my office on the topic was usually "what is your definition of

---

42. Preserving the Open Internet Broadband Indus. Practices, *Report and Order*, FCC 10-201, 25 FCC Rcd. 17905, 18055 (2010) [hereinafter *McDowell Dissent*] (dissenting statement of Comm'r Robert M. McDowell), *aff'd in part, vacated and remanded in part sub nom*. Verizon v. FCC, 740 F.3d 623, 628 (D.C. Cir. 2014).

43. Inquiry Concerning the Deployment of Advanced Telecomm. Capability to All Americans in a Reasonable & Timely Fashion, *Eighth Broadband Progress Report*, FCC 12-90, 27 FCC Rcd. 10342, 10370, para. 46 (2012), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-12-90A1_Rcd.pdf.

44. John Eggerton, *Liberman Settles Indecency Complaint with FCC*, MULTICHANNEL NEWS (Nov. 15, 2013, 11:34 AM), http://www.multichannel.com/policy/liberman-settles-indecency-complaint-fcc/146706.

45. FCC Reduces Backlog of Broad. Indecency Complaints by 70%, *Public Notice*, DA 13-581, 28 FCC Rcd. 4082 (2013) ("Since September 2012, the Bureau has reduced the backlog [of indecency complaints] by 70% thus far, more than one million complaints . . . .").

46. *Biography of Deborah Taylor Tate*, FCC (Jan. 5, 2009), http://transition.fcc.gov/commissioners/previous/tate/biography.html (noting that Commissioner Tate is "[o]ften referred to as the 'Children's Commissioner'").

47. *Cf.* United States v. Williams, 553 U.S. 285, 307 (2008) ("Child pornography harms and debases the most defenseless of our citizens. Both the State and Federal Governments have sought to suppress it for many years, only to find it proliferating through the new medium of the Internet.").

48. *See* MGM Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 961 (2005) (Breyer, J., concurring) ("'No one disputes that 'reward to the author or artist serves to induce release to the public of the products of his creative genius.' And deliberate unlawful copying is no less an unlawful taking of property than garden-variety theft.") (citing United States v. Paramount Pictures, Inc., 334 U.S. 131, 158 (1948)).

net neutrality?" I rarely received the same response. Indeed, net neutrality has been said to be "the most discussed, least understood concept in the world of internet policy."[49] Under the FCC's conception of net neutrality, it requires broadband providers to allow their subscribers to (1) "access the lawful Internet content of their choice," (2) "run applications and use services of their choice, subject to the needs of law enforcement," and (3) "connect their choice of legal devices that do not harm the network."[50]

My second question was "what is the basis of the FCC's legal authority to establish net neutrality regulations?" This question is important for advocates, attorneys, and policymakers, for the government should never reach the definitional question if it has no clear legal authority over the issue at the outset.[51] And, indeed, that is what the D.C. Circuit recently opined—*for the second time*.[52] Simply put, the court held, the FCC lacks the authority to impose common carriage regulation on broadband providers that are classified as information services under Title I of the Communications Act.[53]

IV. NET NEUTRALITY IS NOT A SILVER BULLET

In my work with women's and minority organizations, I am often asked how a particular proposal, law, or regulation may impact those groups specifically. I applaud the FCC for many of its public hearings and ongoing initiatives, especially as they relate to the low percentage of media ownership by women and minorities.[54] The FCC has a long-established and very active Diversity Committee, which advises the Commission on a variety of issues across all sectors and routinely holds public hearings to examine the impact of or need for a particular rule or regulation which may enhance diversity.[55]

When I am asked about net neutrality, my response is always the same: an Internet with light regulation and less oversight or intrusion by the government is better for *all* of us—including new application builders on

49. Alexander Reicher, *Redefining Net Neutrality After* Comcast v. FCC, 26 BERKELEY TECH. L.J. 733, 733 (2011).

50. *Broadband Policy Statement*, *supra* note 10, at 14987–88, para. 4.

51. *See* La. Pub. Serv. Comm'n v. FCC, 476 U.S. 355, 374 (1986).

52. Verizon v. FCC, 740 F.3d 623, 628 (D.C. Cir. 2014).

53. *Id.* at 630 (noting that the Communications Act "subjects telecommunications carriers, but not information-service providers, to Title II common carrier regulation") (citing 47 U.S.C. § 153(53) (2011); NCTA v. Brand X Internet Servs., 545 U.S. 967, 975–76 (2005)).

54. *See, e.g.*, 2010 Quadrennial Regulatory Review—Review of the Commissions Broad. Ownership Rules, *Notice of Proposed Rulemaking*, FCC 11–186, 26 FCC Rcd. 17489 (2011).

55. *See* Statement of FCC Comm'r Mignon L. Clyburn on the Re-Chartering of the Advisory Comm. on Diversity for Commc'ns in the Digital Age (Mar. 11, 2013), *available at* http://www.fcc.gov/document/clyburn-statement-re-chartering-diversity-advisory-committee.

the edge of the ecosystem, women running small businesses from home, and our youngest citizens taking Advanced Placement courses or learning a foreign language that was never before possible in their rural hometown. Allowing infrastructure providers and ISPs to invest in and expand high speed Internet throughout our country helps us all.[56] The Internet's low entry costs and lack of barriers to create, upload, start up, and sell goods and services are especially beneficial to women and minorities with less access to capital than established firms. The underlying reason for the lack of women and minority ownership of radio and television entities is directly related to the high cost of entry and the difficulty of access to large capital or debt. However, since the advent of the Internet, those barriers have decreased greatly; both women and minorities are now unleashing their creativity, developing innovative services, and even producing independent films and videos at record numbers.

Net neutrality proponents need only look to the FCC's media ownership rules to see how a similar scheme might affect women and minorities. The Minority Media and Telecommunications Council ("MMTC"), which has long been an outspoken advocate for minority and women's ownership in the media space, undertook a study regarding the potential impact of similar Internet regulation on their constituencies.[57] The report, entitled *Refocusing Broadband Policy: The New Opportunity Agenda for People of Color*, was co-authored by David Honig, president of MMTC, and Dr. Nicol Turner-Lee, vice president and chief research and policy officer at MMTC.[58] The report explored current trends in minority broadband adoption and assessed the impact of Internet regulation, finding that it is actually diverting attention from important strategies aimed at closing the digital divide.[59]

In a historical review of broadband policies initiated under the leadership of former FCC Chairman William Kennard, Honig and Lee suggest that "innovation has thrived within a minimalist regulatory

---

56. FCC, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 19 (Mar. 16, 2010) [hereinafter *National Broadband Plan*], *available at* http://www.broadband.gov/download-plan/ ("Broadband is a platform to create today's high-performance America . . . . Due in large part to private investment and market-driven innovation, broadband in America has improved considerably in the last decade. More Americans are online at faster speeds than ever before.").,

57. *See generally* David Honig & Nicol Turner-Lee, MINORITY MEDIA & TELECOMM. COUNCIL, REFOCUSING BROADBAND POLICY: THE NEW OPPORTUNITY AGENDA FOR PEOPLE OF COLOR (2013), *available at* http://mmtconline.org/wp-content/uploads/2013/11/Refocusing-Broadband-Policy-112113.pdf.

58. *Id.*

59. *Id.* According to the report, African Americans and Hispanics are still under-adopting broadband, despite slight increases in minority broadband adoption over the last few years. *Id.* at 7. While the use of mobile broadband has increased, especially through smartphones, limited digital literacy skills and the lack of relevance of the Internet to their daily lives have stalled broadband use for African Americans and Hispanics even though broadband is more readily available at lower price points. *Id.* at 8.

framework facilitating technological advances and opportunities for consumers and entrepreneurs of color."[60] Recognizing, however, that adoption gaps between African Americans, Hispanics, and Whites still persist, the authors cautioned against "stringent regulation until more of these communities are enabled by the platforms, products, and services that broadband provides."[61] Honig further emphasized that "more regulation is not always the silver bullet for advancing digital inclusion."[62]

One need only look at the dismal results from past over regulation in the media ownership space to pause before allowing the same to happen to women and minorities embarking on Internet-based businesses.

V. THE DEMOCRATIZATION OF COMMERCE

Beyond the opportunities in the media marketplace, women and minorities have also thrived in the e-commerce marketplace. Like mass media, entering this market is affordable and does not require a physical presence—bricks and mortar have been replaced by colorful graphics and product photos.[63] Indeed, retail e-commerce weathered the recent and extended recession quite well, albeit with slower growth than prior to the financial crisis, falling from a high of forty-two percent year over year growth to about eighteen percent growth during the recession.[64] Globally, e-commerce topped $1 trillion in 2012.[65] All of this is good news for U.S. producers and consumers.

But none of this would have been possible if broadband subscribers were unable to search for and purchase products easily online. Nor would this explosion have occurred if there were providers who were blocking traffic, slowing it down, or otherwise making entrepreneurial entry difficult or expensive. Obviously these potential "what ifs" that net neutrality proponents continue to suggest have not and are not occurring, given that e-commerce is estimated to have a 10 percent global penetration by 2016[66]

---

60. MMTC REPORT CALLS FOR TELECOM POLICYMAKERS TO MAKE BROADBAND ADOPTION THEIR TOP PRIORITY, BROADBAND & SOCIAL JUSTICE (Nov. 21, 2013), *available at* http://broadbandandsocialjustice.org/2013/11/mmtc-report-calls-for-telecom-policymakers-to-make-broadband-adoption-their-top-priority/.

61. *Id.*

62. *Id.*

63. *See e.g.*, Chris G. Christopher, *The Economic Impact of E-Commerce*, SUPPLY CHAIN QUARTERLY, Quarter 2 2011), *available at* http://www.supplychainquarterly.com/print/scq201102monetarymatters/.

64. *Id.*

65. Lauren Indvik, *Study: Global Ecommerce to Hit $1.2 Trillion This Year, Led by Asia*, MASHABLE (June 27, 2013), http://mashable.com/2013/06/27/ecommerce-study-china-asia/.

66. *See e.g.*, SCOTT DEVITT ET AL., MORGAN STANLEY, ECOMMERCE DISRUPTION: A GLOBAL THEME TRANSFORMING TRADITIONAL RETAIL (2013), *available at* http://www.rundlemall.com/bm.doc/ecommerce_bp0106131.pdf.

and Facebook would be the third largest nation in the world based on population.[67]

Regulators should be leveling the playing field and opening the gates to competition at every level.[68] In the former world of the old-fashioned telephone service, when there was one local provider in each market, telephone companies—like other utilities—were highly regulated at both the state and federal levels. This regulation encompassed everything from price to the privacy of customer information to 911 emergency services to the "Chinese wall" required between each phone company and the yellow pages.[69] After the break-up of AT&T into Regional Bell Operating Companies, or "baby bells," the ensuing competition led to a world of choices for voice service on any type of handheld device—which could even be purchased at the local supermarket.[70]

Even when the phone companies were highly regulated, they competed through marketing and advertising products and pricing.[71] "Special access" provided a dedicated, secure line for crucial communications to corporations with hundreds of geographically dispersed retail outlets and hospitals and doctors to share patient information.[72] Thus, even in a highly regulated market, phone companies could negotiate prices for special access and creatively market tools to entice and keep customers.[73] Yet, eighteen years after the passage of the deregulatory 1996 Telecommunications Act,[74] net neutrality proponents advocate turning the clock backwards and re-regulating marketing and pricing of Internet services. They propose a "free and open" Internet that denies broadband providers the freedom to negotiate with content companies to finance the networks of tomorrow.

---

67. Rob Williams, *Revealed: The Third Largest 'Country' in the World - Facebook Hits One Billion Users*, THE INDEPENDENT, Oct. 4, 2012, http://www.independent.co.uk/life-style/gadgets-and-tech/news/revealed-the-third-largest-country-in-the-world--facebook-hits-one-billion-users-8197597.html.

68. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.) (describing the goal of the Act as to "promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies").

69. *See, e.g.*, James Crowe, *Regulation and Free Markets: How to Regulate the Telecommunications Industry in the New Economy*, 2 J. TELECOMM. & HIGH TECH. L. 429 (2003).

70. *See* Michael T. Burr, *The Transformation Myth*, FORT., June 2011, at 4–5, *available at* http://www.fortnightly.com/fortnightly/2011/06/transformation-myth.

71. *Id.*

72. *See* Access Charge Reform, *Fifth Report and Order and Further Notice of Proposed Rulemaking*, FCC 99–206, 14 FCC Rcd. 14221, para. 9 (1999).

73. *Id.* at para. 4.

74. Pub. L. No. 104–104, § 301, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.).

It is widely accepted that broadband penetration and access for all of our citizens is absolutely critical.[75] Nowadays, applying for a job, applying to college, and even making a health care appointment is often done online. Over seventy-five percent of teachers use the Internet for homework.[76] Parents can check on their child's school attendance, test scores, events, and other pertinent educational data—often in real time.[77] Many citizens also seek health care information and even sign up for health insurance online.[78]

All of this requires Internet access—and, in many cases, faster broadband speeds than many Americans currently have. As many groups sought to help with broadband adoption, they found that "cost" was often a reason for lack of uptake even when the service was available to their home.[79] Again, we see that lower cost alternatives—such as a "two-sided market" wherein one or more content companies help broadband providers shoulder the burden of the "last mile"—would be helpful in reaching those last Americans who remain offline.[80]

---

75. *See* LENNARD G. KRUGER & ANGELE A. GILROY, CONG. RESEARCH SERV., RL30719, BROADBAND INTERNET ACCESS AND THE DIGITAL DIVIDE: FEDERAL ASSISTANCE PROGRAMS 12 (2013), *available at* https://www.fas.org/sgp/crs/misc/RL30719.pdf; *but see* Justin Hurwitz, *Five Faulty Premises in Telecom Debates*, (The Free State Found., Perspectives from FSF Scholars Vol. No. 3, 2014), *available at* http://www.freestatefoundation.org/images/Five_Faulty_Premises_in_Telecom_Policy_Debates_010814.pdf.

76. Tom Wheeler, Chairman, FCC, Prepared Remarks for the National Digital Learning Day at the Library of Congress 2-3 (Feb. 5, 2014), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db0205/DOC-325447A1.pdf.

77. *Cf.* John Eggerton, *Survey: Parents, Teachers Believe Broadband Boosts Performance*, BROAD. & CABLE (Sept. 10, 2012, 3:00 PM), http://www.broadcastingcable.com/news/washington/survey-parents-teachers-believe-broadband-boosts-performance/60580.

78. *See, e.g.*, News Release, FCC, *FCC Creates Healthcare Connect Fund to Expand Access to Robust Broadband Healthcare Networks* (Dec. 12, 2012), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-317912A1.pdf.

79. JOHN B. HORRIGAN, PEW INTERNET & AM. LIFE PROJECT, HOME BROADBAND ADOPTION 2009 7 (2009), *available at* http://www.pewinternet.org/files/old-media//Files/Reports/2009/Home-Broadband-Adoption-2009.pdf (noting that one third of "dial-up users cite price as a barrier" to subscribing to home broadband).

80. *See* Christopher S. Yoo, *Network Neutrality and the Economies of Congestion* , 94 GEO. L.J. 1847, 1903 (2006) ("[T]here is no reason to expect that network owners will only attempt to engage in price discriminate vis-à-vis end users. In a two-sided market, network owners are just as likely to try to price discriminate with respect to content and applications providers as well."); *but see* Edward Wyatt, *New F.C.C. Chief Promises He Will Protect Competition*, N.Y. TIMES, Dec. 3, 2013, *available at* http://www.nytimes.com/2013/12/03/technology/tom-wheeler-of-fcc-vows-to-champion-competitiveness.html?_r=0 (FCC Chairman Tom Wheeler "indicated that he would not oppose some type of usage-based pricing, with Internet service providers charging so-called data hogs different amounts for service depending on how much data they receive and transmit").

VI. NET NEUTRALITY'S TENTH ANNIVERSARY

The FCC has signaled it will continue to pursue net neutrality regulations—albeit not in court, for now.[81] I am certain that the FCC's decision not to challenge the D.C. Circuit's decision involved the risk of hearing for the *third* time—and from the U.S. Supreme Court—that its net neutrality rules are illegal.[82] Specifically, as FCC Chairman Tom Wheeler stated:

> The D.C. Circuit ruled that the FCC has the legal authority to issue enforceable rules of the road to preserve Internet freedom and openness . . . I intend to accept that invitation by proposing rules that will meet the court's test for preventing improper blocking of and discrimination among Internet traffic, ensuring genuine transparency in how Internet service providers manage traffic, and enhancing competition.[83]

On February 19, 2014, Chairman Wheeler launched a public inquiry aimed at establishing an "updated" set of rules for an "open Internet."[84] This marks the tenth anniversary of the FCC's original inquiry as to whether and how to regulate the Internet. At the same time, the White House issued a blog post mentioning President Barack Obama's support for net neutrality since his days in the U.S. Senate.[85] It noted specifically that his campaign was "empowered by an open Internet" that allowed millions to interact in an "unprecedented fashion."[86] We indeed have seen a new interest and rise in the civic engagement of our citizens, whether it involves a specific election or an issue or a cause. The Internet has connected people who care about a subject matter no matter where they are physically located. This connectivity is providing opportunities for us to discuss important issues of the day by returning to the "town square" online or becoming "the town crier" like Paul Revere. And who could forget the text messages and photos we all witnessed during the Arab Spring and other

---

81. Jon Brodkin, *FCC Won't Appeal Verizon Ruling, Will Regulate 'Net on "Case-by-Case Basis"*, ARS TECHNICA (Feb. 19, 2014, 12:44 PM), http://arstechnica.com/tech-policy/2014/02/fcc-wont-appeal-verizon-ruling-will-regulate-net-on-case-by-case-basis/.

82. *Id.*

83. Statement by FCC Chairman Tom Wheeler on the FCC's Open Internet Rules (Feb. 19, 2014), *available at* http://www.fcc.gov/document/statement-fcc-chairman-tom-wheeler-fccs-open-internet-rules.

84. New Docket Established to Address Open Internet Remand, *Public Notice*, GN Docket No. 14–28 (Rel. Feb. 19, 2014), *available at* http://www.fcc.gov/document/new-docket-established-address-open-internet-remand.

85. Gene Sperling & Todd Park, *We the People Response: Reaffirming the White House's Commitment to Net Neutrality*, THE WHITE HOUSE BLOG (Feb. 18, 2014, 2:06 PM), http://www.whitehouse.gov/blog/2014/02/17/we-people-response-reaffirming-white-houses-commitment-net-neutrality.

86. *Id.*

democratic movements worldwide.[87] As the White House recognized, "[i]ndeed, an open Internet is an engine for freedom around the world."[88] Later, the White House's blog post references the Internet as a hotbed for low cost entry and innovation, "building companies, creating jobs, improving vital services and fostering even more innovation along the way."[89] Crucially, however, all these incredible successes for individuals, companies, civic engagement, and the spread of our democratic ideals, occurred under the *present regime*—one in which there is less government regulation, not more.[90]

VII. CONCLUSION

The world's insatiable appetite for more content, faster speeds, and wearable devices is almost unfathomable, especially given that much of this extraordinary innovation occurred in just the past few years. It is predicted that the growth will require more and more bandwidth—and, with it, better technologies to accommodate that growth.[91] Advanced network management to enable the best possible consumer experience will rule the marketplace and consumers will continue to adopt and change with each new service, device, or application.[92] Computer-to-computer communication will impact our homes, our vehicles, our health, and our everyday lives.

But this all depends on the ability of companies, investors, management teams, and brilliant young engineers to move nimbly and quickly to take advantage of each new trend by consumers. Nearly two *trillion* dollars sit on the sidelines, held by multinational companies that are waiting to see whether the United States government regulates the Internet, among other things.[93] Meanwhile, regulatory uncertainty persists, even as other nations evolve—perhaps into global high-tech leaders.

---

87. *The Arab Spring's Online Backlash*, THE ECONOMIST, (Mar. 29, 2012, 9:27 PM), http://www.economist.com/blogs/newsbook/2012/03/internet-middle-east (discussing Internet's role in facilitating dissent in the Arab Spring).

88. Sperling & Park, *supra* note 85.

89. *Id.*

90. *See, e.g.*, CLYDE WAYNE CREWS JR., COMPETITIVE ENTER. INST., TEN THOUSAND COMMANDMENTS: AN ANNUAL SNAPSHOT OF THE FEDERAL REGULATORY STATE 41–43 (2013), *available at* http://cei.org/sites/default/files/Wayne%20Crews%20-%2010,000%20Commandments%202013.pdf (discussing the rapid growth of federal telecom regulation and its consequences).

91. *See* Bret Swanson, Op-Ed., *The Coming Exaflood*, WALL ST. J. (Jan. 20, 2007, 12:01 AM), *available at* http://online.wsj.com/news/articles/SB116925820512582318.

92. *See* Yoo, *supra* note 80, at 1849, 1884.

93. Large, multinational U.S. companies have accumulated nearly $2 trillion in cash and equivalent assets abroad as of the end of 2013. Richard Rubin, *Cash Abroad Rises $206 Billion as Apple to IBM Avoid Tax*, BLOOMBERG (Mar. 12, 2014, 2:47 PM), http://www.bloomberg.com/news/2014-03-12/cash-abroad-rises-206-billion-as-apple-to-ibm-avoid-tax.html.

As a nation, we face many challenges: ensuring that all children have access to the Internet at speeds and with devices in order to reach their full potential; conducting an unprecedented spectrum auction to ensure the viability and strength of wireless networks; and implementing technology and strategies to make the Internet as safe and secure as possible for every user and to thwart cybersecurity attacks that occur daily throughout the ecosystem. We want to ensure democracy thrives here and around the world and that the Internet remains an open medium for civic engagement everywhere.

However, none of these goals involve or rely upon new net neutrality rules being adopted and enforced by the FCC. Parents, teachers, consumers, entrepreneurs, and investors will choose the winners and losers through online chat, voting with their wallets, and adopting new technologies that have yet to be invented. The best way the FCC can influence the debate is by ending it. If and when a real problem emerges, shine a light on it and look out for the consumer backlash against any instigator or wrongdoer.[94] Odds are the wrongdoers will not need an FCC monetary penalty, as they will be out of business altogether.[95]

All this incredible success was enabled through the *current* framework of a light-touch regulatory process. Any further net neutrality regulation is not only unnecessary, but might also actually derail the Internet's next great expansion. We must refrain from regulation taking aim at shadows in order to continue the very real progress and promise of unleashing the very best America has to offer to our consumers, our creators, our children and indeed, the world.[96]

---

94. As Randall Rothenberg put it: "The ability of aggrieved Americans to band together and make noise that is either (depending on your point of view) productive or destructive is a reality that organizations as diverse as the Democratic Party and Dell Computer have learned the hard way." "Listenomics," Advertising Age's critic-at-large Bob Garfield calls this new principle: "The herd will be heard." Randall Rothenberg, Op-Ed., *Facebook's Flop*, WALL ST. J. (Dec. 14, 2007, 12:01 AM), http://online.wsj.com/news/articles/SB119760316554728877.

95. *Cf.* ROBERT ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1994) (chronicling how free people govern themselves through informal rules that emerge organically from the bottom-up).

96. *See* John Allison & Ron Johnson, Op-Ed., *Regulations Stifle Economic Growth*, POLITICO (Oct. 4, 2011, 9:47 PM), http://www.politico.com/news/stories/1011/65117.html ("Regulatory bureaucracies also stifle innovation, which is the key to economic growth but requires defying convention, experimenting, making mistakes and correcting them.").

No Dialtone: Second Thoughts on the PSTN's Demise

Gerald R. Faulhaber*

TABLE OF CONTENTS

* Professor Emeritus, Wharton School, University of Pennsylvania (and visiting professor, University of Pennsylvania Law School). This paper draws on the author's previous work: Gerald R. Faulhaber, *Should the FCC Regulate Internet Interconnection?* PENN PROGRAM ON REG. REGBLOG (June 9, 2014), and Gerald R. Faulhaber & David J. Farber, *The Open Internet: A Customer-Centric Framework*, 4 INT'L J. OF COMM. 302 (2010). The author is solely responsible for any errors or omissions.

I. INTRODUCTION

With only mild hyperbole, Werbach states that "[t]he transition from the PSTN to a broadband network of networks is the most important communications policy event in at least half a century."[1] For years, Internet aficionados have proclaimed the imminent death of the Public Switched Telephone Network ("PSTN"), asserting that telephony is just another app. Finally, that day has arrived. People are leaving the PSTN in droves. As Werbach notes, the fraction of U.S. households with a wireline telephone has fallen from 93% in 2003 to 25% in 2013.[2]

In fact, telephone companies are not standing idly by while their PSTN base erodes. The fixed cost of the PSTN is huge, as Werbach points out;[3] as the revenue base erodes, maintaining the PSTN becomes untenable. Telephone companies are actively seeking to sunset the PSTN in two ways: first, by petitioning the FCC to permit them to conduct local trials to transition customers from PSTN to wireless or VoIP; and, second, by announcing plans to transition most customers by 2015.[4]

II. THE PSTN TRANSITION HAS ALREADY STARTED

Werbach is clear that this transition is a good thing. He states:

> The time has come to address the situation squarely. The lesson from prior structural transitions in communications such as digital television, the AT&T divestiture, and the opening of local telephone competition is that, with good planning and the right policy decisions, such shifts can proceed smoothly and open new vistas for competition and innovation.[5]

This is the first indication that Werbach is far off-base. If these are examples of good planning and the right policy decisions, we are all in big trouble.

First, the transition to digital television broadcasting was mandated by the Telecommunications Act of 1996, to be achieved by 2006.[6] Nevertheless, the transition was pushed back several times, and finally

---

1. Kevin Werbach, *No Dialtone: The End of the Public Switched Telephone Network*, 66 FED COMM. L.J. 203, 205 (2014), *available at* http://www.fclj.org/wp-content/uploads/2014/06/66.2.1_Werbach-Final.pdf.

2. *See id.* at 211 n.27. This number refers only to traditional PSTN wireline telephones. VoIP telephony provided over cable is technically wireline as well, but not PSTN.

3. *Id.* at 225 (citing BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES 12–14 (2012)).

4. Werbach, *supra* note 1, at 213–15.

5. *Id.* at 205.

6. *See id.* at 259–60.

implemented in June 2009. While the actual transition went relatively smoothly, thirteen years seems a rather long time for a transition substantially less stressful than the demise of the PSTN.

Second, although the AT&T divestiture broke up the country's largest monopoly three decades ago, after many years of industry evolution and a great deal of cost, we now have two dominant suppliers of telephony that use the PSTN. [7] It is hard to see how this is a major advance, at least as regards telephony.

Third, the introduction of local telephone competition via the Telecommunications Act of 1996 involved over five years of FCC rulings to make competitive local exchange carriers ("CLECs") viable. In this case, competition involved the mandated wholesale of incumbents' local PSTN distribution facilities to new entrants.[8] Today, virtually all PSTN competition is either wireless or VoIP; CLECs have all but disappeared.[9] Again, it's difficult to understand why this was at all useful.

"[G]ood planning and the right policy decisions?" Let's hope we can avoid similar disasters to the ones these exemplars have visited upon us for the PSTN transition.

While Werbach supports the PSTN transition, he is critical of some of what the telephone companies have done so far. He notes that Verizon has offered Voice Link service, a wireless platform, as a substitute for wireline where problems have occurred.[10] He goes on to state that Voice Link is by no means a perfect substitute for PSTN local service.[11] But most of the features he claims Voice Link lacks are either available or insignificant. For example, he claims that one cannot use Voice Link to transmit a fax, as one can do using a wireline phone.[12] But there are numerous wireless fax apps available on smartphone app stores.[13] He also notes that a cell phone cannot be used as a dial-up modem;[14] this is true, but why would anyone want this service? With a smartphone tethered to a computer, a user can access the Internet directly (and at higher speeds than a dial-up modem).[15] Again, he mentions that a wireless phone (and perhaps VoIP) can't be used with current burglar alarms;[16] however, much better

---

7. *Id.* at 225 n.121.
8. *See* Thomas W. Hazlett, *Rivalrous Telecommunications Networks with and Without Mandatory Sharing*, 58 FED. COMM. L.J. 477, 491 (2006).
9. *Id.* at 497–500.
10. Werbach, *supra* note 1, at 216.
11. *Id.*
12. *Id.*
13. *See, e.g.*, FaxFile, eFax, PC-FAX, Mobile Fax Free, and iFax, GOOGLE PLAY, *available at* https://play.google.com/store/search?q=fax (containing such descriptions as "Mobile Fax turns your phone into a fax machine!").
14. Werbach, *supra* note 1, at 216.
15. *See, e.g.*, FoxFi, GOOGLE PLAY, *available at* https://play.google.com/store/apps/details?id=com.foxfi; *see also* FCC, *Verizon Wireless to Pay $1.25 Million to Settle Investigation*, Press Release (July 31, 2012), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-315501A1.pdf.
16. *See* Werbach, *supra* note 1, at 216.

home security systems are currently available that use the Internet, and they are often cheaper than old-fashioned burglar alarms.[17] Werbach's claims thus seem somewhat pedestrian, akin to complaining that modern interstate highways are not very suitable for horses and buggies.

Perhaps more on point is that Voice Link guarantees a 36 hour battery; is this enough? Are extra batteries available for those who need them? How about batteries to run cellular towers in case of a general power outage? We know that in major disasters, such as Hurricane Katrina, all communications may go down: PSTN, wireless, and cable (during Hurricane Katrina, only satellite continued to function).[18] What is an acceptable battery life, and who should decide what's acceptable? Werbach does not say.

Werbach characterizes AT&T's petition for limited trials to replace the PSTN with services subject to fewer regulations as "a dagger to the heart of the telecommunications regulatory structure of the Communications Act,"[19] as it appears to presage the nationwide deployment of PSTN's replacement and, with it, the demise of many longstanding regulations. But isn't this a good thing? We regulated the PSTN because it is (or was) a natural monopoly; if we now use competing Internet and wireless services as alternatives, then the monopoly is no more. So why do we need to keep regulation? Werbach believes the transition from the PSTN natural monopoly is a good thing, but he seems to think residual regulation is a good thing too—even if the rationale for it has disappeared.

III. PRESERVING THE PSTN'S FEATURES WITHOUT REGULATION

Early on, Werbach lays out how the PSTN should be defined in six concepts:

(1) Technical architecture;
(2) Regulatory arrangement;
(3) Market structure;
(4) Universal connectivity;
(5) Strategic infrastructure; and
(6) Social contract.[20]

---

17. *See, e.g.*, Devin Coldewey, *Scout Brings Home Security to the Internet Age (and It's Cheap)*, NBCNews.com (Feb. 14, 2013), *available at* http://www.nbcnews.com/tech/gadgets/scout-brings-home-security-internet-age-its-cheap-f1C8381570.

18. *See* Dr. Robert Miller, *Hurricane Katrina: Communications & Infrastructure Impacts*, in THREATS AT OUR THRESHOLD: HOMELAND DEFENSE AND HOMELAND SECURITY 191, 194-195 (Burt B. Tussing ed., 2006).

19. Werbach, *supra* note 1, at 214.

20. *Id.* at 220.

He sums up his article in this superb statement: "In essence, the first three conceptions of the PSTN are essentially descriptive, while the other three are normative. What the PSTN *is*, should be allowed and even encouraged to change; what the PSTN *does*, should be protected."[21] In other words, the first three conceptions will disappear with the transition, but the second three must be maintained. I fully agree with this statement, and applaud Werbach's insight and concision. However, I would not use the word "protected," as it implies that there must be a "protector," i.e., a regulator. I would rather use the term "assured"; if we are relatively confident that, for example, the market would assure these conceptions survive the transition, with no need for a regulator, then all should be happy with a market solution. Only in the event of a market failure would it be necessary to roll out the regulator.

Yet Werbach seems to believe that the transition from PSTN to IP-based technology would surely result in an oligopoly—a proposition without empirical support—and that an oligopoly requires regulation to control market power. Our economy, however, seems rife with oligopolies in many industries: automobile manufacturing and Internet search engines, to name two, and yet we seem to do well without regulating these oligopolies. Why the need to regulate IP-based telephone providers? The U.S. has two federal agencies responsible for prosecuting anti-competitive behavior: the Federal Trade Commission and the Department of Justice. Surely they are up to the job of policing market power problems.

Werbach then gets to the core of his argument, the three normative conceptions. I address each in turn.

Universal connectivity. The idea is that everyone should be connected to everyone else. There are two parts to this idea. The first is that everyone should have access to the network. Clearly, everyone has access to the PSTN; after the PSTN goes, will everyone have access to the Internet, or to wireless telephony? The data suggests that Internet/wireless access today is universal:[22] over 96% of US households have access to at least one 768 kbps (or greater) broadband provider,[23] plenty enough for VoIP, and 98% have access to at least one wireless provider,[24] all of which was accomplished without any regulatory requirement for universal access. Werbach's point of universal connectivity is important, but it appears that the Internet and wireless markets together have already accomplished this. What is the need for regulation?

The second part is that all the networks that comprise the Internet should interconnect with each other, a principle known as interconnection. This issue arises in the PSTN, wherein interconnection became a total mess

21. *Id.* at 221.
22. *See* NTIA, BROADBAND STATISTICS REPORT (2013), *available at* http://www2.ntia.doc.gov/files/broadband-data/Technology_by_Speed_June2013.pdf.
23. *Id.*
24. *Id.*

during the 1990s and early 2000s, due in large measure to regulation.[25] In contrast, networks in the unregulated Internet have managed to achieve interconnection using private contracts, without any difficulty whatsoever, since the mid-1980s. Werbach describes these various relationships: peering, transit, paid peering, each of which has a traditional commercial arrangement regarding who pays whom. It was only after the FCC adopted its Open Network Order in 2010,[26] thus signaling the FCC's willingness to extend regulation to the Internet, that a string of complaints arose from backbone networks, such as Level 3 and Cogent, against ISPs, such as Comcast and Verizon, demanding that the FCC order ISPs to provide the backbone networks free interconnection—contrary to established industry customary agreements.[27] Thus, over two decades with almost no complaints regarding Internet interconnection broke down when the FCC indicated its willingness to regulate.

Is interconnection important? It is vitally so, as Werbach correctly emphasizes. But is regulation needed to assure interconnection? The evidence suggests the opposite is true; without regulation, the Internet firms interconnected without problems, and certainly without customer outages.[28] With regulation, the PSTN had no end of difficulty maintaining fair and reasonable interconnection.

Strategic infrastructure. Werbach notes that the "[s]trategic aspects of the PSTN include reliability, security, law enforcement access, and public safety."[29] But is the Internet any less strategic than the PSTN? Surely we are concerned with the reliability of the Internet, and much attention has been given to its security in recent months, but these issues are addressed by other agencies without the FCC's help. Further, existing regulations assure that law enforcement has access to VoIP and wireless telephony for legal wiretaps,[30] and also assure that VoIP and wireless telephony provide access to E911 service,[31] so these problems are already solved. Why is more regulation necessary? Certainly the smooth functioning of the PSTN is important to the government, but the smooth

25. Gerald Faulhaber, *Should the FCC Regulate Internet Interconnection?* PENN PROGRAM ON REG. REGBLOG (June 9, 2014), *available at* http://www.regblog.org/2014/06/09-faulhaber-should-the-fcc-regulate-internet-interconnection.html.

26. Preserving the Open Internet, *Report and Order*, FCC 10-201, 25 FCC Rcd. 17905 (2010) [hereinafter *Open Internet Order*], *aff'd in part, vacated in part sub nom.* Verizon v. FCC, 740 F.3d 623, 636–42 (D.C. Cir. 2014).

27. *See* Faulhaber, *supra* note 25, for a detailed history of these recent complaints.

28. For a complete analysis of Internet interconnection disputes, their resolution, and their impact on customers, *see* Hal J. Singer, *Mandatory Interconnection: Should the FCC Serve as Internet Traffic Cop?*, Policy Brief, PROGRESSIVE POL'Y INST. (May 27, 2014), *available at* http://www.progressivepolicy.org/wp-content/uploads/2014/05/2014.05-Singer_Mandatory-Interconnection_Should-the-FCC-Serve-as-Internet-Traffic-Cop.pdf.

29. Werbach, *supra* note 1, at 226.

30. *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended at 18 U.S.C. § 2522 and 47 U.S.C. §§ 229, 1001-1010).

31. *See* 47 C.F.R. § 9 (2014).

functioning of the Internet is at least as important, and yet we have done quite well without the FCC regulating the Internet. What is the rationale to change course now?

Social contract. The initial social contract entailed granting private companies monopolies over telephony in return for their providing affordable service to all. As Werbach notes:

> Even after the opening of all telecommunications markets to competition, incumbent service providers supporting the PSTN still receive a variety of benefits. These include low-cost access to pole attachments and rights-of-way, receipt of universal service subsidies when serving high cost areas, free spectrum for the initial offering of mobile phone service, and protection against antitrust liability on the grounds that the Communications Act comprehensively regulates the field.[32]

Maybe it's time we stop giving incumbents some of these benefits. Since Internet and mobile wireless access is now universal, why is it necessary to provide universal service subsidies anymore? Perhaps doing so was necessary in the last century, but it is certainly not needed today. And the FCC hasn't handed out licensed spectrum for free in two decades. It is indeed true that regulation shields PSTN providers from antitrust liability,[33] but why does this remain necessary? Let's remove the shield by removing regulation and let antitrust authorities police abuses of market power if and when they occur.

Werbach insightfully notes that much of what the FCC regulates is migrating to the regulation-free Internet and the much less intensively regulated wireless industry. "[U]nless the FCC intends to go out of business," Werbach opines, "it must take action."[34] The obvious riposte is: what's the matter with the FCC going out of business? If a regulator is no longer needed, going out of business is exactly what should happen to it. Werbach appears to believe that the FCC should be looking for something, anything, to regulate or else its employees will be out of a job—an outcome he opposes. To the contrary, getting rid of unnecessary bureaucrats and regulations is beneficial to the public interest.

Werbach's fundamental point is that the three "enduring objectives" require that regulations be extended to the Internet in order to ensure their continued existence.[35] Again, while I agree that these enduring objectives are important, I disagree with Werbach that imposing regulation on the Internet to "protect" these enduring objectives is needed. In fact, at present, wireless and voice over the Internet actually meet these objectives with

---

32. Werbach, *supra* note 1, at 228.

33. *See, e.g.*, 15 U.S.C. § 45(a)(2) (2012) (exempting most "common carriers" from the FTC's authority to prohibit unfair practices).

34. Werbach, *supra* note 1, at 229.

35. *Id.* at 226.

little or no regulation. The competitive market has managed to get the job done with *de minimis* help from regulators.

And this is exactly the way the FCC intended the Internet to work. In his earlier work, Werbach himself said as much, noting that "as a practical and policy matter, regulation of Internet telephony would be problematic. It would be virtually impossible, for example, for the FCC to . . . require the ISPs segregate voice and data packets passing through their networks for regulatory purpose."[36] In *No Dialtone*, however, Werbach changes his tune, claiming that the PSTN has been undermined by the "collapse of the regulatory theory for data services."[37] While I agree that this transition is a good thing (for all the reasons Werbach mentions), his assertion about the regulatory theory for data services is a complete puzzle. For years, the FCC has had a strong and consistent position regarding the "regulatory theory" of the Internet (and before that data services), as Jason Oxman has explained:

> Although the FCC has a long tradition of encouraging the growth and development of the Internet by nonregulation, deregulation, and certain affirmative market-opening policies, there are frequent calls from many sources for the FCC to become more heavily involved in Internet regulation . . . . The challenge to the FCC . . . is to . . . further the Commission's longstanding goal of promoting competition, not regulation, in the marketplace.[38]

Further, former FCC Chairman and Clinton appointee William Kennard made the FCC's "regulatory theory" for the Internet even clearer:

> [T]he best decision government ever made with respect to the Internet was the decision that the FCC made . . . NOT to impose regulation on it. This was not a dodge; it was a decision NOT to act. It was intentional restraint born of humility. Humility that we can't predict where this market is going.[39]

This seems to be a very clear statement of the FCC's "regulatory theory for data services," and is perfectly consistent with the transition

---

36. Kevin Werbach, *Digital Tornado: The Internet and Telecommunications Policy* 29 (FCC OPP, Working Paper No. 29, 1997), *available at* http://transition.fcc.gov/Bureaus/OPP/working_papers/oppwp29.pdf.

37. Werbach, *supra* note 1, at 205.

38. Jason Oxman, *The FCC and the Unregulation of the Internet* 22 (FCC OPP, Working Paper No. 31, 1999), *available at* http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp31.pdf.

39. William E. Kennard, Chairman, FCC, The Road Not Taken: Building a Broadband Future for America, Remarks at the National Cable Television Association (June 15, 1999), *available at* http://www.fcc.gov/Speeches/Kennard/spwek921.html.

away from the PSTN. For several decades, the FCC's has clearly embraced a "hands off" policy towards the internet, and during that time, the Internet has been one of the great success stories of the past century.[40] Now, Werbach seems to believe it is time to regulate the Internet. I disagree strongly. The market-based Internet is doing just fine, fulfilling all of Werbach's enduring objectives. It works; let it be.

But how much could a little bit of regulation hurt? Werbach's recommendations sound pretty reasonable. Aren't I being a bit alarmist about the effects of regulation?

Economists have examined the costs of regulation in general for several decades. We need not repeat their arguments here, as they are well-known. The definitive works are Noll[41] and Carlton and Perloff.[42] In practice, regulation often results in firms and customers constrained by inefficient market actions, lessened incentives to invest, and the complete elimination of incentives for entry and innovation.[43] Regulation also opens wide opportunities for rent-seeking, as firms seek market advantage by administrative fiat rather than by serving their customers well.[44] When regulators are open for business, firms are quick to understand that pleasing or manipulating their regulators is far more important than innovating, investing, and pleasing customers. It is precisely because regulators have not been open for business on the Internet that it has been such an innovative and successful enterprise.

Advocates of regulation often ignore its seamy side, hoping that proposed network neutrality regulation will work perfectly or nearly so, without serious unintended consequences and implemented by an FCC that is all-wise, lobby-proof, and above-politics. Those of us with actual experience with regulators, myself included, find this Pollyanna attitude naïve in the extreme. Indeed, even regulators themselves are acutely aware of the serious limitations of regulation. Recently, the Federal Trade Commission warned of these costs when the FCC was considering network neutrality regulation:

> [W]e suggest that policy makers proceed with caution in evaluating calls for network . . . regulation. . . . No regulation, however well-intended, is cost-free, and it may be particularly difficult to avoid unintended consequences here, where the conduct at which regulation would be directed largely has not yet occurred. . . . This is the inherent difficulty in regulating

40. *See id.*

41. Roger G. Noll, *Economic Perspectives on the Politics of Regulation*, in 2 HANDBOOK OF INDUSTRIAL ORGANIZATION 1253–87 (Richard Schmalensee & Robert Willig eds., 1989).

42. DENNIS W. CARLTON & JEFFREY M. PERLOFF, MODERN INDUSTRIAL ORGANIZATION ch. 20 (4th ed. 2004).

43. *See generally* Noll, *supra* note 41.

44. *See id.*

> based on concerns about conduct that has not occurred, especially in a dynamic marketplace.[45]

Indeed, the FCC itself recognized the severe limits and costs of regulation in the broadband market space:

> [B]roadband services should exist in a minimal regulatory environment that promotes investment and innovation in a competitive market. We recognize that substantial investment is required to build out the networks that will support future broadband capabilities and applications. Therefore, our policy and regulatory framework will work to foster investment and innovation in these networks by limiting regulatory uncertainty and unnecessary or unduly burdensome regulatory costs.[46]

Both scholarly research and practical experience with regulation reach the same conclusion: regulation is by necessity a costly process, not to be undertaken without solid empirical proof that the hoped-for benefits outweigh the costs.

The long, depressing history of regulation has taught us two very important lessons that we need to keep firmly in mind at this critical juncture of the Internet. First, when regulators indicate a willingness to intervene in a market, all market participants will turn their attention from satisfying customers to special pleadings to get regulations that favor them and disfavor their competitors. Innovation takes second place to rent-seeking behavior by market participants as they jockey for regulatory advantage.

Second, even regulators who wish to limit the scope of their rules face constant pressure from market participants to expand their regulatory purview to help this or that participant. While the regulators may initially resist this pressure, regulation will inexorably extend to reach the entire industry.[47]

But is there a danger from regulation *now*? Surprisingly, we see the evidence of the pernicious effects of regulation of the Internet even before the regulatory ink has dried, in these very earliest days of Internet regulation. After 40 years of a hands-off-the-Internet policy, the FCC has in

---

45. FED. TRADE COMM'N, FTC STAFF REPORT, BROADBAND CONNECTIVITY COMPETITION POLICY 155, 157 (2007), *available at* http://www.ftc.gov/sites/default/files/documents/reports/broadband-connectivity-competition-policy/v070000report.pdf.

46. Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, *Notice of Proposed Rulemaking*, FCC 02-42, 17 FCC Rcd. 3019, para. 5 (2002).

47. For instance, in the 1930s, regulated railroads (then treated as natural monopolies) demanded extension of regulation to the nascent trucking industry (which was fully competitive), and they got it. This gave us high trucking rates, the Teamsters, and Jimmy Hoffa, until it was eventually undone 40 years later. *See* THEODORE E. KEELER, RAILROADS, FREIGHT, AND PUBLIC POLICY 26 (1983) ("As truck competition increased . . . the railroads clamored more and more loudly for placing the trucking industry under the same regulation they were subject to.").

fact decided to regulate the Internet in the form of the Open Internet Order.[48] Although this rule has yet to be finalized following an appeals court vacating the FCC's earlier rule in January 2014,[49] there is little doubt that some form of net neutrality will soon be (again) imposed on ISPs.

In 2010, when the FCC put up the "Open for Business" sign by issuing net neutrality rules, the rent-seeking started almost immediately. Level 3 objected to Comcast giving them the paid peering treatment when they started carrying Netflix traffic, a change in traffic balance that, according to common Internet practice, called for payment. Level 3, however, called it a violation of net neutrality and requested the FCC to step in to resolve this dispute.[50] Then-Chairman Genachowski dismissed the complaint as having nothing to do with net neutrality, but rather interconnection, and foreswore FCC intervention in the dispute.[51] But the Commission may well have no real choice; as net neutrality architect Tim Wu and his colleague Tejas Narechania explained in a letter they sent recently to the FCC, "the Commission now believes that the statutory aims of the Telecommunications Act are more easily met through regulated access rules rather than deregulated access."[52]

This is not a unique event. Recently, Cogent requested the regulator's help in its disputes with Comcast and Verizon, claiming it was entitled to free interconnection, much as Level 3 complained about four years ago.[53] Eventually, the problem was resolved without any customer losing Internet access, but the issue of interconnection has been put on the table. Despite Chairman Genachowski's decision to punt on the interconnection dispute in 2010, the issue is now squarely before the Commission—whether he (or the current Chairman) likes it or not.

It is worth noting that the rent-seeking that the Open Internet Order unleashed represents an attempt to get the FCC to expand its regulatory writ from net neutrality to interconnection. After 30 years of private contracting without complaint, the presence of the regulator elicits rent-seeking attempts aimed at extending regulation further into the Internet. It didn't take long for the two fundamental principles of regulation to show up, did it? This is an object lesson in the political economy of regulation.

This is not a new observation on my part. Carlton and Picker stated the principle most clearly:

> Competition is diverted from the marketplace to the regulator's office, and the tools for success—ranging from subtle

48. *See Open Internet Order*, *supra* note 26.
49. Verizon v. FCC, 740 F.3d 623, 636–42 (D.C. Cir. 2014).
50. *See* Faulhaber, *supra* note 25, for details of this dispute.
51. *Id.*
52. Tejas N. Narechania & Tim Wu, *Sender Side Transmission Rules for the Internet*, 66 FED COMM. L.J. 467 (2014).
53. *See* Om Malik, *Verizon: That Peering Flap (About Netflix) is Cogent's Fault*, GIGAOM (June 20, 2013, 4:06 AM), https://gigaom.com/2013/06/20/verizon-that-peering-flap-about-netflix-is-cogents-fault/.

> influence to out-and-out bribery—may be very different. Instead, we should regulate only when we must—natural monopoly being the core case—and leave general antitrust doctrine and the court system to handle the rest.[54]

We again seem to be ignoring the wisdom that history teaches us about how regulation evolves, somehow believing that well-intentioned people can regulate lightly, without unintended consequences or politicized rulemaking. We again hear the phrase "light-touch regulation,"—which, like the phrase "jumbo shrimp," is an oxymoron if there ever was one.

IV. CONCLUSION

Kevin Werbach wrote an excellent article on the demise of the PSTN, and he characterizes the challenge extremely well. But I am disappointed that his long experience with regulation and his extensive track record of first-rate scholarship has not guided him away from recommending that regulation be extended to the Internet so as to "protect" the enduring objectives of the PSTN.

The Internet works. Let it be.

54. Dennis Carlton & Randal Picker, *Antitrust and Regulation*, in ECONOMIC REGULATION AND ITS REFORM: WHAT HAVE WE LEARNED? 35 (Nancy L. Rose ed., 2014).

Wi-Fi Security: Shaping Data Privacy Rules

Carla Voigt*

TABLE OF CONTENTS

* J.D., The George Washington University Law School, May 2014.

I. INTRODUCTION

In a world of smartphones and tablets, the risk of revealing personal information never intended to be disseminated publicly is high. Wi-Fi[1] and other wireless communications technologies provide the ability to connect all of one's favorite content with a mobile phone, computer, or other devices easily and quickly.[2] This enables one to stay productive on the go by connecting to the Internet from remote locations.[3]

However, with this convenience comes great risk. For example, "[h]ackers snooping on unprotected or poorly protected Wi-Fi networks have been responsible for some of the biggest cyberheists in recent history, including numerous thefts from Seattle-area businesses from 2006 to 2011 and the 2007 TJX Companies data breach, which exposed 45 million credit card numbers."[4] Using Wi-Fi networks to send or receive confidential information could result in unauthorized disclosure of attorney-client privileged communications, trade secrets, or other confidential information—raising serious malpractice and ethical ramifications for attorneys. Because unencrypted private networks and public hotspots use public airwaves instead of wires for the transmission of communications, the interception of such unencrypted transmissions may not be within the reach of state or federal wiretap laws, even if such communications include user names, passwords, account numbers, credit card numbers, Social Security numbers, trade secrets, or attorney-client privileged communications.[5] Even more troublesome, "the mere use of such networks could call into question the status of such information as being confidential, privileged or trade secret," because exposing the information to an unencrypted network makes that information available for public consumption in its readable form.[6] Though "86% of internet users have taken steps online to remove or mask their digital footprints . . . [and] 55% of internet users have taken steps to avoid observation by specific people,

1. Wi-Fi is wireless transmissions that use 802.11b/g/n/ac specification and are used for wireless Internet access. *See* AIR802, IEEE 802.11 A/B/G/N WI-FI STANDARDS AND FACTS, *available at* http://www.air802.com/files/802-11-WiFi-Wireless-Standards-and-Facts.pdf. Wi-Fi devices use unlicensed spectrum governed by Part 15 of Title 47 of the FCC's rules. *See* 47 C.F.R. § 15 (2013).

2. *Discover and Learn*, WI-FI ALLIANCE, http://www.wi-fi.org/discover-and-learn (last visited Mar. 2, 2014).

3. *See id.*

4. Paul Wagenseil, *Google Spy Case Shows Why You Need to Encrypt Your Wi-Fi*, NBCNEWS.COM (Jan 21, 2012), http://www.nbcnews.com/technology/technolog/google-spy-case-shows-why-you-need-encrypt-your-wi-744411.

5. *See* Richard L. Ravin, *Using Public Wi-Fi Hotspots Can Land You in Hot Water by Risking Disclosure of Confidential Information*, 251 N.J. LAW. MAG., Apr. 2008, at 10, 10; *see also In re* Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888, 888 (N.D. Ill. 2012).

6. Ravin, *supra* note 5, at 10.

organizations, or the government,"[7] cautious Internet users are often at the mercy of their less careful correspondents. For example, the sender of an email attachment containing sensitive personal information sent from a secure, encrypted Wi-Fi network is in no position to ensure that the recipient—be it a doctor, lawyer, accountant, priest, or spouse—has taken care to encrypt her own Wi-Fi network. Therefore, anyone parked outside her house with a packet sniffer while she downloads the attachment could intercept its contents because the *recipient's* Wi-Fi network was not encrypted.[8]

This Note examines the authority of the Federal Communications Commission ("FCC") to address such data privacy concerns under the Wiretap Act and finds that this outdated regulatory framework places the FCC at a regulatory disadvantage. Part II of this Note explains how Wi-Fi works and why many consumers who believe their private information is protected are actually vulnerable to attack. Part III discusses the FCC's authority to regulate the interception of Wi-Fi communications under the agency's general statutory jurisdiction over communications technologies. Part III also explores recent litigation that demonstrates the inconsistencies in statutory interpretation that have arisen as a result of new technology and the ambiguous existing statutory framework. Part IV examines recent FCC administrative litigation and why it is important for the FCC to regulate new technology so as to bolster information privacy. Part V argues that Congress should amend the Wiretap Act to better protect user privacy. Part VI weighs several possible FCC administrative solutions and combinations thereof. Part VII discusses the implications of these administrative and legislative reforms for consumers and corporations.

II. BACKGROUND

Wi-Fi networks wirelessly connect electronic devices such as laptop computers, tablets, video game consoles, and smartphones to the Internet and each other through wireless network access points.[9] These networks operate in the 2.4 and 5 GHz radio bands,[10] and typically have a range of several hundred feet, although performance varies depending on obstructions and interference from other sources.[11]

---

7. LEE RAINIE ET AL., PEW RESEARCH CTR., ANONYMITY, PRIVACY, AND SECURITY ONLINE 2, 4 (Sept. 5, 2013), *available at* http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf.

8. *See* Joffe v. Google, Inc., 729 F.3d 1262, 1272 (9th Cir. 2013), *amended and superseded on reh'g*, 746 F.3d 920 (9th Cir. 2013), *cert denied*, 134 S. Ct. 2877 (2014).

9. *See Discover and Learn*, *supra* note 2.

10. *Id.*

11. *See* GIUSEPPE ANASTASI ET AL., WI-FI IN AD HOC MODE: A MEASUREMENT STUDY 5–6 (2004), *available at* http://pdf.aminer.org/000/538/456/wi_fi_in_ad_hoc_mode_a_measurement_study.pdf.

Today, 70.8% of Wi-Fi networks are estimated to be secured with encryption, leaving nearly 30% of Wi-Fi networks unsecured.[12] Collecting private information from these unsecured networks is easier than the average consumer might believe. Many hackers use packet-sniffing technology, which can unveil the contents of unencrypted network transmissions, to illegally break into networks and capture data including passwords, IP addresses, and other information that will help an attacker infiltrate the network.[13] Essentially, packet sniffing is to computer networks as wiretapping is to a telephone network.

According to Joel Gurin, former Chief of the Consumer and Governmental Affairs Bureau at the FCC, "[w]hether intentional or not, collecting information sent over WiFi networks clearly infringes on consumer privacy."[14] Since the FCC is the agency charged with promoting "safety of life and property" by "regulating interstate and foreign commerce in communication by wire and radio,"[15] the FCC can apply the substantive provisions of the Wiretap Act to emerging technologies such as Wi-Fi networks.

The FCC has examined the interception of private information over unencrypted Wi-Fi networks in the past. For example, in 2010, the agency opened an investigation into Google's Street View project, after the company admitted in May 2010 that its Street View cars had "mistakenly" collected samples of "payload data" including "e-mail and text messages, passwords, Internet usage history, and other highly sensitive personal information" from unsecured Wi-Fi networks.[16] Google subsequently explained that "while most of the data" it had collected was "fragmentary,

12. *See* WIRELESS GEOGRAPHIC LOGGING ENGINE, http://wigle.net/gps/gps/main/stats/ (last visited Mar. 2, 2014).

13. MOHAMMED ABDUL QADEER ET AL., IEEE COMPUTER SOC'Y, NETWORK TRAFFIC ANALYSIS AND INTRUSION DETECTION USING PACKET SNIFFER 313 (2010), *available at* http://eecs.wsu.edu/~nroy/courses/spring2013/cptsee555/papersbystudent/Network%20Traffic%20Analysis%20and%20Intrusion%20Detection%20using%20Packet%20Sniffer_Steven.pdf.

14. Joel Gurin, *Consumer View: Staying Safe from Cyber Snoops,* OFFICIAL BLOG OF THE FCC (June 11, 2010), http://reboot.fcc.gov/blog?entryId=493624.

15. 47 U.S.C. § 151 (2006).

16. Google, Inc., *Notice of Apparent Liability for Forfeiture*, DA 12-592, para. 1 (rel. Apr. 13, 2012) [hereinafter *Notice of Apparent Liability*], *available at* http://transition.fcc.gov/DA-12-592A1.pdf; *see also* Joffe v. Google, Inc., 746 F.3d 920, 922–23 (9th Cir. 2013), *aff'g In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067 (N.D. Cal. 2011) ("Payload data includes everything transmitted by a device connected to a Wi-Fi network, such as personal emails, usernames, passwords, videos, and documents."); *see also* Alan Eustace, *WiFi Data Collection: An Update*, GOOGLE OFFICIAL BLOG (May 14, 2010), http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html.

in some instances entire emails and URLs were captured, as well as passwords."[17]

Although the FCC's Google Street View investigation left observers with many unanswered questions, it also broke new ground for the agency in its role in policing consumer privacy.[18] The FCC's investigation into whether this interception of sensitive and personal information violated section 705(a) of the Communications Act[19] is examined in Part IV below. Since the FCC can enforce civil violations of the Wiretap Act involving Wi-Fi networks, what does that mean for companies and individuals moving forward? The penalty for this type of invasion of privacy was not established in the FCC's Google investigation in part because the agency lacked sufficient information.[20] The FCC issued nothing more than a slap on the wrist in the form of a measly $25,000 fine[21] to Google (which generated revenue of $14,890,000,000 in the third quarter of 2013).[22] Although the Google case suggests that the FCC intends to enforce the Wiretap Act provisions against similar privacy violations in the future, Congress should also take notice of this issue and explore statutory reform.

Since the passage of the 1996 amendments to the Communications Act eighteen years ago, communications technology has evolved more rapidly than lawmakers could have imagined. It is time for Congress to realign the Communications Act and the Wiretap Act with present technological realities. Congress must expand the FCC's authority to regulate emerging technologies. Doing so will allow the FCC to keep up with the "rapid deployment of new technology" it has been asked by Congress to promote.[23] In a world where the unofficial slogan of Silicon Valley is "[b]etter to seek forgiveness than permission,"[24] the FCC's ability

---

17. Alan Eustace, *Creating Stronger Privacy Controls Inside Google*, GOOGLE OFFICIAL BLOG (Oct. 22, 2010), http://googleblog.blogspot.com/2010/10/creating-stronger-privacy-controls.html.

18. In addition to the FCC, the Federal Trade Commission ("FTC") plays a major role in policing consumer privacy violations. Under federal law, the FTC is empowered to "prevent" most companies "from using . . . unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a) (2012).

19. 47 U.S.C. § 605(a) (2006).

20. *Id.*

21. *See* David Streitfeld & Edward Wyatt, *Unanswered Questions in F.C.C.'s Google Case*, N.Y. TIMES, Apr. 16, 2012, at B1, *available at* http://www.nytimes.com/2012/04/16/technology/fccs-google-case-leaves-unanswered-questions.html?pagewanted=all [hereinafter *Unanswered Questions*].

22. *See* Chris Velazco, *Google Beats the Street in Q3 with $14.89B in Revenue, Net Income of $2.97B, and EPS of $10.74*, TECHCRUNCH (Oct. 17, 2013), http://techcrunch.com/2013/10/17/google-q3-2013-earnings/.

23. *See* Elizabeth D. Lauzon, Annotation, *Construction and Application of Communications Act of 1934 and Telecommunications Act of 1996 – United States Supreme Court Cases*, 32 A.L.R. FED. 2D 125 § 2 (2008).

24. *See* David Streitfeld & Claire Cain Miller, *Google Hastens to Show Its Concern for Privacy*, N.Y. TIMES, Mar. 14, 2013, at B1, *available at* http://www.nytimes.com/

to address public concerns about privacy is essential to promoting confidence in new technology.

If Congress were to explicitly define the FCC's authority over new technologies—perhaps by clearly defining the phrases "readily accessible to the general public" and "radio communications," as discussed in Part III—it would remove obstacles to enforcement created by ambiguous language in the statute. Wi-Fi networks and similar technologies have become increasingly more common and in, therefore, merit greater FCC and judicial oversight. Consumer confidence is the backbone of the U.S. technology market, but recent events have caused a plunge in consumer confidence in information privacy and its regulators.[25] Congress must counteract this threat to innovation by overhauling obsolete privacy laws.

III. PRIVACY PROTECTION UNDER THE COMMUNICATIONS AND WIRETAP ACTS

In order to understand the scope of the FCC's jurisdiction over intercepted Wi-Fi communications, it is helpful to understand the two statutes that grant the FCC general jurisdiction over communications technologies and unlawful interceptions. The Communications Act of 1934 created the FCC, granting it "broad authority over interstate and foreign communication by wire or radio . . . ."[26] Congress has amended the Communications Act several times since 1934 in an effort to enable the FCC to regulate new technologies that have rendered old statutory provisions obsolete.[27] In 1968, the Wiretap Act broadened the scope of FCC jurisdiction through an additional grant of authority over electronic communications in addition to the already existing FCC jurisdiction over wire and radio communications.[28] The Wiretap Act, which is cross-referenced through the Communications Act, grants the FCC general authority to regulate emerging technologies, including Wi-Fi networks. The following discussion examines both statutes and their implications in turn.

2013/03/14/technology/google-focuses-on-privacy-after-street-view-settlement.html?pagewanted=all [hereinafter *Concern for Privacy*].

25. *See e.g.*, DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., HOW MUCH WILL PRISM COST THE U.S. CLOUD COMPUTING INDUSTRY? 1, 2 (Aug. 2013); Sam Gustin, *NSA Spying Scandal Could Cost U.S. Tech Giants Billions*, TIME BUS. & MONEY (Dec. 10, 2013), http://business.time.com/2013/12/10/nsa-spying-scandal-could-cost-u-s-tech-giants-billions/.

26. Lauzon, *supra* note 23.

27. *See, e.g.*, Cable Communications Act of 1984, Pub. L. No. 98-549, 98 Stat. 2780; Cable Television Consumer Protection and Competition Act of 1992, Pub. L. No. 102-385, 106 Stat. 1460; 47 U.S.C. § 201 (2006); Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112-96, Title VI, 125 Stat. 156.

28. Wiretap Act, 18 U.S.C. § 2510(12) (2012).

A. The Communications Act of 1934

The Communications Act of 1934 established the FCC "[f]or the purpose of regulating interstate and foreign commerce in communication by wire and radio" in the United States.[29] The Act stripped the Interstate Commerce Commission of its jurisdiction over telecommunications carriers and gave that authority to the newly created FCC.[30] By enacting this statute, Congress intended to make available "a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities" and to promote "safety of life and property through the use of wire and radio communications, and for the purpose of securing a more effective execution of this policy."[31]

The Communications Act also confers broad authority to the FCC to protect the public interest through rules and regulations. The FCC's rulemaking authority comes from section 4(a) of the Act, which provides that "[t]he Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions."[32] Congress' ultimate purpose in establishing the FCC was to set up an expert agency capable of coping with the ever-changing and constantly increasing problems of "a booming industry,"[33] to secure and protect the public interest,[34] and to ensure uniformity of regulation.[35]

In order to address changes in technology and further its effort to preserve and protect the integrity of communications by wire and radio in the United States, Congress enacted the Telecommunications Act of 1996 ("Telecommunications Act").[36] The Telecommunications Act overhauled the Communications Act to provide the FCC with additional authority to promote competition in the telecommunications industry, encourage the rapid deployment of new technology, and regulate nearly all radio communications in the United States.[37]

The FCC's authority to regulate communications intercepted over unencrypted Wi-Fi networks comes from the prohibitions outlined in section 705(a) of the Communications Act. Section 705(a) regulates the unauthorized publication or use of communications, prohibiting certain acts

---

29. 47 U.S.C. § 151 (2006).
30. The FCC replaced the Federal Radio Commission, which regulated radio use from 1926 to 1934. FCC MAX D. PAGLIN, A LEGISLATIVE HISTORY OF THE COMMUNICATIONS ACT OF 1934, at 3 (1989).
31. 47 U.S.C. § 151 (2006).
32. 47 U.S.C. § 154(i) (2006).
33. American Broadcasting Co. v. FCC, 191 F.2d 492, 498 (D.C. Cir. 1951).
34. WOKO, Inc. v. FCC, 109 F.2d 665, 667 (D.C. Cir. 1939).
35. Lauzon, *supra* note 23.
36. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.).
37. *Id.*

such as using and intercepting communications without authorization, except under certain conditions denoted in the Wiretap Act. [38]

B. The Wiretap Act

In response to "congressional investigations and published studies that found extensive wiretapping had been conducted by government agencies and private individuals without the consent of the parties or legal sanction,"[39] Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (commonly known as the "Wiretap Act"),[40] which originally covered only the unauthorized, nonconsensual interception of wire and oral communications by government agencies.[41]

By the 1980s, however, technology had evolved to offer wireless telephone services and communication through data transfer rather than voice. [42] Since the Wiretap Act applied only to voice communications over a wire or face to face, the need for Congressional action was clear.[43] The courts were still uncertain whether the Fourth Amendment protected communications over these new technologies, and the government argued that transmitting data through the computer of an Internet service provider waived any expectation of privacy. [44] According to some advocates, Congress faced the risk of "[a] ruling by the courts that wireless or data communications were not private, [which] would have stopped development of these technologies dead in their tracks." [45] Congress's response was to significantly revise the Wiretap Act by enacting the Electronic Communications Privacy Act ("ECPA").[46]

Title I of ECPA amended the Wiretap Act in 1986 to include "electronic communications" along with the communications by wire and radio already covered by the Wiretap Act.[47] As amended since, the current

---

38. 47 U.S.C. § 605(a) (2006). The exceptions are at chapter 119 of Title 18 of the United States Code.

39. *See Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act)*, DEP'T OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, JUSTICE INFO. SHARING, http://www.it.ojp.gov/default.aspx?area=privacy&page=1284#contentTop (last visited Mar. 2, 2014).

40. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–2520 (1968)).

41. 18 U.S.C. § 2511(1)(a) (1968).

42. *See Security and Surveillance*, CTR. FOR DEMOCRACY & TECH., https://www.cdt.org/issue/wiretap-ecpa (last visited Mar. 2, 2014).

43. *Id.*

44. *Id.*

45. *Id.*

46. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

47. S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557; *see also* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002). Wi-Fi networks are an example of an "electronic communication," which is defined by Congress as a communication transmitted by transferring "signs, signals, writing, images, sounds, data or

Wiretap Act provides that, with certain exceptions, "any person who intentionally intercepts . . . any wire, oral, or electronic communication" shall be subject to criminal and civil liability.[48] The amendments also made it illegal for government agencies or private parties to wiretap telephones or install electronic "sniffers" that read Internet traffic.[49] The Wiretap Act gives a private right of action to individuals aggrieved by the unlawful wiretapping of any person "other than the United States."[50]

C. Applicable Statutes Outdated as a Result of Innovation

The gap between what technology is capable of doing and the farthest reaches of existing regulations is growing. "[T]he FCC's authority under Title I is, at best, uncertain."[51]

In *Konop v. Hawaiian Airlines, Inc*., the United States Court of Appeals for the Ninth Circuit tackled the issue of whether a particular communication was an "electronic communication" and, if so, whether an "interception" had occurred.[52] In its opinion, the court noted that the issue was unnecessarily complicated by the seriously outdated Wiretap Act, observing that "[c]ourts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results."[53] The *Konop* court, back in 2002, recognized the need for Congress to reform the "confusing and uncertain" area of law under the Wiretap Act.[54] Since then, technology has continued to evolve; it is time that Congress act to protect the privacy of the billions of people who transmit private information over Wi-Fi networks every day.

---

intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12) (2012).

48. 18 U.S.C. §§ 2511(1)(a), 2511(4)(a), 2520(a) (2012). "[I]ntercept" as defined by the Wiretap Act "means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (2012).

49. 18 U.S.C. § 2510(6) (2012).

50. 18 U.S.C. § 2520 (2012).

51. James B. Speta, *FCC Authority to Regulate the Internet: Creating It and Limiting It*, 15 LOY. U. CHI. L. J. 15, 22 (2004).

52. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002).

53. *See id.* (citing Robert A. Pikowsky, *Legal and Technological Issues Surrounding Privacy of Attorney Client Communication Via Email,* Advocate, Oct. 2000, at 17–19 (discussing the uncertainty over email privacy caused by ECPA and judicial interpretations thereof); *see also* LeEllen Coacher, *Permitting Systems Protection Monitoring: When the Government Can Look and What It Can See,* 46 A.F. L. REV. 155, 171–74 (1999) (same); Tatsuya Akamine, Note, *Proposal for a Fair Statutory Interpretation: E-mail Stored in a Service Provider Computer is Subject to an Interception Under the Federal Wiretap Act,* 7 J.L. POL'Y 519, 521–29, 561–68 (1999) (criticizing the judiciary's interpretation of ECPA)).

54. *Konop*, 302 F.3d at 874 ("We observe that until Congress brings the laws in line with modern technology, protection of the Internet and websites such as Konop's will remain . . . uncertain . . . .").

D. Exceptions to the Wiretap Act and Related Litigation

The Wiretap Act, as amended by ECPA, makes it illegal to intercept electronic communications, but it includes an important exception that is relevant to the interception of communications over Wi-Fi networks. The Wiretap Act exempts from liability the interception of communications "made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." [55] Communications that fall within this exception may be intercepted legally regardless of whether or not they were *intended* to be made available to the public.[56] The phrase "readily accessible to the general public" is defined in section 2510(16) with respect to radio communication to mean that such communication is not "scrambled or encrypted," among other requirements.[57] The statute does not, however, specifically address when *electronic communications* are "readily accessible to the general public."[58] "The legislative history of ECPA suggests that Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards," as opposed to communications that are easily accessible to the general public.[59]

In 2010, several individuals brought a consolidated class action complaint against Google in the United States District Court for the Northern District of California regarding the company's collection of Wi-Fi payload data, alleging among other things that Google unlawfully intercepted their communications in violation of the Wiretap Act.[60] Google, in defense of its Street View data collection, argued that intercepting payload data transmitted on an unencrypted Wi-Fi network is not a

---

55. 18 U.S.C. § 2511(g)(i) (2012).

56. *But see* Orin Kerr, *District Court Rules that the Wiretap Act Does Not Prohibit Intercepting Unencrypted Wireless Communications*, VOLOKH CONSPIRACY (Sept. 6, 2012, 7:08 PM), http://www.volokh.com/2012/09/06/district-court-rules-that-the-wiretap-act-does-not-prohibit-intercepting-unencrypted-wireless-communications/.

57. 18 U.S.C. § 2510(16) (2012). It is important to note that section 2510(16) specifies radio communication when addressing whether something is "readily accessible to the public."

58. Joffe v. Google, Inc., 746 F.3d 920, 924 (9th Cir. 2013).

59. *Konop*, 302 F.3d at 874 (quoting S. REP. NO. 99-541, at 35–36, *reprinted in* 1986 U.S.C.C.A.N. at 3599 ("This provision [the SCA] addresses the growing problem of unauthorized persons deliberately gaining access to . . . electronic or wire communications that are not intended to be available to the public.") and H.R. REP. NO. 99-647 at 41, 62–63 (1986) ("[D]escribing the Committee's understanding that the configuration of the electronic communications system would determine whether or not an electronic communication was readily accessible to the public . . . .")).

60. Joffe v. Google, Inc., 746 F.3d 920, 924 (9th Cir. 2013). The consolidated class was comprised of all persons whose electronic communications were intercepted by Google Street View vehicles since May 25, 2007. For a discussion of Google's alleged conduct, see *infra* Part IV.

violation of the Wiretap Act because it falls into the exception in 18 U.S.C. section 2511(2)(g)(i)[61] ("G1"), which states as follows:

> (g) It shall not be unlawful under this chapter or chapter 121 of this title for any person – (i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.[62]

The court thus faced the question whether the phrase "readily accessible to the general public" applies to *unencrypted* Wi-Fi networks and, accordingly, whether Wi-Fi networks fall into the G1 exception.[63]

The consolidated class action plaintiffs argued that the phrase "'readily accessible to the general public' applies solely to 'radio communications,' as specified [in the definition in 18 U.S.C. section 2510(16)], and thus would only apply to exemption G2 ('radio communications') [64] and not exemption G1 ('electronic communications')."[65] The court acknowledged in its opinion that this

> case of first impression as to whether the Wiretap Act imposes liability upon a defendant who allegedly intentionally intercepts data packets from a wireless home network . . . presents a novel question of statutory interpretation as to how the definition in Section 2510(16) of 'readily accessible to the general public' modifies exemption G1, if at all.[66]

---

61. *In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1073 (N.D. Cal. 2011).

62. 18 U.S.C. § 2511(2)(g)(i) (2012).

63. *See* Andrew Fong, *In re Google Inc. Street View Electronic Communications Litigation: Radio Communications and Privacy by Convention*, BERKELEY TECH. L.J. BOLT (July 4, 2011), http://btlj.org/2011/07/04/in-re-google-inc-street-view-electronic-communications-litigation-radio-communications-and-privacy-by-convention/.

64. 18 U.S.C. § 2511(2)(g)(ii) ("G2") states that:

> (g) It shall not be unlawful under this chapter or chapter 121 of this title for any person – . . . (ii) to intercept any radio communication which is transmitted – (I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress; (II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public; (III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or (IV) by an marine or aeronautical communications system.

18 U.S.C. § 2511(2)(g)(ii) (2012).

65. *See In re Google*, 794 F. Supp. 2d at 1073.

66. *Id.* at 1074; *see also* 18 U.S.C. § 2510(16) (2012) ("'[R]eadily accessible to the general public' means, with respect to a radio communication, that such communication is not . . . (A) scrambled or encrypted.").

The court further noted that "Congress has not expressly declared its intent as to how Section 2510(16) should apply to exemption G1 in the plain text of the statute, nor has Congress defined 'radio communication' anywhere within the Act."[67] Therefore, courts "must ascertain the statute's plain meaning by looking to the particular language at issue and the language and design of the statute as a whole."[68] In doing so, the district court determined that an unencrypted *radio communication* is "readily accessible to the general public," so its interception does not give rise to liability under the Wiretap Act because of the combination of the G1 exemption and the section 2510(16) definition.[69] Because "radio communication" is not defined by the Wiretap Act, the court reasoned, "'radio communication' encompasses only 'traditional radio services,' and not other technologies that also transmit data using radio waves, such as cellular phones and Wi-Fi networks."[70] Therefore, the section 2510(16) definition of "readily accessible to the general public" does not apply to Wi-Fi networks because the definition is limited to electronic communications that are radio communications.[71] Acknowledging that the plain language of the statute is ambiguous, for it does not define the phrase "readily accessible to the general public" as it applies to an "electronic communication" that is not a "radio communication," the court denied Google's motion to dismiss the Wiretap Act claim.[72] "[W]ithout more," the court held, "merely pleading that a network is unencrypted does not render that network readily accessible to the general public and serve to remove the intentional interception of electronic communications from that network from liability under the [ECPA]."[73]

Google sought interlocutory review of the district court's ruling from U.S. Court of Appeals for the Ninth Circuit, arguing that the trial court had misconstrued the Wiretap Act.[74] Specifically, Google contended that the district court erred in finding that Congress did not intend for "electronic communications," such as Wi-Fi, to be included in the narrow G1 exception for electronic communications "readily accessible to the general public."[75] The Ninth Circuit held that the phrase "readily accessible to the general public" in section 2510(16) with respect to a radio communication does not apply to the exemption for an "electronic communication" that is "readily accessible to the general public" under the G1 exemption.[76]

---

67. *In re Google*, 794 F. Supp. 2d at 1075.
68. *See* K Mart Corp. v. Cartier, Inc., 486 U.S. 281, 282 (1988).
69. Joffe v. Google, Inc., 746 F.3d 920, 924 (9th Cir. 2013) (citing *In re Google*, 794 F. Supp. 2d at 1076–81).
70. *Id.*
71. *Id.*
72. *In re Google*, 794 F. Supp. 2d at 1084.
73. *Id.*
74. *See generally Joffe*, 746 F.3d at 920.
75. *See In re Google*, 794 F. Supp. 2d at 1068.
76. *Joffe*, 746 F.3d at 926.

Further, the court determined that the ordinary meaning of "radio communication" does not include data transmitted over a Wi-Fi network and that the payload data transmitted over unencrypted Wi-Fi networks that was captured by Google is not predominantly auditory and is therefore outside of the section 2510(16) definition.[77] In essence, the Ninth Circuit ruling determined that intercepting Wi-Fi communications can violate the Wiretap Act.

E. Inconsistencies in the Courts

In affirming the district court's denial of Google's motion to dismiss, the Ninth Circuit examined the provisions of the Wiretap Act by looking to the plain language of the statute,[78] congressional intent,[79] and the statute as a whole.[80] The district court, in determining that Wi-Fi transmissions are not radio communications, acknowledged that the data on an open Wi-Fi network is only accessible in plain text via sophisticated technology.[81]

However, in a different case—*In re Innovatio IP Ventures, LLC Patent Litigation*—Judge Holderman of the United States District Court for the Northern District of Illinois ruled otherwise.[82] In that case, the district court granted Innovatio's Rule 16(c)(2) motion, holding that Innovatio's use of commercially available Wi-Fi network analyzers to collect information about the wireless network users' allegedly infringing Wi-Fi networks was legal and not in violation of the Wiretap Act.[83] Innovatio argued, and the court agreed, that the Wiretap Act does not apply because

---

77. *Id.* at 926–28.

78. *See id.* at 926–29 (defining the ordinary meaning of the phrase "radio communications" to be (1) predominantly auditory and (2) broadcast and holding that the payload data collected by Google over unencrypted Wi-Fi networks cannot be classified as predominantly auditory).

79. *See id.* at 927–28 (identifying similar terms in the Wiretap Act that Congress chose to provide definitions for and noting that Congress refrained from providing a technical definition of "radio communication" that would have altered the notion that it should carry its common, ordinary meaning).

80. *See id.* at 928–36.

81. *See In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1071 (N.D. Cal. 2011).

82. *See generally In re* Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888 (N.D. Ill. 2012); *see also* Mike Masnick, *Judge Says Sniffing Unencrypted WiFi Networks is Not Wiretapping*, TECHDIRT (Sept. 10, 2012, 7:15 AM), http://www.techdirt.com/blog/wireless/articles/20120907/16331020314/judge-says-sniffing-unencrypted-wifi-networks-is-not-wiretapping.shtml.

83. *In re Innovatio*, 886 F. Supp. 2d at 889–90. ("The packet capture adapter can intercept data packets that are traveling wirelessly between the Wi-Fi router provided by the Wireless Network Users and any devices that may be communicating with it, such as a customer's laptop, smartphone, or tablet computer. Innovatio then uses Wireshark network packet analyzer software to analyze the data packets, revealing information about the configuration of the network and the devices in the network. The data packets also include any substantive information that customers using the Wi-Fi network may have been

> even assuming that Innovatio's proposed protocol intercepts Wi-Fi communications, Innovatio's proposed protocol falls into the exception to the Wiretap Act allowing a person 'to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.'[84]

The court noted, however, that "an individual's online activity can be chilled merely by the knowledge that a third party has the power to acquire, however briefly, the contents of his communication."[85] Thus, the real issue is not "whether the *networks* are 'readily accessible to the general public,' but instead whether the network is configured in such a way so that the *electronic communications* sent over the network are readily available."[86]

Judge Holderman held that the proposed sniffing protocol is permissible under the G1 exception to the Wiretap Act and that "[a]ny tension between that conclusion and the public's expectation of privacy is the product of the law's constant struggle to keep up with changing technology."[87] Judge Holderman also held that the sniffing technology involved in this case did not amount, in his opinion, to "*sophisticated* packet sniffer technology."[88] However, the Ninth Circuit in *Joffe* held just

---

transmitting during the interception of the data packets, including e-mails, pictures, videos, passwords, financial information, private documents, and anything else a customer could transmit to the internet.").

84. *Id.* at 892 (quoting 18 U.S.C. § 2511(g)(i) (2006)).

85. *Id.* (quoting Amati v. City of Woodstock, 829 F. Supp. 889, 1008 (N.D. Ill. 1993) ("holding that the privacy interests of an individual whose conversations come under the power of another are implicated 'even if the individual was assured no one would listen to his conversations, because the individual's privacy interests are no longer autonomous'") and United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992) ("acquisition occurs 'when the contents of a wire communication are captured or redirected *in any way*'" (emphasis added))).

86. *Id.* It is important to note that the court here was only considering the sniffing of "Public-facing Networks" and declined to address "whether Innovatio should be allowed to sniff the defendants' private networks that are not available to the public," which was a central issue in *In re Google* and other Google Street View litigation. *Id.* at 894, n. 6.

87. *Id.* at 894.

88. *Id.* at 893 (emphasis added).

> Moreover, upon examination, the proposition that Wi-Fi communications are accessible only with sophisticated technology breaks down. As mentioned above, Innovatio is intercepting Wi-Fi communications with a Riverbed AirPcap Nx packet capture adapter, which is available to the public for purchase for $698.00. *See Riverbed Technology Product Catalog,* http://www.cacetech.com/products/catalog/ (last visited Aug. 21, 2012). A more basic packet capture adapter is available for only $198.00. *Id.* The software necessary to analyze the data that the packet capture adapters collect is available for download for free. *See Wireshark Frequently Asked Questions,* http://www.wireshark.org/faq. html#sec1 (last visited Aug. 21, 2012) ("Wireshark® is a network protocol analyzer. . . . It is freely available as open source. . . ."). With a packet capture

the opposite, noting that "'radio hobbyists' do not mistakenly use packet sniffers to intercept payload data transmitted on Wi-Fi networks" and a definition of "radio communications" that encompasses data transmitted over Wi-Fi networks "would obliterate Congress's compromise [89] and create absurd applications of the exemption for intercepting unencrypted radio communications."[90]

Though *In re Innovatio* and *In re Google* approach the same issue from different angles and appear to have opposite holdings, the two cases contain a common message: "[I]t is not the court's job to update the law to provide protection for consumers against ever changing technology. Only Congress, after balancing any competing policy interests, can play that role."[91] The uncertainty present in the current state of the law is evidenced by the different approaches taken by the courts in trying to determine whether the interception of private information transmitted on unencrypted Wi-Fi networks is a violation of the Wiretap Act. This murkiness stands as a barrier to enforcement and must be remedied so that consumers continue to believe that new technologies are safe and that their private information is protected.

IV. FCC PRIVACY LITIGATION

The major purpose of the FCC is to protect the public interest, which includes protecting the privacy of consumers. However, the agency currently faces the problem of how best to protect the public interest within the limitations of the Wiretap Act. If consumers lose confidence in new technology for fear of invasion of their privacy—and therefore forego using such technologies—innovation will suffer.[92] In order to change this outdated and confusing area of law into a viable framework from which effective regulation can flow, the FCC and Congress must address whether

---

> adapter and the software, along with a basic laptop computer, any member of the general public within range of an unencrypted Wi-Fi network can begin intercepting communications sent on that network. Many Wi-Fi networks provided by commercial establishments (such as coffee shops and restaurants) are unencrypted, and open to such interference from anyone with the right equipment. In light of the ease of "sniffing" Wi-Fi networks, the court concludes that the communications sent on an unencrypted Wi-Fi network are readily available to the general public.

Id. at 393.

89. The Ninth Circuit noted that in order to address concerns by radio hobbyists that traditional radio services can be easily and mistakenly intercepted, Congress modified the original language of the Wiretap Act as a compromise. Joffe v. Google, Inc., 746 F.3d 920, 931 (9th Cir. 2013).

90. *Id.* ("It seems doubtful that Congress wanted to emphasize that Google or anyone else could park outside of a police station that carelessly failed to secure its Wi-Fi network and intercept confidential data with impunity.").

91. *In re Innovatio*, 886 F. Supp. 2d at 894.

92. *See e.g.*, CASTRO, *supra* note 25, at 1–2; Gustin, *supra* note 25.

Wi-Fi networks are "readily accessible to the general public"[93] and how the Wiretap Act will be applied to emerging technologies going forward. In 2010, the FCC attempted to do just that.

A. Google Street View Litigation

In 2010, the FCC opened an investigation into Google after the company admitted publicly that from 2007 to 2010, as part of its Street View project, it had collected private user data from Wi-Fi networks throughout the United States.[94] This unauthorized collection of data, which was alleged to be a violation of the Wiretap Act, included sensitive "payload" data, which Google did not need for the purposes of its project.[95] This "payload" data included the content of users' Internet communications, specifically personal information such as "e-mails and text messages, passwords, Internet usage history, and other highly sensitive personal information."[96] Google Street View cars collected this personal information through "wireless sniffer" technology concealed in its cars, which was added by Google engineers to "secretly capture[] data packets as they stream across Wi-Fi connections and then decode[] or decrypt[] the data packet and analyze[] the contents."[97] At first, Google claimed it did not have knowledge of the addition of wireless sniffers to the Street View cars.[98] However, it was later alleged that other people at Google were aware of the wireless sniffers and the data they were collecting.[99]

By the time the European privacy authority opened its investigation against Google in 2010, Google admitted to collecting "about 600 gigabytes of data from more than 30 countries."[100] As discussed in Part III, serious privacy concerns also prompted a series of class action lawsuits in the United States, as well as in Europe and Australia, all alleging that Google used this "Wi-Fi sniffer" technology to eavesdrop on unsecured Wi-Fi networks and thus unlawfully intercept users' private data.[101]

---

93. 18 U.S.C. § 2511(2)(g)(ii) (2012).
94. *See Notice of Apparent Liability*, *supra* note 16, at para. 1.
95. *Id.*
96. *Id.*
97. *In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1071 (N.D. Cal. 2011); *see generally* ANASTASI ET AL., *supra* note 11, at 150.
98. *See Unanswered Questions*, *supra* note 21.
99. *See id.*
100. *In re Google*, 794 F. Supp. 2d at 1071; *see also* Joffe v. Google, Inc., 746 F.3d 920, 923 (9th Cir. 2013).
101. *See Investigations of Google Street View*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/streetview/ (last visited Mar. 2, 2014) ("As of 2012, investigations have gone forward in at least 12 countries, and at least 9 countries have found Google guilty of violating their laws."). The FCC noted that "several countries, including Canada, France, and the Netherlands, have determined that Google's collection of payload data violated their data protection, online privacy, or similar laws and regulations." *See Notice of Apparent*

B. FCC Decision

The well-established threat to privacy that drove Congress to pass ECPA was exemplified in the 2010 FCC investigation of Google's Street View project. Intercepting sensitive payload data from users who believe their data to be private and secure falls within the spirit of ECPA and the privacy invasions it seeks to prevent. Although the interception of payload information from private and residential Wi-Fi networks clearly invades consumer privacy,[102] the FCC declined to charge Google with violating the Communications Act after determining that there was no "clear precedent for applying Section 705(a) of the Communications Act to the Wi-Fi communications at issue."[103] Additionally, the FCC lacked a significant evidentiary basis for applying the Communications Act to Google's conduct due to a software developer's refusal to testify based on his Fifth Amendment right against self-incrimination.[104]

The FCC opted to fine Google $25,000 for "willfully and repeatedly violating an Enforcement Bureau directive to respond to a letter of inquiry."[105] Thus, because Google failed to produce evidence regarding whether the payload information was reviewed or accessed after it was collected, and because the agency lacked a precedent for applying section 705(a) in the context of Wi-Fi, the FCC did not find a violation of section 705(a).[106] By nonetheless publicly reprimanding Google for its conduct in this manner, the FCC has given Congress another example of how the Wiretap Act has not kept up with advances in digital communications.[107]

C. Why Regulation of Interceptions of Information Transmitted over Unencrypted Wi-Fi Networks Is Important

Google faced even more litigation over its Street View Program when thirty-eight state attorneys general brought an action against Google

---

Liability, *supra* note 16, at para. 15. The European investigations found that these violations were serious and have taken the issue of data privacy in the private sector much more seriously as compared to the United States. *See FCC Investigation of Google Street View*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/google/fcc_investigation_of_google_st.html (last visited Mar. 2, 2014); *PBS NewsHour: How Will FCC's Google Street View Fine Shape Data Privacy Rules?* (PBS television broadcast Apr. 16, 2012), *available at* http://www.pbs.org/newshour/bb/law/jan-june12/google_04-16.html.

102. *See FCC Investigation of Google Street View*, *supra* note 107; *PBS NewsHour*, *supra* note 101.

103. *Notice of Apparent Liability*, *supra* note 16, at para. 5.

104. *See id.*; *see also* David Kravets, *Contradicting a Federal Judge, FCC Clears Google in Wi-Fi Sniffing Debacle*, WIRED (Apr. 16, 2012, 6:41 PM), http://www.wired.com/threatlevel/2012/04/fcc-clears-google/.

105. *Notice of Apparent Liability*, *supra* note 16, at para. 54.

106. *Id.* at para. 53.

107. *See Unanswered Questions*, *supra* note 21.

for its violation of consumer privacy.[108] In a settlement reached by the parties, Google agreed to pay a $7 million fine to the states involved, to set up a privacy program, to hold an annual privacy week event for employees, to make privacy certification programs available to select employees, to provide refresher training for its lawyers overseeing new products, and to train its employees who deal with privacy matters.[109] A large part of the settlement involves outreach in the form of educational advertisements and educating the public as to how to encrypt their data on their wireless networks.[110] This settlement signifies the interest of the states' attorneys general in protecting the privacy rights of Internet users as information sharing technology evolves and their willingness to prosecute violations.[111]

The settlement, however, once again demonstrates the insufficiency of the current state of the law. Critics expressed skepticism about the efficacy of the settlement, voicing concerns that it will not make much of a difference in how Google behaves."[112] Bolstering these doubts, Google has made similar educational promises before, yet it continues to be involved in litigation over its privacy practices.[113] This $7 million dollar settlement is a trivial amount for the company, given its net income in 2013 of around $32 million per day.[114]

Even more troublesome, the *Innovatio* court effectively granted permission under the Wiretap Act to hackers and other malicious actors to *legally* use packet sniffing technology similar to that used by Google in its Street View Program to access personal passwords, financial records, and other sensitive information from unencrypted Wi-Fi networks.[115] The myriad of decisions and agreements coming from the FCC, the courts, and the states have only contributed to the unsettled state of the law. Although individuals harmed by the interception of their unencrypted Wi-Fi communications may be able to maintain causes of action based on common law and other statutes,[116] the Wiretap Act is uniquely in its clear-

---

108. *See* Press Release, George Jepsen, Office of the Attorney Gen., Attorney General Announces $7 Million Multistate Settlement with Google Over Street View Collection of WiFi Data (Mar. 12, 2013) [hereinafter Jepsen Press Release], *available at* http://www.ct.gov/ag/cwp/view.asp?Q=520518.

109. *See id.*

110. *Id.*

111. *Id.*

112. *Concern for Privacy*, *supra* note 24.

113. *Id.*

114. David Streitfeld, *Google Concedes that Drive-By Prying Violated Privacy*, N.Y. TIMES, Mar. 13, 2013, at A1, *available at* http://www.nytimes.com/2013/03/13/technology/google-pays-fine-over-street-view-privacy-breach.html [hereinafter *Drive-By Prying*].

115. *In re* Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888, 894 (N.D. Ill. 2012).

116. *E.g.*, 18 U.S.C. § 1030 (2012) (criminalizing the act of knowingly accessing a protected computer without authorization or in excess of authorized access); RESTATEMENT (SECOND) OF TORTS § 652B (1977 & Supp. 2014) (imposing tort liability on the intentional, offensive intrusion upon the seclusion of another).

cut and consistent applicability to unauthorized interception of communications not intended to be made publicly available.

Technological innovation will suffer if consumers are unwilling to buy cutting-edge products for fear that their private information will be compromised. If information is legally accessible to anyone willing to purchase the technology needed to intercept private data from Wi-Fi networks, consumer privacy will suffer. Congress has attempted to update privacy protections in response to technological innovation multiple times through legislative endeavors such as the Telecommunications Act and ECPA.[117] Through ECPA, Congress sought to ensure that the "readily accessible to the general public" exception to the Wiretap Act included only those communications in which the operator makes it clear, through the volitional configuration of their device, that they intend that their communications be public.[118] It is inconsistent with the intent of ECPA to imagine that the operator of a wireless home network intends that their network be accessible to the general public,[119] so courts should not impute this intent on unsuspecting private network owners.

Although most consumers encrypt and protect their private Wi-Fi communications, many other consumers either do not know how to do so or do not realize the risk they are taking by failing to affirmatively act to protect their data. Google's new obligation to educate the public about data encryption is a step in the right direction,[120] but the privacy risk is far too severe for Congress to leave the statutory framework in its current, ambiguous form. The courts have attempted to protect users' rights and impose liability for privacy infringement. The FCC has also looked at the statutory framework and attempted to clarify this murky area of the law, for the most part to no avail.

V. A CALL FOR CONGRESSIONAL ACTION

The conflicting rulings and difficulties expressed by the courts and the FCC are evidence that Congress must clarify and provide an enforcement mechanism for the FCC and the judiciary to use in order to further the goals of the Communications Act and the Wiretap Act. Although challenges will arise in determining exactly where to draw the line between a reasonable expectation of privacy and communications that are readily accessible to the general public, a clear boundary is necessary so that the FCC and the judiciary have a clear understanding of and consistently apply the law going forward.

---

117. *See id.* at 9; *see also In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 18 (1st Cir. 2003) ("The paramount purpose of the Wiretap Act is to protect effectively the privacy of communications.").

118. *See id.*

119. *Id.*

120. Jepsen Press Release, *supra* note 108.

To interpret this convoluted area of law, the FCC and the judiciary have relied primarily on statutory language and legislative intent, with little case law to guide them.[121] Today's outdated statutes create confusion and unpredictability in regulation, ultimately allowing an unsuspecting consumer's privacy to be violated legally.[122] On the one hand, the *In re Google* court suggested that Wi-Fi communications are not readily accessible to the general public, even if they are sent unencrypted.[123] Similarly, the FCC discussion of the Wiretap Act and current lack of evidence from Google in its investigation of the Street View Project implies that if the agency had information showing that Google intended to intercept the contents of Wi-Fi networks, the agency could construe the Wiretap Act as applying to such interceptions.[124] On the other hand, the *In re Innovatio* court ruled the opposite, holding that the technology needed to intercept the communications was not "sophisticated" enough to make the communications non-public.[125]

Legal scholars have taken to the blogs to speak out against all three of these decisions. For example, legal scholar Orin Kerr disagrees with Judge Holderman's reasoning in the *In re Innovatio* case, noting,

> No one suggests that unsecured wireless networks are set up with the goal that everyone on the network would be free to read the private communications of others. In my view, that ends the matter: the exception doesn't apply, and the interception of the contents of wireless communications is covered by the Wiretap Act.[126]

Kerr argues that the issue under G1 "is what the designers [of the network] intended users to be able to do, not what someone can do contrary to the designer's intentions."[127] Others point to the fact that the necessity of

---

121. *See e.g.*, *In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1074 (N.D. Cal. 2011) (examining novel question of statutory interpretation and relying instead on legislative intent as a result of ambiguous statutory language as applied to new technology).

122. *But see supra* note 116.

123. *Id.*

124. *See generally Notice of Apparent Liability*, *supra* note 16.

125. *In re Innovatio*, 886 F. Supp. 2d at 893.

126. Kerr, *supra* note 56 (arguing that "'configured so that such electronic communication is readily accessible to the general public' focuses on the intent of the designer—the person who does the configuring of the network so that it works a particular way—to design the network so that the general public was supposed to be able to access them.").

127. *Id.* (discussing *In re Innovatio*, 886 F. Supp. 2d at 888); *but see* Brief for Elec. Privacy Info. Ctr. as Amicus Curiae Supporting Plaintiffs at 3, *In re Google*, 794 F. Supp. 2d 1067 (No. 5:10-md-02184-JW) ("The term 'configured' in the evaluation of those communications that are 'publicly accessible' reflects an intent by Congress to create a presumption in favor of confidentiality except in those circumstances where the *user* has knowingly chosen to broadcast communications to the general public." (emphasis added)).

specialized or sophisticated equipment to decode the intercept should not be a factor in its legality.

Many legal scholars have framed Google's conduct as a prime example of a failing statute in need of congressional attention. In an interview with PBS, legal scholar Jeffrey Rosen discussed Judge Ware's holding in *In re Google*, noting,

> [T]here's a strong case that this is illegal under existing law. Certainly, if it's not, it should be. And the fact that the FCC chose not to investigate shouldn't [be] seen as a clean bill of health for Google, because every other European regulator that has looked into this question has found unequivocal violations.[128]

This call to action to update the law is long overdue. By enacting ECPA in 1986, Congress sought to encourage the creation of new technologies by preserving "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement."[129] Now, twenty-eight years later, it is time for Congress to again pass an amendment to the Communications Act to expressly permit the FCC to impose liability to protect private information shared through new technologies that have emerged in the last three decades. Historically, Congress has done this by amending the Communications Act to accommodate the dramatic changes in communications technology that have taken place since the FCC's creation, including the introduction of television, satellite and microwave communications, cable television, the cellular telephone, and Personal Communications Services.[130]

Recently, former FCC Chairman Julius Genachowski recommended an amendment to the Communications Act during the hearing on the fiscal year 2013 FCC budget, and Senator Dick Durbin (D–IL) said that he would consider changes to the law if that is the necessary course of action.[131] Senator Durbin criticized the FCC for "decid[ing] to impose a fine of $25,000 on a company worth $111 billion," noting that the small fine is

---

128. Interview by Ray Suarez with James Rosen, Professor of Law, The George Washington Univ. Law Sch., and David Bennahum, Founder & CEO, Punch! Media (Apr. 16, 2012), *available at* http://www.pbs.org/newshour/bb/law/jan-june12/google_04-16.html.

129. H.R. REP. NO. 99-647, at 19 (1986); *see also* J. BECKWITH BURR, WILMERHALE, THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986: PRINCIPLES FOR REFORM 1 n.3 (Mar. 30, 2010), *available at* http://digitaldueprocess.org/files/DDP_Burr_Memo.pdf.

130. *See, e.g.*, Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–21 (1988).

131. *See generally Hearing on Expanding Broadband Access, Promoting Innovation, and Protecting Consumers in a Communications Revolution: FY 2013 Resource Needs for the FCC Before the Subcomm. on Fin. Servs. & Gen. Gov't of the S. Comm. on Appropriations*, 112th Cong. (2012) [hereinafter *FY 2013 Appropriations Hearing*] (hearing beginning at 32:20), *available at* http://www.appropriations.senate.gov/webcasts.cfm?method=webcasts.view&id=4eade537-0f2b-4280-84fa-c3a2bf8ded89.

"somewhere short of a tap on the wrist."[132] Genachowski explained that the FCC Enforcement Bureau and the General Counsel's office decided that, as a legal matter, because the information was collected from unencrypted Wi-Fi signals, it did not violate the law as written. The former Chairman suggested that Congress look at the law and that consumers encrypt their networks.[133] However, the FCC and the courts have reached opposite conclusions regarding the application of the Wiretap Act to unencrypted Wi-Fi networks. It is time that Congress clarifies the issue.

Congress should amend the Wiretap Act and Communications Act to clarify that private communications are protected regardless of their underlying technology so long as they are not intentionally configured to be "readily accessible to the general public." This amendment must allow for the imposition of liability for privacy violations involving new technology, thus ensuring that privacy protections are not eroded in the near future as technology continues to evolve. Congress should amend the Wiretap Act to expressly exclude Wi-Fi networks and similar technologies from the definition of radio communications, thus ensuring that these technologies are not included in the Wiretap Act's G1 exception for electronic communications readily accessible to the general public. This would make collection of information over Wi-Fi networks a violation of the Wiretap Act, regardless of whether the consumer acted to encrypt their network—subject only to the exceptions in G2. Congress should also include in the amendment a technology neutral explanation of this provision to address the intent of the amendment and the need for the provisions to evolve in accordance with technology.

Additionally, Congress should also change the definition of "readily accessible to the general public"[134] in section 1510(16) to better protect consumer privacy. This amendment should clarify that the legality of intercepting personal information over a Wi-Fi network does not depend on whether the Wi-Fi network is encrypted. Congress must draw a clear line between protected and unprotected communications so that consumers can more effectively protect themselves. Congress, through the Communications Act and the Wiretap Act, should protect private communications transmitted on private networks, encrypted or unencrypted, just as communications by telephone are protected even if transmitted insecurely. Thus, it should be illegal for persons to intercept data transmitted over a Wi-Fi network.

---

132. *See generally id.*

133. *See generally id.* (adding that the "educational purposes that have been served by this [FCC investigation], educating [Google] and other companies, educating Congress, [and] educating consumers, [are] certainly important benefits of [the] process."); *see also On Google Spy-Fi, Senator Durbin Calls for Update to Wiretap Law, FCC Chair Agrees Law Should Protect Unencrypted Communications*, ELEC. PRIVACY INFO. CTR. (May 11, 2012), http://epic.org/2012/05/on-google-spy-fi-senator-durbi.html.

134. 18 U.S.C. § 2510(16) (2012).

An interesting line drawing issue arises in the context of public versus private networks when defining the term "readily accessible to the general public" line. Public "Wi-Fi Hotspots," which are hotspots in places of public accommodation such as hotels, restaurants, and Starbucks, have become common throughout the world and should perhaps be treated differently than private residential networks. Users connecting to Wi-Fi hotspots in public places may not have the same expectation of privacy as users of residential networks; however, their communications should arguably still be protected. The data transmitted over both public and private networks is most often sent with an expectation that unauthorized parties will not collect or use the data. Naiveté should not warrant an invasion of privacy.

There are many approaches Congress could take to clarify the regulatory framework. If Congress were to exclude "public-facing networks" from Wiretap Act liability, hackers using sniffer technology would have the ability to *legally* access personal information and search history through the Wi-Fi connection and access personal data that can then be used for purposes contrary to the protections provided by the Wiretap Act.[135] Therefore, any exclusion regarding public-facing networks would need to be counterbalanced by consumer education programs designed to teach the public which types of networks are open and which provide protection for their private information. Neither approach is obviously more logical or fair than the other, but whether there is an exception for public-facing Wi-Fi hotspots is not as important as drawing a clear line. It is more important that the issue be settled than that it be settled in a particular way because, presently, consumers have a false sense of security on their networks—and the FCC and the judiciary have a morass of law they must untangle before protection can be provided. To encourage innovation, Congress must also encourage consumer confidence and trust in new technology.

VI. FCC PRIVACY AUTHORITY AND DUE PROCESS

Updating the Wiretap Act is necessary, and it will likely occur at some point—though the precise timeline is uncertain. In the meantime, however, the FCC faces the problem of how to administer the Wiretap Act to best protect users' Wi-Fi networks and prosecute hackers who collect and use private information. Regardless of the prospect of congressional action, the FCC should take to its interpretative powers to address the growing privacy concerns of the public.

Although many of the terms in the Wiretap Act are defined in the statute, those definitions have been expanded through FCC litigation and policy statements throughout the years. Title I of the Communications Act

135. *But see supra* note 116.

grants the FCC the authority to make policy through case-by-case adjudication, in addition to its rulemaking procedures.[136] This power is limited by the Due Process Clause of the Fifth Amendment as incorporated into administrative law, which prohibits the FCC from penalizing a person who has not been given adequate notice that their conduct violates a particular policy.[137] Nonetheless, the FCC is authorized to make policy decisions through adjudicatory proceedings even when applying statutory language to a new technology as a matter of first impression so long as the FCC complies with the due process notice requirement.[138]

A. Statutory Authority to Act

The FCC has the power under the Administrative Procedures Act ("APA") to engage in statutory interpretation through both adjudication and rulemaking.[139] Since the Communications Act authorizes the FCC to engage in adjudicatory proceedings but does not require that they be "on the record," the FCC is free to engage in adjudication subject only to the modest procedural restraints in APA section 555.[140] When an agency's adjudication relies on its interpretation of ambiguous terms in its enabling statute, the reviewing court will defer to the agency's reasonable interpretation of the statute.[141] The FCC may also act through notice and comment rulemaking, by issuing interpretative rules, and by issuing policy statements.[142]

The FCC is also constrained by constitutional limitations. Specifically, the FCC does not have the power to impose legal consequences without adequate notice at the time of the violation.[143] This presents an obstacle to case-by-case expansion of the Wiretap Act to include new technologies as they arise.

B. FCC Action: A Step by Step Plan

The FCC has the power to address the meaning of the Wiretap Act to protect consumer privacy in the absence of congressional action. Pursuant to the APA and the FCC's enabling statute, the Communications Act, the

---

136. *See* 47 U.S.C. § 151 (2006).
137. *See* Satellite Broadcasting Co., Inc. v. FCC, 824 F.2d 1, 3 (D.C. Cir 1987).
138. *See* SEC v. Chenery Corp., 332 U.S. 194, 203 (1947).
139. *See* 47 U.S.C. § 154(i) (2006); *see also* Aaron K. Brauer-Rieke, Note, *The FCC Tackles Net Neutrality: Agency Jurisdiction and the Comcast Order*, 24 BERKELEY TECH. L. J. 593, 599–601 (2009).
140. *See* 47 U.S.C. § 154(i) (2006).
141. Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 842–44 (1984).
142. *Rulemaking Process at the FCC*, FCC ENCYCLOPEDIA, http://www.fcc.gov/encyclopedia/rulemaking-process-fcc (last visited Mar. 2, 2014).
143. *See* FCC v. Fox Television Stations, Inc., 132 S. Ct. 2307, 2317 (2012).

FCC has the power to issue its own rules and regulations in order to further the provisions of the Act. The FCC may do this in one of three ways: (1) legislative rulemaking; (2) interpretive rulemaking and policy statements; or (3) case-by-case adjudication.

1. Legislative Rulemaking

The FCC's first option is to issue a Notice of Proposed Rulemaking and begin the process of issuing a legislative rule. The Communications Act grants the FCC the power to issue legislative rules through its broad grant of rulemaking power necessary to carry out the provisions of the Act.[144] Through "notice and comment" rulemaking, the FCC can propose a new interpretation of the Wiretap Act in order to correct a problem the agency has identified, such as "industry behavior that adversely affects consumers."[145] As in the case of Wi-Fi network regulation, the FCC "may have difficulties enforcing existing rules and this may provide evidence of a need to modify the rules . . . [o]r, changes in technology may suggest that it is time to update a rule."[146]

The FCC could issue a rule clarifying that unencrypted Wi-Fi networks do not fall under the "readily accessible to the general public" exception of 18 U.S.C. § 2511(g)(i).[147] The Wiretap Act's goal of protecting consumers and their private information provides a justification for an FCC interpretation of the statute to include a prohibition on the interception of data not that was not intended to be public.[148] A legislative rule would have the force of law and would allow the FCC, the expert agency most familiar with the issues at stake, to determine exactly where the "readily accessible to the general public" line should be drawn.[149]

2. Interpretive Rulemaking and Policy Statements

Additionally, the FCC could issue an interpretive rule or policy statement. Although this option would not create any binding legal effect, it

144. *See* 47 U.S.C. § 154 (2006).
145. *Rulemaking Process at the FCC*, *supra* note 142.
146. *Id.*
147. *See* 18 U.S.C. § 2511(g)(i) (2012).
148. *See* 18 U.S.C. § 2510 (2012); *see Konop*, 302 F.3d at 875 ("The legislative history of the [Wiretap Act] suggests that Congress wanted to protect electronic communications that are configured to be private, such as email."); *also In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 18 (1st Cir. 2003) ("The paramount objective of the Wiretap Act is to protect effectively the privacy of communications.").
149. *See Rulemaking Process at the FCC*, *supra* note 142. However, a legislative rule passed through the notice and comment rulemaking procedure would not assist the FCC in addressing the issue at hand in the immediate future because the notice and comment procedure can take years to complete.

provides an instrument to interpret the binding statute and clarify the scope of pre-existing rights and duties.[150]

Pursuant to APA section 553(b), "interpretive rules, general statements of policy, or rules of agency organization, procedure, or practice" are all categories of rules that are exempt from procedural requirements, meaning the FCC can avoid the extensive notice and comment rulemaking procedures mandated by the APA for formal rulemaking and still succeed in putting the public on notice that they plan to exercise their jurisdiction under the statutes.[151] By declaring that the provisions of the Wiretap Act regarding unlawful interception of data seriously pre-date the current wireless Internet technologies available today, the FCC could interpret the plain language of the statute to give protection to data transmitted over Wi-Fi networks, thereby enabling the FCC to carry out the legislature's intent to protect the public interest.[152]

3. Case-by-Case Adjudication

Another means by which the FCC has the power to regulate interceptions of electronic and radio communications is on a case-by-case adjudicatory basis. Through adjudications, the FCC can exercise its enforcement jurisdiction as a Title I regulatory regime and place the public on notice of its interpretation of the Communications Act and its provisions as amended.

As discussed above, before the FCC can expand existing policies and regulations, it must first provide adequate notice as to what actions constitute violations of existing policies. An agency may not impose civil or criminal penalties when neither the regulation nor the Commission's related statements gave fair notice of that requirement.[153] The FCC order in *Google Street View* can be read as a warning to those that intercept data on Wi-Fi networks, and could thus have major implications for Internet users and companies gathering data both actively and passively.[154] Although the FCC declined to enforce the Wiretap Act against Google, the FCC extended the Wiretap Act to include data interception from unencrypted Wi-Fi networks.[155] The FCC explained in its *Notice of Apparent Liability for Forfeiture* that it declined to enforce section 705(a) of the Wiretap Act

150. *Id.*
151. *See* 5 U.S.C. § 553(b) (1966).
152. *See infra* Part III.A; *see also In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1076 (N.D. Cal. 2011) (citing 18 U.S.C. § 2511(5)(a)(i)(B) (2006)) (noting "the lack of any explicit reference to wireless internet technologies does not itself preclude an interpretation of 'radio communications' that would include these later-developed technologies.").
153. *See, e.g.*, Trinity Bd. of Fla., Inc. v. FCC, 211 F.3d 618, 619 (D.C. Cir. 2000).
154. *See generally Notice of Apparent Liability*, *supra* note 16.
155. *See id.* at para. 52.

against Google because it lacked both information[156] and Commission precedent addressing the application of section 705(a) to Wi-Fi communications.[157] This rationale implies that, in the future, if the FCC has evidence that information was collected from unencrypted Wi-Fi networks, it could choose to take enforcement action.

At this point, the state of the law includes inconsistent decisions by courts and the FCC interpreting the same statutory provisions. Congress has the power to amend the Communications Act to either override or adopt any of these interpretations. The FCC, as the expert agency tasked with regulation of communications technology, is perhaps in the best position to issue rules that adapt to new and emerging technologies.[158] The conflicting holdings between the FCC and the judiciary are confirmation that it is time that Congress step in and update the statutes to fit the times.

VII. IMPLICATIONS FOR THE FCC, CORPORATIONS, AND CONSUMERS

The full implications of the FCC decision to fine Google and the subsequent class action decisions concerning Google Street View remain to be determined. The Wiretap Act was enacted in 1968 and amended by ECPA in 1986. As technology has since changed, so too should the FCC's interpretation of its jurisdiction under the Act. When faced with a violation of the Wiretap Act in the future, the FCC may hold an extensive adjudication in which it declares that the agency has authority to pursue the interception of data over unencrypted Wi-Fi networks as announced in *Google Street View* and may at that point define the scope of that power in an enforcement proceeding. Alternatively, as discussed above, the FCC may issue an interpretive rule in the meantime, expanding its interpretation of the Wiretap Act to include interceptions over unencrypted Wi-Fi networks as violations of the Act, in order to protect users who are concerned about the security of their Wi-Fi enabled communications.

The approaches taken by the FCC and Congress will soon be relevant not only as Google revamps its Street View project, but in other mapping projects as well. The new privacy programs Google has agreed to implement over the next ten years and the company's recent admission it invaded consumer privacy will affect many of the products Google sends out to the market, including its most recent product, Google Glass.[159] As

156. *See id.* at para. 53 ("The Bureau's inability to compel an interview of Engineer Doe made it impossible to determine in the course of our investigation whether Google did make any use of any encrypted communications that it collected.").

157. *Id.*

158. *See* Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 980 (2005) (holding the Commission is free within the limits of reasoned interpretation to change course if it adequately justifies the change).

159. *See Drive-by Prying*, *supra* note 114.

companies such as Apple and Google update their maps applications in the future, they will have to be especially careful to collect only authorized data, leaving the personal payload data behind. These companies should interpret the Google Street View litigation at the FCC and in the courts to as a warning that any interceptions of unencrypted Wi-Fi networks may violate the Wiretap Act. In addition, educating consumers so that they have a realistic idea of how easy it is to become a victim of Wi-Fi sniffers should be a priority for both Congress and the FCC moving forward.

VIII. CONCLUSION

In the last decade, the world has seen incredible advancements in communications technology and witnessed how entrepreneurship and innovation can spur economic growth.[160] Unfortunately, the laws governing communications interception in the United States are seriously outdated. The FCC, the judiciary, legal scholars, and the public have all called upon Congress to update the Wiretap Act in order to accommodate innovation in communications technology. To further the public interest, the FCC should encourage technological innovation while ensuring the safety and privacy of consumers. For the FCC to effectively carry out this mission, Congress should amend the Wiretap Act to clarify the definition of radio communications so that Wi-Fi networks and other new technologies carry the privacy protections of the Wiretap Act, whether or not their transmissions are encrypted. In the meantime, the FCC should interpret the Wiretap Act to include this unencrypted Wi-Fi communication by exercising the broad rulemaking powers granted to it by the Communications Act. In addition, the FCC's decision in *Google Street View* constitutes notice that the FCC can take enforcement action against interceptions of data over Wi-Fi networks—including unencrypted networks—to protect the public and its privacy in future adjudications. Unfortunately, the FCC can only stretch the Communications Act so far; the rest is up to Congress.

When a crisis emerges in the United States, Congress should look to the underlying causes of that crisis and seek a solution that benefits the country as a whole. The current privacy crisis in the United States is a result of outdated statutes and new technology. Unfortunately, only one of these two phenomena can survive—either Congress updates the Communications Act to keep up with technology, or consumers will lose faith and trust in technology, causing innovation in the United States to experience a decline. The time to act is now.

160. *See generally FY 2013 Appropriations Hearing*, *supra* note 131 (statement of Sen. Moran, Member, S. Comm. on Appropriations).

35573-fcl_66-3 Sheet No. 82 Side B 10/21/2014 10:02:02

The Likely Regulators? An Analysis of FCC Jurisdiction over Cybersecurity

Mike Sherling*

TABLE OF CONTENTS

* J.D., *cum laude*, The George Washington University Law School, May 2014. The Author would like to thank Ethan Lucarelli and Charlie Pollack as well as the *FCLJ* members and editorial board for their valuable suggestions and feedback. The author would also like to thank his partner and his family for their support.

35573-fcl_66-3 Sheet No. 83 Side B 10/21/2014 10:02:02

I. INTRODUCTION

In October 2012, Former Secretary of Defense Leon Panetta warned the nation of the potential for a "cyber Pearl Harbor" that would cause physical destruction and the loss of life.[1] "In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability," he stated gravely.[2] The attack could "be as destructive as the terrorist attack on 9/11."[3] While the Secretary's statements were arguably hyperbolic,[4] ineffective cybersecurity in the United States is a pressing problem, jeopardizing both national security and individual online safety.[5] Recent events clearly illustrate that cyber-attacks have become almost a daily part of life. Skilled attackers can use computer and network vulnerabilities to do everything from commit bank fraud to disrupt uranium enrichment.[6]

Part of the reason for this vulnerability to cyber-attacks is the lack of uniform implementation of existing, authoritative network security standards for Internet service providers ("ISPs"),[7] a problem that persists

---

1. Leon E. Panetta, Sec'y of Def., Dep't of Def., Speech before the Business Executives for National Security: Defending the Nation from Cyber Attack (Oct. 11, 2012), *available at* http://www.defense.gov/speeches/speech.aspx?speechid=1728.

2. *Id.*

3. *Id.*

4. While hyperbolic, recent disclosures by Edward Snowden show the extent of United States cyber capabilities. These disclosures reveal wide-ranging abilities to infiltrate communications networks and platforms once thought secure. *See* Claudia Diaz, Omer Tene & Seda Gürses, *Hero or Villain: The Data Controller in Privacy Law and Technologies*, 74 OHIO ST. L.J. 923, 933–34 (2013); *see generally Edward Snowden*, THE GUARDIAN, http://www.theguardian.com/world/edward-snowden (last visited Dec. 25, 2013) (compiling articles on the NSA disclosures).

5. *See, e.g.*, Michael Riley, *Exxon, Shell, BP Said to Have Been Hacked Through Chinese Internet Servers*, BLOOMBERG (Feb. 24, 2011), http://www.bloomberg.com/news/2011-02-24/exxon-shell-bp-said-to-have-been-hacked-through-chinese-Internet-servers.html (detailing recent cyber-attacks).

6 *See generally* RYAN SHERSTOBITOFF, ANALYZING PROJECT BLITZKRIEG, A CREDIBLE THREAT, MCAFEE (Dec. 2012), *available at* http://www.mcafee.com/us/resources/white-papers/wp-analyzing-project-blitzkrieg.pdf; NICOLAS FALLIERE, LIAM MURCHU & ERIC CHIEN, W32.STUXNET DOSSIER, SYMANTEC (Feb. 2011), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; Jim Finkle & Dhanya Skariachan, *Target Cyber Breach Hits 40 Million Payment Cards at Holiday Peak*, REUTERS (Dec. 19, 2013), http://www.reuters.com/article/2013/12/19/us-target-breach-idUSBRE9BH1GX20131219.

7. *See, e.g.*, *DNS-based Authentication of Named Entities*, IETF (2012), https://datatracker.ietf.org/wg/dane/. The Internet Engineering Task Force ("IETF") is an international community of network designers, operators, vendors, and researchers with the goal of creating specifications of high technical quality while considering the interests of all of the affected parties and while establishing widespread community consensus. *See IETF Standards Process*, IETF (2012), http://www.ietf.org/about/standards-process.html. Throughout this Note, the terms "minimum cybersecurity standards," "minimum standards," and "industry best practices" are used interchangeably. *See 911 Reliability Order*, *infra* note 192, at para. 46 (noting that "best practices are developed in a 'consensus-based

because ISPs are under no obligation to implement these standards.[8] Together, these factors have created a market that often fails to provide adequate cybersecurity.[9]

When a market fails to provide a necessary service, such as the guaranteed integrity of the communications network, the government can step in to fill the gap. This Note argues that the Federal Communications Commission ("FCC") has the authority to require ISPs to implement network level cybersecurity measures to maintain the integrity and security of the networks. The FCC derives this power from its ancillary authority in Title I of the Communications Act of 1934 and its statutory mandates to ensure a reliable communications network and implement 9-1-1 service over VoIP.[10]

To establish the FCC's authority in this area, this Note examines some of the causes of and partial solutions to cyber-attacks in relation to FCC authority. Part II gives background on network security and cyber-attacks, and details the FCC's ancillary authority, which allows the FCC to promulgate regulations concerning technology over which it does not have a direct statutory mandate. Part III analyzes the FCC's ability to use its ancillary authority to require ISPs to implement cybersecurity standards, concluding that the FCC has jurisdiction to implement minimum standards because insufficient cybersecurity could catastrophically impact services the FCC oversees. Part IV considers whether the FCC should exercise its ancillary authority, determining that the market failure in cybersecurity vulnerability information and network reliability, together with the compelling need for a reliable communications system, justifies

---

environment' reflecting the collective judgment of industry, government, and other stakeholders.").

8. *See* Austin Schlick, FCC General Counsel, FCC, *A Third-Way Legal Framework for Addressing the* Comcast *Dilemma* (May 6, 2010), *available at* http://fjallfoss.fcc.gov/edocs_public/attachmatch/DOC-297945A1.pdf (noting "the Commission's settled, deregulatory policy framework for broadband communications services.").

9. *See, e.g.*, ATLANTIC COUNCIL, A FIERCE DOMAIN: CONFLICT IN CYBERSPACE 13 (Jason Healey ed., forthcoming 2013) (on file with editor) ("We've had market failure when it comes to cybersecurity. Security doesn't come out of voluntary actions and market forces.") (quoting Deputy Secretary of Defense Ashton Carter at the RSA Conference in 2012); *see also id.* ("The market does not work well enough to raise the security of computer systems at a rate fast enough to match the apparent growth in threats to systems.") (quoting National Academy of Science report, Computers at Risk in 1991); Christian F. Binnig, *The Legal and Policy Challenges of a Rapidly Changing Telecommunications Industry*, *in* RECENT DEVELOPMENTS IN TELECOMMUNICATIONS LAW 9 (Oct. 2013), *available at* 2013 WL 6117748; *cf.* Proposed Extension of Part 4 of the Commission's Rules Regarding Outage Reporting, *Notice of Proposed Rulemaking*, FCC 11-74, para. 20 (2011) [hereinafter VoIP Outage Reporting NPRM] ("The economic justification to ensure [Internet] service appears to be limited, and does not consider network externalities. Moreover, even if incentives did motivate individual market participants to optimize their own reliability, they do not necessarily optimize systemic reliability.") (citations omitted).

10. *See* 47 U.S.C. § 615a-1 (2006); Communications Act of 1934, ch. 652, 48 Stat. 1064 (codified as amended at scattered sections 47 U.S.C.).

government regulation. The Note concludes with a brief discussion of the costs and benefits of potential regulation.

II. BACKGROUND

The near consensus is that the current state of cybersecurity is abysmal.[11] For example, the computer security firm McAfee has over 100 million samples of malware in its database.[12] The National Vulnerability Database contains over 50,000 software vulnerabilities that malicious actors can exploit;[13] myriad industries experience cyber-attacks daily.[14] The magnitude of the problem is staggering.

With threats coming from all over the world this is both a national and international problem.[15] In 2005, American corporations lost an estimated $867 million due to cyber-attacks, cyber theft, and other computer security incidents.[16] Recent high-profile events include attacks against the security firm RSA,[17] Google,[18] the financial sector,[19] oil companies,[20] and several others.[21] Moreover, it is more than just corporate

11. Jason Ryan, *NSA Director on Cyberattacks: 'Everybody's Getting Hit'*, ABC NEWS (Nov. 7, 2012), http://abcnews.go.com/blogs/politics/2012/11/nsa-director-on-cyberattacks-everybodys-getting-hit (cataloging a myriad range of companies hit by cyber-attacks in 2011). *But see* Jerry Brito & Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, 3 HARV. NAT. SEC. J. 39 (2011) (desiring a more thorough justification to buttress calls for increased resources to be devoted to cyber-threats), *available at* http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Brito_Watkins.pdf.

12. MCAFEE LABS, *McAfee Threats Report: Third Quarter* 2012, at 9, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2012.pdf (last visited Nov. 15, 2012).

13. NATIONAL VULNERABILITY DATABASE, http://nvd.nist.gov (last visited Nov. 17, 2012). As of November 17, 2012, the database contained 53,914 common vulnerabilities and exposures. *Id.*

14. MCAFEE LABS, *supra* note 12, at 23–24.

15. *See, e.g.*, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS, MANDIANT 22 (2013) [hereinafter MANDIANT REPORT], *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (noting attacks originating from China against 15 different countries).

16. RAMONA R. RANTALA, DEP'T OF JUSTICE, *Cybercrime Against Businesses,* at 1 (Sept. 2008), *available at* http://bjs.ojp.usdoj.gov/content/pub/pdf/cb05.pdf. Other computer security incidents include attacks using spyware, ad-ware, hacking, phishing, spoofing, pinging, port scanning regardless of whether the attack was successful. *Id.* at 2.

17. *See generally* Zeljka Zorz, *RSA Hacked, SecurID Users Possibly Affected*, HELP NET SEC. (Mar. 18, 2011), http://www.net-security.org/secworld.php?id=10763.

18. Kevin P. Newmeyer, *Cyber Espionage: A Threat to National Security*, 10 SEC. & DEF. STUD. REV., Spring-Summer 2010, at 116.

19. *See* MCAFEE LABS, *supra* note 12, at 7.

20. *See, e.g.*, Michael Riley, *Exxon, Shell, BP Said to Have Been Hacked Through Chinese Internet Servers*, BLOOMBERG (Feb. 24, 2011), http://www.bloomberg.com/news/2011-02-24/exxon-shell-bp-said-to-have-been-hacked-through-chinese-Internet -servers.html.

21. *See* Ryan, *supra* note 11.

networks that are under attack; cyber-attacks also compromise the basic computer infrastructure of the Internet.

A. Network Security Standards and Cyber-attacks

Uniform implementation of industry-developed network security standards by ISPs could significantly reduce overall vulnerability to cyber-attacks. For example, one of the foundational elements of the Internet, the Domain Name System ("DNS"), has well-known flaws.[22] The DNS is a set of computers that translates user-friendly text, such as website addresses, into the string of numbers (Internet Protocol, or IP, addresses)[23] that computers use to communicate on the Internet.[24] In the Internet's nascent days, the engineers who created the Internet chose a standard that did not emphasize security, instead focusing on ease of integration and interoperability.[25] As a result, the DNS is vulnerable to attacks By malicious actors who can hijack and reroute Internet traffic from the intended website to their own server.[26] In a case involving bank fraud, for example, when a person tries to access an online banking website, her computer connects to a DNS server on the Internet and receives the IP address of the bank website.[27] However, if a cyber-attacker provides the DNS server with the wrong IP address, the server would direct her browser to a malicious website that can capture bank login information.[28]

In the mid-1990s, as the vulnerabilities of DNS became apparent, the development of a more secure system—known as Domain Name System Security Extensions ("DNSSEC")—began in earnest. DNSSEC was finalized in 2005, and by 2010, major Internet authorities, such as the Internet Corporation for Assigned Names and Numbers ("ICANN") and

---

22. *See* JOHN KRISTOFF & RODNEY JOFFEE, NEUSTAR ULTRA SERVICES, *Botnets and Packet Flooding DDoS Attacks on the Domain Name System* 1 (2007), *available at* http://layer9.com/~jtk/papers/dnsddos.pdf; *see generally DNS Threats & Weaknesses of the Domain Name System*, DNSSEC: DNS SECURITY EXTENSIONS, http://www.dnssec.net/dns-threats.php (last visited Nov. 15, 2012).

23. This Note uses the term IP or Internet Protocol as shorthand for the TCP/IP Suite and related technologies that mediate the packet-switched communications. For an in-depth discussion of the technology that powers the internet and modern communications networks, see Douglas C. Sicker & Lisa Blumensaadt, *Misunderstanding the Layered Model(s)*, 4 J. TELECOMM. & HIGH TECH. L. 299 (2006) and Christopher S. Yoo, *Protocol Layering and Internet Policy*, 161 U. PA. L. REV. 1707 (2013).

24. CSRIC III WORKING GROUP 5, *DNSSEC Implementation Practices for ISPs*, at 10 (2012), *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG5-Final-Report.pdf.

25. *See* PAUL MOCKAPETRIS, INFORMATION SCIENCES INSTITUTE, *Domain Names - Concepts and Facilities*, at 2–3 (1987), *available at* http://tools.ietf.org/html/rfc1034 (discussing purposes of the Domain Name System).

26. *DNSSEC Implementation Practices for ISPs*, *supra* note 24, at 17.

27. *See id.* at 10.

28. *See id.* at 17.

VeriSign, had upgraded to DNSSEC.[29] In domain name resolution, distinct roles are performed by root servers, ISP DNS servers, and Internet domains. A critical mass of all three types of operators is necessary for DNSSEC to function as intended. So far, only the root servers, some ISPs, and government servers have implemented DNSSEC, as there is no requirement to adopt it.[30] As of 2013, only Comcast has deployed DNSSEC in its subsidiary DNS servers,[31] and a paltry two percent of non-government domains run DNSSEC in the United States, reflecting the lack of incentive to do so.[32]

Another security standard that, if uniformly implemented, would strengthen the resiliency of the Internet is the Secure Border Gate Protocol ("BGP").[33] The insecure nature of the current BGP standard creates opportunities for malicious action by misconfiguring one BGP router to send out false information so as to capture or reroute private traffic as it travels over the Internet to a targeted server or group of IP addresses.[34] Other BGP routers will utilize that information to send traffic to the erroneous address.[35] The world saw this firsthand when Pakistan famously "took down YouTube" by configuring its BGP router to broadcast that it had the YouTube IP addresses within its network.[36] That information spread to other BGP routers, who started sending traffic intended for

---

29. Press Release, Dep't of Commerce, ICANN and VeriSign Deploy New Technology to Enhance the Security and Stability of the Internet (Jul. 16, 2010), *available at* http://www.commerce.gov/news/press-releases/2010/07/16/commerce-department-icann-and-verisign-deploy-new-technology-enhance-.

30. *DNSSEC Implementation Practices for ISPs*, *supra* note 24, at 17.

31. Jason Livingood, *Comcast Completes DNSSEC Deployment*, COMCAST VOICES (Jan. 10, 2012), http://blog.comcast.com/2012/01/comcast-completes-dnssec-deployment.html.

32. *Estimating IPv6 & DNSSEC Deployment Status*, NAT'L INST. OF STANDS. & TECH., http://usgv6-deploymon.antd.nist.gov/snap-all.html (last visited Nov. 17, 2012) (showing 2% of domains have DNSSEC operational, 1% are in progress, and 98% have no progress).

33. BGP is one way that servers route Internet packets through the network. CSRIC III WORKING GROUP 6, *Secure BGP Deployment*, 12 (2012), *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG6-Final-Report.pdf. By way of background, the Internet is a set of interconnected networks. Each major service provider has its own self-contained network, called an Autonomous System, which is a collection of IP addresses that all connect to the rest of the Internet through the service provider's "gates." *Id.* The ISP uses the Border Gate Protocol to control how traffic moves into and out of its network. *Id.* Each ISP chooses how its BGP routes traffic to its internal network according to a multitude of considerations, such as business relationships and the other Autonomous Networks to which the ISP connects. *Id.* Because of the great power these servers have in controlling Internet traffic, each ISP relies on and trusts each other ISP to implement their BGP routing policy in a truthful way, i.e. in a way that reasonably passes along traffic that does not terminate within its network. *Id.* This trust manifests in the fact that BGP routers blindly accept information from other BGP routers about what is on their networks. *Id.*

34. *Id.*

35. *Id.* at 12.

36. Martin A. Brown, *Pakistan Hijacks YouTube*, RENESYS (Feb. 24, 2008), http://www.renesys.com/blog/2008/02/pakistan-hijacks-youtube-1.

YouTube to Pakistan's servers.[37] Internet operators can remedy this misinformation relatively quickly; for example, in this case, network operators isolated Pakistan and fixed the routing tables within two hours.[38] A standard that cryptographically secures the designated path so malicious routers cannot alter the path of specific traffic within the packet could prevent this from happening again in the future.[39]

The examples above are just two of the innumerable security vulnerabilities that exist. To stem the abuse of these vulnerabilities, the National Institute of Standards and Technology recently developed a Cybersecurity Framework to help organizations secure critical infrastructure.[40] Implementing some of these suggestions could fix a portion of the security problems facing ISPs.[41]

These and other vulnerabilities have never been more important given the impending transition of our communications networks from the circuit-based Public Switched Telephone Network ("PSTN") to a flexible, all-IP network over which voice, video, and Internet traffic flow.[42] After this transition, communications that were once transmitted through separate networks, such as telephone and cable networks, will be transmitted through the Internet or using Internet Protocol, both of which are far more susceptible to cyber-attacks than the PSTN.[43] In contrast to the separate communications networks of the twentieth century, when there were only a small number of notable broadcast signal intrusion events and

---

37. *Id.*

38. *Id.*

39. *Id.*

40. *See* FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, *infra* note 66.

41. *Id.*

42. *See* AT&T, Petition to Launch a Proceeding Concerning the TDM-to-IP Transition at 2, FCC GN Docket No. 12-353 (rel. Dec. 18, 2012) [hereinafter AT&T IP Transition Petition], *available at* http://apps.fcc.gov/ecfs/document/view?id=7022086087 (quoting Connect America Fund, *Report and Order and Further Notice of Proposed Rulemaking*, FCC 11-161, 26 FCC Rcd. 17663, 17926 (2011)) (asking the FCC to "take the next steps to 'facilitate the transition' away from the legacy TDM-based network to an 'all-IP network' that is capable of supporting broadband Internet access, higher-layer VoIP, and other advanced communications services"); *see also* FCC, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN § 4.5 (2010), *available at* http://download.broadband.gov/plan/national-broadband-plan.pdf.

43. *See* Initial Comments of the National Association of State Utility Consumer Advocates at 18, AT&T Petition to Launch a Proceeding Concerning the TDM-to-IP Transition, FCC GN Docket No. 12-353 (rel. Jan. 28, 2013), *available at* http://apps.fcc.gov/ecfs/document/view?id=7022113102 (stating concerns about cybersecurity as a result of the transition); Reply Comments of the Computer & Communications Industry Association (CCIA) at 13, AT&T Petition to Launch a Proceeding Concerning the TDM-to-IP Transition, FCC GN Docket No. 12-353 (rel. Feb. 25, 2013), *available at* http://www.ccianet.org/wp-content/uploads/library/FCC%20Comments%20on%20Transition_to_IP_Networks.pdf (requesting that the FCC consider cybersecurity when proposing regulations on the transition).

communication disruptions,[44] the Internet has made it possible to communicate—or, in some cases, alter others' communications—throughout the world. This is a double-edged sword, as interconnection is essential in a networked world.[45] Governments recognize this and hack administrators of telecommunications networks to intercept the communications on those networks; while this has been used for surveillance, it could be also be used to disrupt communications.[46]

The Internet is built on the idea that packets may take many different paths to get from their source to their destination.[47] But this interconnectedness is also what makes the network vulnerable to cyber-attacks, as a failure or error in one system can propagate through the network.[48] Today, websites are routinely defaced, denial of service attacks prevent people from accessing the Internet,[49] and, significantly, it is easy to commandeer the Emergency Alert System.[50] Even though the distributed nature of the network provides some internal resilience, that resilience can be strained. If many networks or connections between networks are brought down in a cyber-attack, the remaining nodes on the Internet will have fewer routing options, which could cause a bottleneck that slows communications down or stops them completely.[51] Finally, if the routers and servers use the

---

44. *See, e.g.*, Alan Bellows, *Remember, Remember the 22nd of November*, DAMN INTERESTING (Jan. 9, 2007), http://www.damninteresting.com/?p=776 (detailing the Max Headroom broadcast signal intrusion event in Chicago on November 22, 1987 where an unknown person hijacked the signal of WGN-TV and WTTW to broadcast an impersonation of the character Max Headroom). The Max Headroom broadcast signal intrusion event is available on YouTube at http://www.youtube.com/watch?v=h5mzkt4N77s.

45. 47 U.S.C. § 251(a)(1); Kevin Werbach, *Off the Hook*, 95 CORNELL L. REV. 535, 588 (2010).

46. *Cf.* Ryan Gallagher & Peter Maass, *Inside the NSA's Secret Efforts to Hunt and Hack System Administrators*, THE INTERCEPT (Mar. 20, 2014), https://firstlook.org/theintercept/article/2014/03/20/inside-nsa-secret-efforts-hunt-hack-system-administrators/ (detailing NSA efforts to hack system administrators to gain access to the networks they administer). Indeed, the NSA disclosures show that the U.S. government has the ability to prevent a user from reaching websites. *See* THERE IS MORE THAN ONE WAY TO QUANTUM, NAT'L SEC. ADMIN., *available at* https://firstlook.org/theintercept/document/2014/03/12/one-way-quantum/ (describing QUANTUMSKY, an NSA technique that denies access to a webpage through RST packet spoofing).

47. *Id.*

48. *See* Brown, *supra* note 36 (describing the propagation of Pakistan's BGP problem); Randy Picker, *Cybersecurity: Of Heterogeneity and Autarky*, *in* THE LAW & ECONOMICS OF CYBERSECURITY 115, 124 (Mark F. Grady & Francesco Parisi eds., 2005).

49. Jeffrey L. Goldings, *Hackers Leave Their Mark on Websites*, 2 No. 8 QUINLAN, COMPUTER CRIME & TECH. IN LAW ENFORCEMENT art. 13, Aug. 2006.

50. *See Zombies? Emergency Broadcast System Hacked*, UPPERMICHIGANSSOURCE.COM, WLUC TV6 (Feb. 12, 2013), http://www.uppermichiganssource.com/news/story.aspx?id=859352#.

51. *See, e.g.*, Michael Lee, *The Largest DDoS Attack Didn't Break the Internet, but It Did Try*, ZDNET (Mar. 28, 2013), http://www.zdnet.com/the-largest-ddos-attack-didnt-break-the-internet-but-it-did-try-7000013225/ (discussing slow Internet speeds in Europe as a result of a recent cyber-attack).

same insecure standards, attacks can propagate through the whole network. This is the lens through which one must view FCC authority.

B. The FCC's Historical Role in Cybersecurity

The FCC has previously attempted to improve cybersecurity and the security of the communications grid. In these attempts, the FCC has expressed skepticism about whether market forces adequately incentivize ISPs to implement "measures to maintain the high-quality security, reliability and resiliency of their respective services."[52] Because the FCC has expertise in communications issues, other federal agencies expect it to comment on cybersecurity policy; this is evidenced by the FCC's substantial contribution to the White House 60-Day Cyberspace Policy Review.[53]

In the National Broadband Plan, the FCC discussed the need for improved cybersecurity in the telecommunications sector and potential methods of implementation.[54] Perhaps the most comprehensive and important work that the FCC has produced on cybersecurity has been through federal advisory committees.[55] In most circumstances, a federal advisory committee has solely an advisory role, with its recommendations not carrying the force of law.[56] One such committee was the Network Reliability and Infrastructure Council ("NRIC"). It developed a number of cybersecurity best practices and made a recommendation that private industry voluntarily implement these best practices.[57]

The successor to NRIC, is the Communications Security, Reliability and Interoperability Council ("CSRIC"). It focuses on strengthening cybersecurity, ensuring availability of communications networks during an emergency or disaster, and developing procedures that communications providers can take to improve cybersecurity.[58] CSRIC has made significant recommendations on ways to improve cybersecurity at the network level.

---

52. *See* VoIP Outage Reporting NPRM, *supra* note 9, at para. 20.

53. Cyber Sec. Certification Program, *Notice of Inquiry*, FCC 10-63, para. 5, (2010) [hereinafter Cyber Sec. Certification Program NOI], *available at* http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-10-63A1.pdf; WHITE HOUSE, CYBERSPACE POLICY REVIEW, at 4 (2009) [hereinafter CYBERSPACE POLICY REVIEW], *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (discussing U.S. Government cybersecurity initiatives).

54. *See National Broadband Plan*, supra note 42, § 16.2.

55. A federal agency can convene advisory committees that consist of private sector experts for the purpose of advising the agency. *See* 5 U.S.C. app. 2 § 2 (2006).

56. *See id.* at § 2(b). This is the case for the FCC advisory committees discussed here.

57. *See* Cyber Sec. Certification Program NOI, *supra* note 53, at paras. 6-7.

58. *See Charter of Network Reliability and Interoperability Council* at 1, *available at* http://transition.fcc.gov/hspc/NRIC_recharter.pdf (last accessed on Nov. 15, 2012); *Charter of the FCC's Communications Security, Reliability, and Interoperability Council*, at 1 [hereinafter *CSRIC Charter*], *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC%20Charter%20Renewal%202011%20FINAL.pdf (last accessed on Nov. 15, 2012).

Like NRIC, however, the Council is purely advisory, so it lacks the authority to require the FCC or private industry to follow its recommendations.[59]

CSRIC III [60] issued recommendations for voluntary industry guidelines to combat three major cybersecurity threats, including botnets, attacks on the Domain Name System, and Internet route hijacking through the use of the insecure Border Gate Protocol. [61] These security vulnerabilities are particularly important, as attacks on these systems could cause widespread access problems for certain parts of the Internet.[62]

However, CSRIC's guidelines are voluntary, so the major ISPs pledging to implement them serve only fifty percent of residential broadband users. [63] There are currently no mandatory cybersecurity standards for our nation's private telecommunications networks.

One promising recent development is an Executive Order entitled *Improving Critical Infrastructure Cybersecurity*.[64] It mandated that the National Institute of Standards and Technology and the Department of Homeland Security ("DHS") create a set of standards and procedures that align policy, business, and technological approaches to address cyber-threats to all sectors of the nation's critical infrastructure, including the nation-wide communications infrastructure.[65] NIST released Cybersecurity Framework Version 1.0 on February 12, 2014.[66] As a methodology, the Framework does not require organizations to implement specific standards to improve cybersecurity.[67] Instead, NIST suggests that organizations use

---

59. *See* 5 U.S.C. app. 2 § 2; *CSRIC Charter*, *supra* note 58, at 1.

60. CSRIC III is the third authorization of the federal advisory committee.

61. Press Release, FCC, FCC Advisory Committee Adopts Recommendations to Minimize Three Major Cyber Threats, 2012 WL 983082, at *2 (Mar. 22, 2012), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-313158A1.pdf.

62. I do not discuss the Anti-Botnet Code of Conduct. Botnets can perform distributed denial of service attacks on a website or computer connected to the Internet. However, the solutions proposed by CSRIC III to combat botnets are not technical, but instead rely on user education and notification, and as such do not lend themselves to standardization. *See* CSRIC III WORKING GROUP 7, *Final Report: U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs)*, at 3 (Mar. 2012), *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf; *see also* T. Luis de Guzman, Comment, *Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges*, 59 CATH. U. L. REV. 527, 528–29 (2010).

63. CSRIC Press Release, *supra* note 61, at *2.

64. *Improving Critical Infrastructure Cybersecurity*, Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013) [hereinafter Cybersecurity Executive Order].

65. *Id.* at 11,741.

66. FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, VERSION 1.0, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, February 12, 2014, *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

67. The Framework does contain "Informative References," which are "specific sections of standards, guidelines, and practices common among critical infrastructure sectors

the Framework to identify opportunities to strengthen and communicate their management of cybersecurity risk while aligning with industry practices.[68]

The most recent incarnation of the Communications Security, Reliability, and Interoperability Council, CSRIC IV, is currently working to evaluate CSRIC's most critical existing cybersecurity best practices and determine how best to improve them to account for changes in cybersecurity practice and the threat landscape.[69] It will then harmonize and update these best practices with the NIST Cybersecurity Framework.[70] However, as noted above and discussed in detail in Part VI below, firms currently have no incentive other than market pressure to upgrade the cybersecurity of the Internet. Even with the NIST Cybersecurity Framework and CSRIC's best practices as guides, mandating that ISPs implement them would bring the FCC into new territory, as the Internet is outside of the FCC's traditional regulatory role.

C. The FCC's Jurisdiction over the Internet

The FCC's power to regulate communications activities is quite broad. For example, Title I of the Communications Act of 1934 gives the FCC jurisdiction over "all interstate and foreign communication by wire or radio and all interstate and foreign transmission of energy by radio."[71] The 1934 Act enumerates specific responsibilities and powers with respect to common carriers and wire communication (Title II)[72] and radio wave transmissions (Title III);[73] Congress gave the FCC jurisdiction over cable service in 1984 (Title VI).[74]

These statutes mandate FCC oversight and promotion of specific communications services. For example, the FCC oversees common carriers,[75] ensures interconnection between telecommunications carriers,[76] promulgates rules to ensure 9-1-1 service,[77] and promotes diversity of

---

that illustrate a method to achieve" certain security outcomes. However, these are illustrative and not exhaustive. *See id.* at 8.

68. *Id.* at 4.

69. CSRIC IV - Working Group 4: Cybersecurity Best Practices Status Update, March 20, 2014 at 5, *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC_IV_WG4_STATUS_03202014.pdf.

70. *Id.*

71. Communications Act of 1934, ch. 652, § 2, 48 Stat. 1064 (codified as amended at 47 U.S.C. § 152(a) (2006)).

72. *Id.* § 201 (codified as amended at 47 U.S.C. § 201 (2006)).

73. *Id.* § 301 (codified as amended at 47 U.S.C. § 301 (2006)).

74. Cable Communications Policy Act of 1984, Pub. L. No. 98–549, 98 Stat. 2779 (1984) (codified at scattered sections 47 U.S.C.). This statute was enacted after the FCC successfully asserted its jurisdiction over cable services in the 1960s. *See* United States v. Southwestern Cable Co., 392 U.S. 157 (1968), *infra* note 99 and accompanying text.

75. *See* 47 U.S.C. §§ 201-231 (2006).

76. *See* 47 U.S.C. § 251 (2006).

77. 47 U.S.C. § 615a-1 (2006).

information sources and services provided in cable communications.[78] Furthermore, the FCC's general purpose is to regulate "interstate and foreign commerce in communication by wire and radio so as to make available . . . a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of the national defense [and] promoting safety of life and property."[79] However, the FCC's enabling statutes do not confer upon it direct authority over the Internet.[80]

The character of the regulation the FCC can promulgate depends heavily on the type of service regulated, as evidenced by the demarcation between the different titles of the FCC's enabling statutes. One of the FCC's primary areas of authority throughout the twentieth century was the regulation of the Public Switched Telephone Network ("PSTN"), which AT&T provided as a common carrier.[81] In the 1970s, "enhanced" services such as data transmission became available.[82] The FCC did not have direct authority over enhanced services, as they differed from basic telephone service.[83] The statutory distinction between "telecommunications service" and "information service" reflects the historical distinction between basic and enhanced services, and maintains the practice restricting FCC direct authority to telecommunications services.[84]

The Telecommunications Act of 1996 defines a telecommunications service as the "offering of telecommunications for a fee directly to the public . . . regardless of the facilities used."[85] The FCC must treat telecommunications carriers as common carriers "only to the extent that [they] . . . engage[] in providing telecommunications services."[86] In contrast, an information service is one that offers the "capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and

78. *See* 47 U.S.C. § 521 (2006) (FCC mandated to assure that cable communications provide and are encouraged to provide the widest possible diversity of information sources and services to the public).

79. 47 U.S.C. § 151 (2006).

80. *But see* 47 U.S.C. § 230(b) (stating broad policy statements about the Internet and immunizing ISPs from liability for content they did not create); 47 U.S.C. § 1302(b) (requiring the FCC to promote broadband deployment under certain circumstances).

81. *See* United States v. AT&T, 552 F. Supp. 131, 178 (D.D.C. 1982), *aff'd sub nom.,* Maryland v. United States, 460 U.S. 1001 (1983) (discussing AT&T's business in the last half of the twentieth century).

82. *See* Computer & Commc'ns Indus. Ass'n v. FCC, 693 F.2d 198, 203–06 (D.C. Cir. 1982) (*CCIA v. FCC*).

83. *Id.* at 207.

84. *See* Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 996 (2005).

85. Telecommunications Act of 1996, Pub. L. No. 104-104, § 101(a), 110 Stat. 56 (1996) (codified at 47 U.S.C. § 153(53) (2006)).

86. *Id.* § 3 (codified at 47 U.S.C. § 153(51) (2006)). The FCC wields substantial authority over the practices of telecommunications carriers because they are regulated as common carriers. *See generally* 47 U.S.C. §§ 201-231.

includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service."[87] There are no corresponding common carriage or regulatory requirements for information services.[88]

In a series of rulemakings conducted in the early 2000s, the FCC classified broadband services as information services, thereby precluding the agency from regulating broadband service as a common carrier.[89] The information service classification includes cable broadband service,[90] wireless broadband service,[91] wireline broadband service,[92] and broadband service over power lines.[93] The FCC makes a delicate distinction between the services that an ISP provides, ultimately concluding that ISPs provide a connection to the Internet "via telecommunications."[94] This formulation indicates that the FCC cannot use its traditional Title II regulatory tools to regulate broadband.[95]

D. The FCC's Ancillary Authority

Because broadband ISPs provide information services, the FCC's ability to place regulatory obligations on ISPs is limited. The FCC can regulate an information service, however, if the information service impacts another service the FCC is empowered to regulate by statute. This is known as the FCC's ancillary authority.[96] The Communications Act of 1934 authorized the FCC to "perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as

87. Communications Act of 1934, ch. 652, § 153(20), 48 Stat. 1064 (codified as amended at 47 U.S.C. § 153(24) (2006)).

88. *See* Verizon v. FCC, 740 F.3d 623, 649–51 (D.C. Cir. 2014).

89. *Id.*

90. Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 986–87 (2005); *see generally* High-Speed Access to the Internet Over Cable and Other Facilities, *Declaratory Ruling and Notice of Proposed Rulemaking*, FCC 02-77 (2002) [hereinafter Cable Broadband Ruling].

91. Appropriate Regulatory Treatment for Broadband Access to the Internet over Wireless Networks, *Declaratory Ruling*, FCC 07-30, paras. 22, 29 (2007) [hereinafter Wireless Broadband Ruling].

92. Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, *Report and Order and Notice of Proposed Rulemaking*, FCC 05-150, paras. 15, 103–04 (2005) [hereinafter Wireline Broadband Report and Order], *aff'd sub nom.,* Time Warner Telecom, Inc. v. FCC, 507 F.3d 205 (3d Cir. 2007).

93. Classification of Broadband over Power Line Internet Access Service as an Information Service, *Memorandum Opinion and Order*, FCC 06-165, paras. 9, 12 (2006).

94. Cable Broadband Ruling, *supra* note 90, at para. 41. This distinction contrasts with another possible interpretation, that broadband service itself is actually providing telecommunications.

95. *See* 47 U.S.C. §153(20); Verizon v. FCC, 740 F.3d 623, 649–51 (D.C. Cir. 2014).

96. *See* Comcast Corp. v. FCC, 600 F.3d 642, 646–47 (D.C. Cir. 2010); *see generally id.* (giving a summary of the early Supreme Court ancillary authority rulings).

may be necessary in the execution of its functions."[97] The Supreme Court has interpreted this authority to allow the FCC to take actions that further its statutory mandate, even if not expressly contemplated by a statute.[98] The purpose of this penumbra of authority surrounding the FCC's statutorily conferred power is to allow the FCC to adapt government telecommunications policy to new technology in a more efficient and flexible way than Congress could.[99]

Ancillary authority has been used most prominently to regulate communications services over which the FCC does not have an explicit grant of authority, but that nevertheless affect services that the FCC regulates. The Court's treatment of cable television in *United States v. Southwestern Cable Co.*[100] provides an example of the FCC's lawful regulation of a technology that did not exist when the Communications Act of 1934 was enacted, but that had the potential to disrupt the broadcast television market—over which the FCC has a mandate.[101] The Court stated that the characteristics of the new service are relevant only to determine whether it satisfies the FCC's general jurisdictional grant, which includes interstate communication by radio or wire, as a prerequisite to jurisdiction.[102] After this threshold is satisfied, a reviewing court then looks to the impact the new service has on existing regulated services.[103] If the new service could prevent the FCC from achieving statutory goals associated with the established service, then a court looks to how the proposed regulation fits into the Commission's current rules.[104]

The D.C. Circuit, in *American Library Association v. FCC*,[105] issued the pronouncement on FCC ancillary authority that governs to this day.[106] To use its ancillary authority as a basis for a regulation, the FCC must satisfy two requirements. First, the FCC's "general jurisdictional grant" under Title I must cover the regulated subject.[107] Second, the regulations must be reasonably ancillary to the FCC's effective performance of its statutorily mandated responsibilities.[108]

---

97. Communications Act of 1934, ch. 652, § 4(i), 48 Stat. 1066 (codified at 47 U.S.C. § 154(i) (2006)).

98. United States v. Midwest Video Corp. (*Midwest I*) 406 U.S. 649, 669-70 (1972) (plurality opinion).

99. *See* United States v. Southwestern Cable Co., 392 U.S. 157, 172 (1968) (quoting FCC v. Pottsville Broad. Co., 309 U.S. 134, 138 (1940)).

100. *See id.* at 172.

101. *Id.*

102. *See Midwest I*, 406 U.S. at 659-60; *see also* Werbach, *supra* note 45, at 580.

103. *See Southwestern Cable*, 392 U.S. at 174–78.

104. *See id.* at 178-79; *see also* Werbach, *supra* note 102, at 580.

105. Am. Library Ass'n v. FCC, 406 F.3d 689, 691-92 (D.C. Cir. 2005).

106. *Id.*

107. *Id.*

108. *Id.* Stated another way, the regulation at issue should be "imperative if [the FCC] is to perform with appropriate effectiveness . . . its other responsibilities." *Southwestern Cable*, 392 U.S. at 173.

Regarding the first requirement, the FCC's general jurisdictional grant is broad, encompassing authority over "all interstate and foreign communication by wire or radio."[109] Even where a communication emanates from and is received within the same state, it falls within the reach of Title I insofar as it is part of a broader national network.[110] Accordingly, the FCC's Title I general jurisdiction likely includes the provision of communications services over the Internet such as broadband Internet access.[111]

The second requirement, that the regulations must be reasonably ancillary to the FCC's effective performance of its statutorily mandated responsibilities, is more difficult to satisfy. A court evaluates the permissibility of each new exercise of ancillary authority on its own terms.[112] That is, the FCC cannot justify a new use of ancillary authority by reference to previous incarnations of this authority.[113]

For example, in the seminal ancillary authority case, *Southwestern Cable*, the Supreme Court analyzed the FCC regulations over community antenna television ("CATV"), a service known today as cable television.[114] When the Court heard the case in 1968, Congress had not afforded the FCC express authority over CATV, but Congress had mandated that the Commission ensure "a widely dispersed radio and television service, with a fair, efficient, and equitable distribution of service among the several States and communities."[115] The FCC reasonably concluded that CATV could "'destroy or seriously degrade the service offered by a television broadcaster, and thus ultimately deprive the public of the various benefits of a system of local broadcasting stations."[116] Accordingly, because CATV posed a threat to a service that Congress required the FCC to keep operational, the FCC's exercise of its ancillary authority to promulgate CATV regulations was upheld as valid.

---

109. *See* 47 U.S.C. § 152 (2006).

110. *See Southwestern Cable*, 392 U.S. at 168–69 (stating that intrastate broadcasting and cablecasting still fall within the FCC's Title I authority because they consist of programming devised for and distributed to a national audience).

111. That neither the FCC nor Comcast disputed the validity of broadband falling with the Commission's Title I grant tilts heavily toward this conclusion. However, because the court reversed the FCC on other grounds, this issue has not been conclusively decided. *See Comcast*, 600 F.3d at 646–47 (stating that "Comcast concedes that the Commission's action here [regulating broadband Internet] satisfies the first requirement because the company's Internet service qualifies as 'interstate and foreign communication by wire' within the meaning of Title I of the Communications Act") (citation omitted).

112. *Id.* at 650; *see Midwest Video I*, 406 U.S. at 669–70 (plurality opinion).

113. Comcast Corp. v. FCC, 600 F.3d 642, 650 (D.C. Cir. 2010).

114. *Evolution of Cable Television*, FCC ENCYCLOPEDIA (2012), http://www.fcc.gov/encyclopedia/evolution-cable-television.

115. *Southwestern Cable*, 392 U.S. at 174–76 (internal quotation marks and citations omitted); *see* 47 U.S.C. § 307(b).

116. *Southwestern Cable*, 395 U.S. at 175–76 (quoting Grant of Authorizations in the Bus. Radio Serv. for Microwave Stations to Relay Television Signals to Cmty. Antenna Sys., *First Report and Order*, Dkt. No. 14895, 38 F.C.C. 683, 699–700 (1965)).

Conversely, in *Echostar Satellite, LLC v. FCC*,[117] the D.C. Circuit held that the FCC could not exercise ancillary authority over satellite television encoding, as the Commission could not show that satellite television encoding was preventing the Commission from fulfilling its statutory responsibilities.[118] At issue was a congressional mandate to promote the commercial availability of cable set-top boxes.[119] The *Echostar* court rejected the FCC's assertion that the requirements for satellite providers promoted the statutory mandate to make cable set-top boxes commercially available.[120] Unlike *Southwestern Cable*, wherein the FCC found that CATV directly threatened its statutory mandate over broadcast television, the FCC showed no such connection in *Echostar*. The court noted that the only link between the satellite providers and the statute was a memorandum of understanding between the FCC and cable providers setting out the cable industry's commitment to future adoption of standards to promote competitive set-top boxes, and conditioned on the FCC requiring satellite MVPDs to adopt the same standard.[121]

Further adding to the body of ancillary authority jurisprudence, the D.C. Circuit clarified in *Comcast v. FCC*[122] that the FCC cannot rely on congressional statements of policy alone to support exercises of ancillary authority.[123] The FCC must instead rely on express congressional delegations of authority in the text of Titles II, III, and VI of the Act.[124] This confines the FCC's power to explicit statutory authorities, as opposed to broad assertions of policy that would potentially give the FCC unrestrained power in furtherance of those policy goals.[125] While this restraint on ancillary authority makes sense, on its face it prevents the FCC from regulating in ways that further the goals of Congress when changes in technology move faster than legislation.

117. Echostar Satellite, LLC v. FCC, 704 F.3d 992, 999 (D.C. Cir. 2013).
118. *Id.* at 998–1000.
119. *Id.* at 997–98; *see* 47 U.S.C. § 549(a) (Cable set-top boxes are termed "navigation devices.").
120. *Echostar Satellite*, 704 F.3d at 997–98.
121. *Id.* This memorandum of understanding was not agreed to by satellite MVPDs but imposed conditions on them through FCC rules.
122 . Comcast Corp. v. FCC, 600 F.3d 642 (D.C. Cir. 2010).
123. *See id.* at 653–54; Nat'l Ass'n of Regulatory Util. Comm'rs v. FCC (*NARUC I*), 533 F.2d 601, 612 (D.C. Cir. 1976). For an exhaustive discussion of pre-*Comcast* ancillary authority jurisprudence, *see* Werbach, *supra* note 102, at 571-77.
124. *Comcast*, 600 F.3d at 654 (internal quotation marks omitted).
125. *Id.* at 655–56.

E. The FCC's Authority in the Context of Rapid Technological Change

The FCC's ancillary authority is set against the backdrop of technological change.[126] Increasingly, our communications are conducted through the Internet, with the eventual goal of having an all-IP communications system.[127] One of the consequences of this transition to a new communications architecture is that it incentivizes telecommunications companies to shut down the old copper telephone network to avoid duplicative costs.[128] If a current telephone service provider shuts down its copper PSTN network and transfers all of the telephone traffic over IP links, the FCC could lose its authority to regulate the network via its Title II jurisdiction.[129] As the communications network transitions to Internet Protocol, the network consequently becomes more vulnerable to cyber-attacks and potentially more isolated from FCC authority.[130]

Because of the intertwining of an all-IP network and cybersecurity, securing Internet infrastructure poses questions about the scope of the FCC's authority over it. Recent D.C. Circuit decisions and FCC orders make it clear that if the FCC has authority to require that cybersecurity best practices be followed, that regulation must be grounded in some positive grant of statutory authority.

---

126. *See* United States v. Southwestern Cable Co., 392 U.S. 157, 174–76 (1968) (approving of ancillary authority over a potentially disruptive new technology).

127. *See* Part II.A *supra* notes 42 and 43 and accompanying text (discussing the transition away from the copper PSTN to platform agnostic internetworking to transport voice, video, and data communications); *see also* PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE, NETWORK SECURITY VULNERABILITY ASSESSMENTS TASK FORCE REPORT (Mar. 2002) [hereinafter NSVASTF REPORT], *available at* https://www.hsdl.org/?view&did=1540; Werbach, *supra* note 102, at 588.

128. Sean Buckley, *PSTN-to-IP Migration Must Be Done with Care, Say Verizon, AT&T*, FIERCETELECOM (May 15, 2012), http://www.fiercetelecom.com/story/pstn-ip-migration-must-be-done-care-say-verizon-att/2012-05-15; *see also* AT&T Petition to Launch Proceeding Concerning The TDM-to-IP Transition, WC Docket No. 12-353 (2012).

129. *See* Part II, *supra* notes 22-24; *see generally* Kevin Werbach, *No Dialtone: The End of the Public Switched Telephone Network*, 66 FED. COMM. L.J. 203, 234–61 (2014) (noting that many regulatory requirements for the PSTN do not hold after the IP transition, and making recommendations for which aspects of the PSTN should carry over to the new IP network, including universal service and reliability in this recommendation).

130. NSVASTF REPORT, *supra* note 127; Werbach, *supra* note 102, at 588. This becomes more clear as people increasingly use Internet services as their primary method of communication. *See* Outage Reporting to Interconnected Voice over Internet Protocol Serv. Providers, *Report and Order*, FCC 12-22, para. 2 (2012) [hereinafter VoIP Outage Order] (noting that about 27 million people had VoIP residential telephone subscriptions as of December 31, 2010); Cablevision Sys. Corp. v. FCC, 597 F.3d 1306, 1323 (D.C. Cir. 2010); Buckley, *supra* note 128.

III. THE FCC'S ANCILLARY AUTHORITY TO PROMULGATE CYBERSECURITY STANDARDS

There has been little discussion of the FCC's authority to create cybersecurity standards. In the realm of cybersecurity, authors have acknowledged that today's hodgepodge method of trying to ensure network infrastructure security is not working.[131] Members of Congress have introduced numerous bills to promote cybersecurity.[132] As evidenced by the introduction of these bills and the history of cybersecurity regulatory attempts, it is currently unclear which agency should be taking the lead. Furthermore, fear of regulation has foreclosed discussions of private industry regulation.[133] This Note shows a possible solution to this problem of insufficient cybersecurity by detailing a basis of FCC authority to require ISP implementation of cybersecurity best practices that result in increased reliability.

Evidence that poor cybersecurity impedes the actualization of statutory obligations would support the FCC's authority to create cybersecurity standards for ISPs. Because of the impact that cyber-attacks can have on the national communication infrastructure, the FCC could take regulatory action to prevent the disruption of those networks. As a federal agency, the FCC would first have to consider avenues of direct authority; however, the Communications Act does not directly authorize the FCC to implement cybersecurity regulations.[134] The Commission would therefore have to rely on its ancillary authority to implement any such regulations.

The ability of the FCC to exercise its ancillary authority depends on whether: (1) the service to be regulated falls within the FCC's Title I grant;

---

131. Karson K. Thompson, Note, *Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate*, 90 TEX. L. REV. 465, 491 (2011) (stating that cybersecurity policy must be uniform and come from the top down because this structure eliminates the problems inherent in asking individual agencies to develop their own security strategies, such as a lack of uniformity and consistency). Other commenters assert that problems with cybersecurity manifest primarily in stolen data and not in problems with communications reliability. *See* Peter M. Shane, *Cybersecurity: Toward a Meaningful Policy Framework*, 90 TEX. L. REV. 87, 87 (2012). While many cyber-attacks result in a loss of data, the same methods that are used to compromise the network to steal the information can be used to disrupt the network. *Id.*

132. *See, e.g.*, Cybersecurity Enhancement Act of 2013, H.R. 756, 113th Cong. (2013); Cybersecurity and Internet Safety Standards Act, S. 372, 112th Cong. (2011); Homeland Security Cyber and Physical Infrastructure Protection Act of 2011, H.R. 174, 112th Cong. (2011); *see also* Thompson, *supra* note 131, at 482-88 (discussing seven cybersecurity proposals in the 112th Congress).

133. *See* Shane, *supra* note 131, at 91.

134. *See generally* 47 U.S.C. §§ 151-1473; *see also supra* text accompanying notes 90-93 (discussing FCC authority over broadband Internet).

and (2) the regulations are reasonably ancillary to the effective performance of a statutory mandate.[135]

A. *Broadband Internet Service as Within the FCC's General Jurisdictional Grant*

The FCC's general jurisdictional grant under Title I likely covers cyber-attacks and corresponding regulation of broadband Internet if these attacks are transmitted over an interstate all-IP communications network.[136] Title I gives the Commission jurisdiction over "interstate . . . communication by wire or radio."[137] Cybersecurity, or the lack thereof, affects both interstate communications by radio or wire and the Internet as a national network. The Supreme Court in *Southwestern Cable* set a low threshold for a service to fall within the Commission's Title I authority.[138] There, the Court found that cable systems carry programming made for a national audience, and so constituted interstate communications.[139] Today, Internet traffic has a worldwide reach; even if it is within an autonomous network, Internet traffic likely travels across state lines.[140] Furthermore, the general content of the traffic could be intended for a national audience. Cyber-attacks, in particular, have interstate and international character.[141] In a recent cyber-threat analysis, Mandiant, an information technology security company, found 115 instances of attacks originating from China from 2006 to 2012. [142] Because of the interstate and international characteristics of Internet traffic and disruptions, cybersecurity regulations fall within the FCC's Title I jurisdiction.

B. *Mandatory Cybersecurity Standards for ISPs as Reasonably Ancillary to the FCC's Statutory Responsibilities*

The creation of cybersecurity standards is reasonably related to the FCC's effective performance of its statutorily mandated responsibilities.[143] In the past, courts have upheld FCC assertions of ancillary authority when the regulated technology affected communications networks such as

---

135. Am. Library Ass'n v. FCC, 406 F.3d 689, 691–92 (D.C. Cir. 2005).
136. *See* 47 U.S.C. § 152 (2006); *see also* VoIP Outage Order, *supra* note 130, at paras. 60-61.
137. 47 U.S.C. § 152 (2006).
138. United States v. Southwestern Cable Co., 392 U.S. 157, 175–76 (1968).
139. *Id.*
140. *See* CSRIC III WORKING GROUP 6, SECURE BGP DEPLOYMENT 12 (Mar. 2012), *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG6-Final-Report.pdf.
141. *See, e.g.*, MANDIANT REPORT, *supra* note 15, at 22.
142. *Id.* These intercontinental attacks necessitate the utilization of interstate communication. *See id.* at 21.
143. *See* Am. Library. Assoc. v. FCC, 406 F.3d 689, 691–92 (D.C. Cir. 2005).

broadcast television and the telephone network.[144] For example, in *Southwestern Cable*, the order at issue was designed to remedy aspects of CATV, a new technology that had the potential to frustrate FCC obligations to ensure the continued viability of the broadcast television medium.[145]

Title 47 of the United States Code obligates the FCC to perform myriad other functions, including the creation of regulations for common carriers, rules for interconnection between telecommunications carriers, rules to ensure 9-1-1 services, and regulations to promote diversity of information sources and services provided in cable communications.[146] Furthermore, the FCC has a general obligation to make available "a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of the national defense [and] promoting safety of life and property."[147] These are some of the core functions of the FCC. But a transition from a Title II to a Title I classification of the nation's communications system jeopardizes core FCC regulatory powers that exist only in Title II. If the FCC cannot exercise its Title II authority over the U.S. communications network, it must turn to ancillary authority, relying on the fact that an all-IP network without adequate cybersecurity safeguards could have disastrous effects on critical telecommunications and emergency services.[148]

These attacks have the potential to impair vital communications that the FCC oversees, such as telephony, Multichannel Video Programming Distributor ("MVPD") services,[149] and 9-1-1 functionality. FCC regulations requiring uniform implementation of cybersecurity best practices and updated network standards, such as those proposed by IETF and CSRIC, could mitigate the negative effects of these attacks on communications.[150]

Regulations aimed at ensuring the continuity of a communications service were examined in one of the seminal ancillary authority cases.[151] In *Southwestern Cable*, the Supreme Court upheld the FCC's exercise of ancillary authority because of CATV's potential to disrupt the broadcast television market.[152] Similarly, because of the possibility of communications disruption through the Internet, FCC mandatory cybersecurity standards are also reasonably ancillary to the FCC's effective

144. *See* United States v. Southwestern Cable Co., 392 U.S. 157, 174–76 (1968); CCIA v. FCC, 693 F.2d 192, 210 (D.C. Cir. 1982).
145. *See Southwestern Cable*, 392 U.S. at 175.
146. *See* Part II.D, *supra* notes 75-79.
147. 47 U.S.C. § 151 (2006).
148. NSVASTF REPORT, *supra* note 127, at 65–66; *see, e.g.*, *See Zombies? Emergency Broadcast System Hacked*, *supra* note 50; Lee, *supra* note 51.
149. An MVPD is a cable, satellite, or IP-based service provider that distributes video programming. *See* 47 U.S.C. § 522(13).
150. *See supra* Part II.B.
151. *See* United States v. Southwestern Cable Co., 392 U.S. 157, 174–76 (1968).
152. *See id.*

performance of its statutorily mandated responsibilities of overseeing telephony, MVPD service, and 9-1-1 service. Furthermore, these attacks affect the FCC's general obligation to make available "a rapid, efficient, Nation-wide . . . wire and radio communication service," [153] where Congress has further required the FCC to make certain services available to the public, such as 9-1-1 service and broadband Internet. This is not to say that the FCC can regulate any communications platform at risk of a cyber-attack. The FCC would only be able to regulate the security of ISPs insofar as that insecurity poses a threat to the viability of functions the FCC is required to maintain.

Beyond interconnection and general network reliability, the FCC has a duty to promulgate regulations that ensure that Voice over Internet Protocol ("VoIP") providers give their users access to 9-1-1 service on parity with PSTN providers.[154] In doing so, the FCC can "take into account any technical, network security, or information privacy requirements that are specific to IP-enabled voice services."[155] Because cyber-attacks could disrupt 9-1-1 service on VoIP connections, requiring cybersecurity improvements is reasonably ancillary to the FCC's performance of its statutory obligations.

This situation does not suffer from the lack of a connection between the regulation and the service to be regulated seen in *Echostar*, where the FCC artificially conflated satellite service regulations with cable industry dealings.[156] The cyber-threats to the telecommunications networks are real; they were not created through jurisdictional bootstrapping.[157] Here, the FCC has ample evidence to support a finding that cyber-attacks could create a real obstacle to enforcement of its statutory obligation to ensure an efficient and reliable telecommunications network.

Since the FCC's inception, it has been obligated to ensure the efficiency of the nation's communications network.[158] Courts have consistently acknowledged that, as new technologies appear, the FCC must adapt.[159] And never before has the ability to disrupt our communications

153. 47 U.S.C. § 151 (2006).

154. 47 U.S.C. § 615a-1 (2006).

155. *Id.* This phrase represents an acknowledgement by Congress of the special security considerations that are necessary when transitioning to an all-IP communications infrastructure.

156. *See* Echostar Satellite, LLC v. FCC, 704 F.3d 992, 997-99 (D.C. Cir. 2013).

157. *See* Part II.D *infra*.

158. *See* 47 U.S.C. § 151 (2006).

159. *See, e.g.*, United States v. Southwestern Cable, 392 U.S. 157, 175–77 (1968) (noting that "Congress could not in 1934 have foreseen the development of community antenna television systems, but it seems to us that it was precisely because Congress wished 'to maintain, through appropriate administrative control, a grip on the dynamic aspects of radio transmission,' that it conferred upon the Commission a 'unified jurisdiction' and 'broad authority.' Thus, '(u)nderlying the whole (Communications Act) is recognition of the rapidly fluctuating factors characteristic of the evolution of broadcasting and of the

networks been so widely available.[160] Therefore, mandating standards is likely ancillary to the FCC's statutory responsibilities, and the FCC may use its ancillary authority to promulgate rules accordingly.

IV. THE DECISION TO REGULATE CYBERSECURITY OF INTERNET SERVICE PROVIDERS

Having concluded that the FCC likely has authority to regulate the cybersecurity practices of ISPs under its Title I ancillary authority, the question remains whether the FCC should exercise this authority. The FCC is the unifying authority for telecommunications regulation,[161] a status that reflects the belief that an administrative agency can adapt its regulations to changes in technology more quickly than Congress.[162] The FCC's relative nimbleness suggests that the FCC should play a role in cybersecurity. This has already been recognized to an extent in the the Presidential Policy Directive accompanying the Cybersecurity Executive Order, where the FCC is charged with coordinating with the communications sector in developing and implementing the Cybersecurity Framework.[163] It has superior institutional competence regarding communications networks in addition to its longstanding relationship with companies in the telecommunications industry. As more people and communications technologies use the Internet as their sole communications network, the FCC's obligations to ensure a reliable communications network will increasingly intrude on the Internet domain.

The FCC already has a good model for what cybersecurity standards should look like. CSRIC recommendations and finalized IETF security standards provide a trusted way of determining the standard with expertise.[164] Furthermore, the Cybersecurity Executive Order tasks NIST and DHS, with input from the FCC, with creating a Cybersecurity

---

corresponding requirement that the administrative process possess sufficient flexibility to adjust itself to these factors." (citations omitted)).

160. *See* NSVASTF REPORT, *supra* note 148, at 4, and accompanying text.

161. *Southwestern Cable*, 392 U.S. at 168.

162. *Id.* at 172-73.

163. Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience, Feb. 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (directing the FCC to "exercise its authority and expertise to partner with DHS and the Department of State, as well as other Federal departments and agencies and SSAs as appropriate, on: (1) identifying and prioritizing communications infrastructure; (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and (3) working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends").

164. *See* CSRIC Press Release, *supra* note 61, at *2; Bush, *supra* note 38.

Framework for the private sector to implement.[165] The implementation of the Framework could improve cybersecurity as well. With these resources in mind, this section of the Note addresses whether the FCC should regulate the cybersecurity of ISPs.

Deciding whether and how to regulate can be a hard choice for agencies to make, especially given the wide discretion they are afforded. The calculus involves two separate inquiries. Initially, the agency must decide whether to regulate, which involves an evaluation of agency goals and the problem the agency seeks to address, along with a determination of whether the problem lends itself to a regulatory fix.[166] After determining that regulatory action is appropriate, the agency must analyze the costs and benefits of different regulatory alternatives and choose the best one.[167]

This Part's analysis first focuses on resolving the dilemma of whether the FCC should regulate ISPs' cybersecurity practices in the first place. The contrasting options are relatively straightforward: impose regulation that will result in basic infrastructure cybersecurity protections or choose not to regulate and instead let the market provide the level of protection its participants deem necessary. This Part then briefly considers the basic cost-benefit analysis and offers recommendations on how to apply that analysis to the problem of protecting network infrastructure from cyber-attacks.

A. Deciding When to Regulate

1. Appropriate Considerations for Deciding When to Regulate

In 2003, the Office of Management and Budget issued a circular to help guide agency decisions of whether and how to regulate.[168] It recognized that good regulatory analysis requires justifications of the need for the proposed action.[169] This Part's description of the initial determination of whether to regulate borrows heavily from the circular.

---

165. Cybersecurity Executive Order, *supra* note 64, at 11,739-41.

166. *See* OFFICE OF MGMT. & BUDGET, CIRCULAR A-4: A REGULATORY ANALYSIS, at 3–5 (2003) [hereinafter Circular A-4], *available at* www.whitehouse.gov/sites/default/files/omb/assets/omb/circulars/a004/a-4.pdf.

167. *See id.* at 2.

168. *See generally id.* These principles have been reaffirmed by the Obama Administration in recent Executive Orders. *See* Exec. Order No. 13,563, 76 Fed. Reg. 3821 (Jan. 21, 2011) (President Obama) (stating that the benefits of proposed and final rules must "justify" the costs); Exec. Order No. 13,579, 76 Fed. Reg. 41,587 (Jul. 14, 2011) (stating that independent regulatory agencies "should promote" the goals expressed in EO 13,563); *see also* BENEFIT-COST ANALYSIS AT INDEPENDENT REGULATORY AGENCIES COMMITTEE ON REGULATION, ADMINISTRATIVE CONFERENCE OF THE UNITED STATES (Apr. 23, 2013) (draft recommendation), *available at* http://www.acus.gov/sites/default/files/documents/IRC%20BCA%20Recommendation%20for%204-29-13%20Mtg%20FINAL.pdf.

169. *See id.* at 2.

The determination of the need for the regulatory action incorporates the statutory or judicially recognized basis for the action and considers the specific conditions that generate the need for action.[170] When not explicitly mandated by law, regulatory action is warranted when there is a compelling need for action.[171] Examples of compelling needs include remedying material failures of private markets to protect or improve public health, safety, and well-being, and meeting other compelling public needs such as "promoting intangible values such as distributional fairness or privacy."[172] Finally, this assessment involves a tentative determination of the effectiveness of government action, including whether any proposed government regulation would do more good than harm.[173] To satisfy this last factor, the agency must overcome a presumption against economic regulation.[174] The legal authority for any potential cybersecurity regulation was discussed in the preceding sections.[175] Accordingly, this section will focus on the other aspects of agency decision-making.

a. *Market Failures and Other Compelling Needs*

Market failures occur for three primary reasons: externalities, abuse of market power, and inadequate or asymmetric information.[176] Externalities allow one party to "impose uncompensated benefits or costs on another party."[177] A firm with a dominant position in a market abuses its market power when it increases the price or reduces the output of its products so as to earn profits in excess of what would be attainable in a competitive market.[178] Inadequate information creates a market failure when it inhibits producer or consumers from making informed decisions about their participation in the market.[179] This allows actors with superior information to use it to their benefit or to the detriment of those without

170. *See id.* at 3–4 (citing Executive Order 12866, which states that "Federal agencies should promulgate only such regulations as are required by law, are necessary to interpret the law, or are made necessary by compelling need, such as material failures of private markets to protect or improve the health and safety of the public, the environment, or the well being of the American people"). The previous sections of this Note discuss the legal basis for regulatory action relying on the Commission's ancillary authority. *See* Part III *supra*.

171. Executive Order 12866 §1(a).

172. *See* Circular A-4, at 4.

173. *Id.*

174. *Id.* at 6.

175. *See* Part III *supra*.

176. *See* Circular A-4, at 4.

177. *See id.*

178. *See id.* at 4–5.

179. *See generally* Aidan R. Vining & David L. Weimer, *Information Asymmetry Favoring Sellers: A Policy Framework*, 21 POLICY SCIENCES 281 (1988).

information.[180] For example, a food producer is in a much better position to know the quality and ingredients of its food than the would-be buyer. The producer could use this information to induce the consumer to pay a higher price for food than she would otherwise if she had known the true quality and ingredients of the food.[181] However, when the information available to participants in a market is incomplete, market failure does not necessarily result. The primary generator or holder of relevant information need not always serve as the supplier of that information; it may also be provided by third parties.[182] This does not, however, mean that when information is available, it will be adequate to remedy a market failure, because of the inability of the public or other market participants to process the information in a relevant way. This most often "occurs in cases of low probability, high-consequence events."[183] Furthermore, "[w]hen it is time-consuming or costly for consumers to evaluate complex information about products or services . . . , they may expect government to ensure that minimum quality standards are met."[184]

Circular A-4 recognizes that situations other than market failures can provide compelling justifications for regulations.[185] Examples include congressionally created programs to redistribute resources or ensure efficient, non-discriminatory distribution of resources.[186] Other examples include regulation to protect privacy, permit more personal freedom, or promote other democratic considerations.[187]

b. *Federal Regulation as the Best Method to Solve the Problem*

Even when the above concerns exist and create the problem, an agency should consider alternatives to regulation, including antitrust enforcement, consumer-initiated product liability lawsuits, administrative compensation systems, and state regulation or enforcement.[188] When considering regulation, agencies must be cognizant of the presumption against economic regulation.[189] A high burden of proof must be met to demonstrate the need for "mandatory uniform quality standards for goods or services if the potential problem can be adequately dealt with through

180. *See id.* at 291–98 (detailing situations where information asymmetries create market failures and giving suggestions for government interventions in appropriate circumstances).
181. Circular A-4, *supra* note 166,at 5.
182. *Id.*
183. *Id.*
184. *Id.*
185. *See id.*
186. *See id.*
187. *Id.*
188. *Id.* at 6.
189. *Id.* at 7.

voluntary standards or by disclosing information of the hazard to buyers or users."[190]

2. The Decision to Regulate Cybersecurity to Ensure Network Reliability

Both a market failure and a compelling need for a reliable communications network justify regulating insufficient ISP cybersecurity and network reliability. While such regulation can engender concerns of government overreach through economic regulation, well-thought-out federal regulation is the best way to solve the problem. The Commission should regulate broadband Internet Service Providers' cybersecurity measures to increase network reliability. This subsection addresses each justification in turn.

a. *Market Failure Through Inadequate Information*

Network reliability and cybersecurity are susceptible to problems resulting from inadequate information, both for consumers and governments. Part II of this Note documented the failings of only some of the standard protocols through which the Internet operates; the reality of computer vulnerabilities is that they are numerous and hard to discern.[191] Further, most network operators do not make their downtime statistics available to the public or the FCC.[192] It is therefore hard to measure how often the network is unavailable to consumers. If consumers and the government had data on vulnerabilities and network downtime, they could demand a more reliable network that is hardened against future attacks. This lack of information creates a market failure, inasmuch as consumers

---

190. *Id.*

191. See Dan Assaf, Government Intervention in Information Infrastructure Protection, in IFIP International Federation for Information Processing, Vol. 253, (E. Goetz & S. Shenoi eds.) 35–38 (2008) (noting a lack of cybersecurity information sharing between actors in the private sector). Further, many cyber-attacks rely on "zero-day vulnerabilities," which are previously unknown computer flaws. *See* McKay Cunningham, *Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law*, 44 GEO. WASH. INT'L L. REV. 643, 686 (2012); Jeremy Richmond, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?* 35 FORDHAM INT'L L.J. 842, 853-54 (2012).

192. Many telecommunications companies strongly disapprove of releasing network outage reporting data already collected by the FCC through the NORS and 9-1-1 reliability program to the public. *See, e.g.*, Improving 911 Reliability, *Report and Order*, FCC 13-158, 28 FCC Rcd. 17476, para. 153. (2013) [hereinafter *911 Reliability Order*]. While not the focus of this Note, many web services do publish service availability information, including historical data. See, for example, http://status.aws.amazon.com/ and http://www.google.com/appsstatus#hl=en&v=status&ts=1395719999000.

cannot accurately assess the risks of network vulnerabilities and cannot appraise the value of the service accordingly.

Further, it is unclear if a traditional market model applies in the case of the Internet, given the differences between last mile connections and general network infrastructure. While network infrastructure is shared and used by everyone who traverses the network, the market for last mile connectivity is in many places a monopoly for consumers.[193] Further, because of common utilization, the origins and destinations of the traffic on this segment of the network are most likely connected by numerous different paths.[194] This characteristic makes the network infrastructure as a whole less vulnerable to failure, assuming no vulnerability is shared by the operators of multiple paths. However, given that a single manufacturer dominates the market for network switches and that the aforementioned vulnerabilities afflict many protocols that virtually all network operators use, it is likely that vulnerabilities do exist.[195]

Network packets can take multiple different paths, so ISPs do not have incentives to upgrade the security on their networks or make them more reliable because increased information is less likely to impact consumers' choices in ISPs. However, individual ISPs do have limited control over the network infrastructure and over which path data takes to get to its destination. While ISPs can and do route their traffic to different networks with differing priorities,[196] it is unclear if they have the knowledge or the incentive to route traffic to more secure networks. Because of the lack of information accessible to the public about cyber vulnerabilities, the FCC should conclude that a market failure justifies a decision to regulate. There is, however, a stronger rationale that justifies regulation of ISPs' cybersecurity practices—the compelling need for a reliable communications network.

---

193. *See generally* SUSAN CRAWFORD, CAPTIVE AUDIENCE: THE TELECOM INDUSTRY AND MONOPOLY POWER IN THE NEW GILDED AGE (2013) (arguing that residentially broadband users have essentially one choice for high speed Internet).

194. *See* Inquiry Concerning the Deployment of Advanced Telecomms. Capability to All Americans in A Reasonable & Timely Fashion, *Second Report*, FCC 00-290, CC Docket No. 98-146, 15 FCC RCD. 20913, 20922-23, paras. 17-18 (2000).

195. *See* Part II *supra* (discussing BGP and DNS); Ahsan Aslam Khan, *Cisco's Clear Dominance in Data Networking*, THE MOTLEY FOOL (June 25, 2013) http://www.seattlepi.com/business/fool/article/Cisco-s-Clear-Dominance-in-Data-Networking-4486272.php (noting that Cisco Systems has over 60% of the market share for routers and switches); Snowden, *supra* note 4.

196. That is, Comcast might have a more favorable traffic payment arrangement or peering with certain backbones, and would preferentially divert traffic to those networks if possible, at the expense of using other potential paths to get its traffic to the same destination. *See generally* Daniel Golding, *The Real Story Behind the Comcast-Level 3 Battle*, GIGAOM (Dec. 1, 2010), http://gigaom.com/2010/12/01/comcast-level-3-battle/.

b. *Compelling Need for a Reliable Nationwide Communications Network*

As early as 1934, with the passage of the Communications Act, Congress recognized the importance of a reliable, nationwide communications network.[197] The purpose of the FCC is to ensure "a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities . . . for the purpose of the national defense [and] promoting safety of life and property."[198] The FCC has realized its purpose with the telephone network, and to a lesser extent with the Internet. Both have immensely increased the productivity and prosperity of the United States.[199]

Although the word "reliable" is not in section 151, it is implied by our dependence on the interstate and international communications network. Much of our daily communications traverse the Internet, from phone conversations converted to VoIP and back to the PSTN to entertainment and banking. The Internet has provided significant benefits to society and countless new ways to communicate.[200] With regard to public disasters, the FCC has recently shown a desire to improve network reliability, indicating that this is an essential aspect of the communications network.[201] The promotion of a reliable communications network serves intangible values such as public safety and national security. The FCC recently expounded upon this idea in an order requiring increased reliability and certification oversight for service providers to 9-1-1 public-safety answering points.[202] This compelling need would likely justify government regulation of the cybersecurity practices of ISPs even if there were not a market failure caused by a lack of information.

c. *Federal Regulation as the Best Way to Ensure a Reliable Communications Network*

Even if remedying vulnerabilities in the communications network is justified by a market failure or a compelling need, the FCC must consider

197. 47 U.S.C. § 151 (2006).
198. 47 U.S.C. § 151 (2006).
199. *See* REED HUNDT & BLAIR LEVIN, THE POLITICS OF ABUNDANCE ch. 2 (2012).
200. *See* HUNDT & LEVIN, *supra* note 199, ch. 2 (noting the benefits of the Internet and making recommendations to improve society through future technologies that take advantage of this interconnectedness).
201. *See generally* Improving the Resiliency of Mobile Wireless Commc'ns Networks, *Notice of Proposed Rulemaking*, Release No. FCC 13-125, (2013), *available at* http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-13-125A1.pdf (introducing measures to increase transparency to consumers regarding the ability of different wireless service providers to maintain their networks operational during emergencies); *911 Reliability Order*, *supra* note 192 (adopting rules to ensure that 911 communications networks nationwide are dependable and resilient).
202. *See 911 Reliability Order*, *supra* note 192, paras. 1-6.

other options before making a decision to regulate. Many of the alternative options suggested by the Office of Management and Budget in the A-4 Circular cannot remedy the problem of network reliability. This is not an antitrust issue, nor is it a products liability issue.[203] The Internet and nationwide communications network are archetypical interstate systems and are not amenable to regulation by the states.[204] These considerations all weigh heavily in favor of federal regulation.

However, the FCC should be mindful of the presumption against economic regulation.[205] It is possible that FCC regulation would take the form of mandatory, uniform quality standards for goods or services. This type of regulation requires a hard look at its necessity. Specifically, the FCC must consider whether "the potential problem can be adequately dealt with through voluntary standards or by disclosing information of the hazard to buyers or users."[206] This is the most significant criticism of FCC regulation.

If ISPs start to disclose their security practices, consumers may choose the best security among service providers, providing an incentive for ISPs to compete for customers over the issue of cybersecurity. While recent disclosures of network vulnerabilities provide some information about the state of cybersecurity to consumers,[207] there is no indication that ISPs are planning to compete in this arena. The FCC's Cyber Security Certification Program Notice of Inquiry might have also provided information to consumers, however, that docket has not been revisited since 2011.[208] Voluntary cybersecurity and network reliability commitments may be an adequate solution to this problem, and the FCC has moved in this direction. The Communications Security, Reliability and Interoperability Council already convened by the FCC is one avenue to encourage network operators to make voluntary commitments. Indeed, the FCC has secured voluntary commitments from many of the largest Internet service providers to address vulnerabilities with DNS and BGP,[209] and

---

203. See RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 19 (1998) (stating that services, "even when provided commercially, are not products," and so are not subject to the rules of products liability).

204. Indeed, the Communications Act "must be construed in light of the needs for comprehensive regulation and the practical difficulties inhering in state by state regulation of parts of an organic whole." Gen. Tel. Co. of Cal. v. FCC, 413 F.2d 390, 398 (D.C. Cir. 1969). The whole point of the Federal Communications Commission is to regulate the communications industry. ON/TV of Chicago v. Julien, 763 F.2d 839, 842 (7th Cir. 1985).

205. Circular A-4, *supra* note 166, at 6.

206. *Id.* at 7.

207. The NSA disclosures provide a wealth of data on the state-of-the-art intrusion techniques used by the U.S. Government. Some of these techniques targeted ISPs with previously unknown cybersecurity vulnerabilities.

208. Cyber Sec. Certification Program NOI, *supra* note 53.

209. *See* FCC Advisory Committee Adopts Recommendations to Minimize Three Major Cyber Threats, *supra* note 61, at 1. However, as noted in Part II.C, these commitments cover only fifty percent of residential broadband users. *Id.*

CSRIC IV will be making recommendations for voluntary adoption of other cybersecurity best practices in conjunction with the NIST Cybersecurity Framework.[210]

However, not all cybersecurity problems that threaten network reliability can be solved in such a manner; a recent proceeding addressing 9-1-1 reliability shows why. Over the last ten years, the Commission had relied on assurances by 9-1-1 service providers that they would voluntarily implement industry best practices such as backup power and connection diversity for public-safety answering points.[211] When considering the causes of 9-1-1 service failures, the FCC determined that the adoption of these industry best practices could have prevented the 9-1-1 outages experienced during and after the 2012 derecho; unfortunately, that implementation did not happen.[212] This is a clear example that reliance on voluntary commitments to adopt these best practices did not produce the reliability needed for this service.[213] With cybersecurity, voluntary commitments by ISPs may also result in lack of implementation, especially given the lackadaisical adoption of DNSSEC noted above.[214] The FCC must also consider the feasibility of obtaining commitments from all service providers. Furthermore, will these commitments encompass new vulnerabilities and changing technology? Will these commitments actually ensure reliability? These are difficult questions, and the gravity of ensuring the safety of our economy militates toward obtaining more certain assurances that reliability is paramount.

Ensuring high reliability and protection from cyber-attacks on the communications infrastructure may be possible only with regulation. Having concluded that the FCC should regulate, this Note now turns to a brief discussion of the FCC's considerations for *how* it should regulate.

B. Cost-Benefit Analysis and Cost-Effectiveness Analysis

Once an agency has decided to regulate, it must choose the best method of regulation to achieve its goal. Cost-benefit analysis and cost-effectiveness analysis are prominent methodologies to help agencies make this choice.[215] As the influential scholar and Supreme Court Associate Justice Stephen Breyer wrote, cost-benefit analysis embodies "a simple axiom for creating and implementing any program: determine the

---

210. CSRIC IV, *supra* note 69, at 5.

211. *See 911 Reliability Order*, *supra* note 192, paras. 11-14.

212. *See id.* at para. 21.

213. *Id.* at paras. 24-26 (noting that "service providers may choose–and have chosen–to disregard these voluntary recommendations, even when they concern critical 911 services").

214. *See* Part II.A *supra*.

215. Circular A-4, *supra* note 166, at 9; *see generally* Cass R. Sunstein, *Cost-Benefit Default Principles*, 99 MICH. L. REV. 1651, 1662 (2001). The initial description here applies to both cost-benefit analysis and cost-effectiveness analysis, even if cost-benefit analysis is the methodology mentioned by name.

objectives, examine the alternative methods of obtaining these objectives, and choose the best method for doing so."[216] Cost-benefit analysis is a way of producing a full appraisal of a proposal that reflects the shortcomings inherent in the human decision-making process.[217] In addition, cost-benefit analysis forces agencies to explicitly state their rationale for regulating. By articulating the basis for the decision, agencies allow the public an opportunity to provide input in a way not necessarily required by the minimum notice and comment procedures.[218]

In 1993, President Bill Clinton issued an Executive Order setting out general principles of regulation.[219] These have been lauded as a codification of the principles of cost-benefit analysis,[220] and subsequent guidance from the Office of Management and Budget has expanded upon the principles in the Executive Order.[221] While the FCC, as an independent agency, is not obligated to take these considerations into account or to obtain Office of Information and Regulatory Affairs ("OIRA") approval before it promulgates regulations,[222] these principles provide an excellent foundation to guide the decision of whether or not to mandate cybersecurity standards.[223] Summarizing the principles produces several overarching considerations:

---

216. STEPHEN G. BREYER, REGULATION AND ITS REFORM 5 (1982).

217. *See* Sunstein, *supra* note 215, at 1662 (observing that people "have difficulty in calculating probabilities, and they tend to rely on rules of thumb, or heuristics, that can lead them to make systematic errors . . . in thinking about the seriousness of certain risks.").

218. *Id.*; *see also* Michael A. Livermore & Richard L. Revesz, *Regulatory Review, Capture, and Agency Inaction*, 101 Geo. L.J. 1337, 1370 (noting that the cost-benefit analysis methodology reduces agency capture through "requiring the examination of a wide range of regulatory effects; . . . [being] standardized and supported by a set of professional norms; and . . . improv[ing] transparency, by publishing for public scrutiny agency estimates of regulatory effects.").

219. Exec. Order 12,866, 58 Fed. Reg. 51,735 (Sept. 30, 1993).

220. *See* Sunstein, *supra* note 215, at 11655-656. More recently, Commissioner Maureen Ohlhausen drew upon the principles and adapted them to form principles for when the Federal Trade Commission should use its unfair methods of competition authority to regulate. *See Section 5: Principles of Navigation*, Remarks of Maureen K. Ohlhausen, Commissioner, Federal Trade Commission at the U.S. Chamber of Commerce (Washington, D.C., July 25, 2013).

221. *See* Circular A-4, *supra* note 156, at 1.

222. *See* Exec. Order 12,866, 58 Fed. Reg. §6(a)(3). To reduce the paperwork burden businesses, people, and small governments, the FCC does have to submit proposed regulations to OMB when obtaining information from ten or more persons. *See* 5 C.F.R. §§ 1320.3, 1320.4.

223. Exec. Order 12,866, 58 Fed. Reg. §1(b). Not every principle applies in this analysis. For reference the twelve principles are:

> (1) Each agency shall identify the problem that it intends to address (including, where applicable, the failures of private markets or public institutions that warrant new agency action) as well as assess the significance of that problem.
> (2) Each agency shall examine whether existing regulations (or other law) have created, or contributed to, the problem that a new regulation is

1. Identify the problem that the regulation seeks to address.

---

intended to correct and whether those regulations (or other law) should be modified to achieve the intended goal of regulation more effectively.

(3) Each agency shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, such as user fees or marketable permits, or providing information upon which choices can be made by the public.

(4) In setting regulatory priorities, each agency shall consider, to the extent reasonable, the degree and nature of the risks posed by various substances or activities within its jurisdiction.

(5) When an agency determines that a regulation is the best available method of achieving the regulatory objective, it shall design its regulations in the most cost-effective manner to achieve the regulatory objective. In doing so, each agency shall consider incentives for innovation, consistency, predictability, the costs of enforcement and compliance (to the government, regulated entities, and the public), flexibility, distributive impacts, and equity.

(6) Each agency shall assess both the costs and the benefits of the intended regulation and, recognizing that some costs and benefits are difficult to quantify, propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs.

(7) Each agency shall base its decisions on the best reasonably obtainable scientific, technical, economic, and other information concerning the need for, and consequences of, the intended regulation.

(8) Each agency shall identify and assess alternative forms of regulation and shall, to the extent feasible, specify performance objectives, rather than specifying the behavior or manner of compliance that regulated entities must adopt.

(9) Wherever feasible, agencies shall seek views of appropriate State, local, and tribal officials before imposing regulatory requirements that might significantly or uniquely affect those governmental entities. Each agency shall assess the effects of Federal regulations on State, local, and tribal governments, including specifically the availability of resources to carry out those mandates, and seek to minimize those burdens that uniquely or significantly affect such governmental entities, consistent with achieving regulatory objectives. In addition, as appropriate, agencies shall seek to harmonize Federal regulatory actions with related State, local, and tribal regulatory and other governmental functions.

(10) Each agency shall avoid regulations that are inconsistent, incompatible, or duplicative with its other regulations or those of other Federal agencies.

(11) Each agency shall tailor its regulations to impose the least burden on society, including individuals, businesses of differing sizes, and other entities (including small communities and governmental entities), consistent with obtaining the regulatory objectives, taking into account, among other things, and to the extent practicable, the costs of cumulative regulations.

(12) Each agency shall draft its regulations to be simple and easy to understand, with the goal of minimizing the potential for uncertainty and litigation arising from such uncertainty.

2. Analyze the costs, benefits, and impacts on incentives for each alternative regulatory option, recognizing that some costs and benefits are difficult to quantify.
3. Choose the option in which the benefits best justify the costs, avoiding inconsistent or duplicative regulation.
4. Provide clear guidance for stakeholders and those affected by the proposed regulation.[224]

The FCC has shown implicit acceptance of these considerations when deciding whether to regulate.[225]

Cost-benefit analysis is not at odds with regulation, nor is it a purely economic approach to regulation.[226] Instead, it is an "instrument designed to ensure that the consequences of regulation are placed before relevant officials and the public as a whole, and intended to spur attention to neglected problems while at the same time ensuring that limited resources will be devoted to areas where they will do the most good."[227] It is important that agencies do not engage in cost-benefit analysis to the detriment of society by failing to come to a conclusion using cost-benefit tools.[228] This "paralysis by analysis" can prevent desirable regulations from going forward.[229]

1. Principles of Cost-Benefit Analysis and Cost-Effectiveness Analysis

The considerations of cost-benefit analysis and cost-effectiveness analysis fall along different axes. Cost-benefit analysis is used to compare regulatory options that have outcomes that can be measured in dollar values, while cost-effectiveness analysis looks to the efficacy of each potential regulatory measure.[230] If possible, agencies should perform both analyses when choosing among regulatory alternatives.[231] The background section of this Note identified the problem that the FCC must address. Having dispensed with the first step, the following discussion will focus on steps two through four.

---

224. *See id.*; Livermore, *supra* note 218, at 1370-71.
225. *See* Preserving the Open Internet, *Notice of Proposed Rulemaking*, FCC 09-93, 24 FCC Rcd. 13064, paras. 48-80 (2009) (discussing the need for Commission action by considering the goals of the Commission, the current state of broadband and the Internet marketplace, and the debate regarding traffic management pricing and practices).
226. *See* Sunstein, *supra* note 215, at 1663.
227. *Id.*
228. *Id.*
229. *Id.*
230. Circular A-4, *supra* note 166, at 10.
231. *Id.* at 9.

a. *Determining the Costs and Benefits of the Alternatives*

The agency must show how the proposed action will bring about the anticipated costs and benefits.[232] Cost-benefit analysis reduces both the costs and the benefits of proposed regulation to monetary units, thereby facilitating the evaluation of the proposal through a common metric.[233] Accordingly, the agency should show the monetized values of the benefits and costs to society.[234] When benefits are not amenable to measurement using monetary units, agencies must still try to measure the outcomes in terms of physical units.[235] When direct measurements of costs and benefits are not possible, either because the market does not exist or because the costs and benefits are intangible, an agency can use implicit price estimates,[236] revealed preference measures,[237] and stated preference measures[238] to determine a monetized value for goods and services. Costs and benefits are measured against a baseline of outcomes expected to occur if the regulation is not implemented.[239] This baseline must consider how the market will likely evolve and external factors affecting expected costs and benefits.[240] Agencies should generally analyze at least three options: "the preferred option; a more stringent option that achieves additional benefits (and presumably costs more) beyond those realized by the preferred option; and a less stringent option that costs less (and presumably generates fewer benefits) than the preferred option."[241]

Agencies must consider the costs of a regulation in addition to its benefits.[242] A regulatory approach that is blind to its costs reduces societal benefits in the aggregate, even if the regulatory goal has a higher positive effect in remediating the problem. Professor Cass Sunstein, former Administrator of the Office of Information and Regulatory Affairs, describes this principle in the context of environmental regulation:

---

232. *Id.* at 18.
233. *Id.* at 10.
234. *Id.* at 18.
235. *Id.* at 10.
236. *Id.* at 20.
237. *Id.* at 20–21. One caveat for the revealed preference measure is that it requires a well-informed market participant to obtain accurate measures. *Id.* This may pose difficulties when measuring reveal preference for cybersecurity and network reliability. *Id.*
238. *Id.* at 22–23.
239. *Id.* at 15–16.
240. *Id.* at 15.
241. *Id.* at 16.
242. While this may seem intuitive and will certainly be brought up by the regulated entities, it is important to see its rationale, as it focuses agency efforts. Sunstein, *supra* note 215 (explaining the rationale for considering both costs and benefits in addressing agency efforts).

> The basic idea is that a "benefits only" approach also reflects a kind of tunnel vision, a myopic focus on only one of the variety of things that matter. Suppose, for example, that one approach to regulation would produce a certain level of air quality benefits, but at a cost of $800 million, and that a competing approach would produce a trivially lower level of air quality benefits, but at a cost of $150 million. If costs can be made relevant, the agency is permitted to do what seems quite sensible: save the $650 million, because the benefits would not be high enough to justify the expenditure.[243]

This approach leads to more rational regulation.[244]

When determining costs and benefits, there are a number of considerations suggested by Executive Order 12866.[245] One common measure of cost is the economic criterion of the "private willingness to pay."[246] This is a measure of how much individuals would be willing to forgo to enjoy a particular benefit.[247] However, this measure suffers from a number of deficiencies. Willingness to pay depends on having information about the problem and its consequences and the means to pay once the consequences of maintaining the status quo are known.[248] Further, private willingness to pay does not necessarily take into account intangible costs and benefits that society as a whole would receive from a regulation.[249] Accordingly, this should be one factor among many considered, including the measures mentioned above such as implicit price estimates, revealed preference measures, and stated preference measures.

Another consideration is a "feasibility requirement," which considers whether it is feasible for the regulated industry to implement the regulation.[250] However, at its heart, a feasibility requirement involves no balancing of costs and benefits.[251] This is because any "significant increase in costs is likely to prove 'not feasible' for at least some companies."[252] Using the "feasibility requirement" is appropriate in extreme cases, i.e. a regulation is infeasible if it significantly harms the industry resulting in

---

243. *Id.* at 1691.
244. *See id.* at 1684 (noting that "Justice Breyer expressly endorses the default rule of *Michigan v. EPA*, saying that in the face of statutory ambiguity, agencies should be allowed to consider costs, if only because that approach would increase the likelihood of rational regulation.").
245. *See* Exec. Order 12,866, 58 Fed. Reg. 51,735 § 6(a)(3)(C) (Sept 30, 1993).
246. See Sunstein, *supra* note 215, at 1661.
247. Circular A-4, *supra* note 166, at 18.
248. Sunstein, *supra* note 215, at 1661.
249. *See id.*
250. *See id.* at 1701.
251. *Id.* (citing Am. Textile Mfrs. Inst. v. Donovan, 452 U.S. 490 (1981)).
252. *See* Sunstein, *supra* note 215, at 1701.

"large numbers of business failures, substantial losses of jobs, or the equivalent."[253]

When possible, agencies should use market data about the actual prices for the goods or services affected by regulation.[254] Market prices provide good data for estimating costs and benefits if the services affected by the regulation are traded in a "well-functioning competitive market."[255] For many costs, it may be difficult to quantify the consequences of either regulating or not regulating.[256] Regardless of whether they are quantifiable, though, these costs and benefits must be considered.[257] Qualitative measures for assessing the consequences of inaction or regulation include "distributive impacts" and "equity" analyses.[258]

When analyzing non-quantified costs and benefits, the agency must carefully describe these intangibles *qualitatively*.[259] The agency must "present any relevant quantitative information along with a description of the unquantifiable effects, such as . . . improvements in quality of life . . . [with] a discussion of the strengths and limitations of the qualitative information."[260] This description should also include reasons why the information cannot be quantified.[261]

b. *Cost-Effectiveness Analysis*

Cost-effectiveness analysis is used to identify the most effective uses of resources, comparing different regulatory actions with the same primary outcome.[262] The most cost-effective regulatory alternative is the one that achieves the best outcome at a reasonable or threshold cost; it is not necessarily the alternative with the highest cost-to-effectiveness ratio.[263] To perform the analysis, an agency must carefully construct the cost and performance measures (effectiveness) for the regulatory alternatives.[264] Cost is the net cost of the regulation, subtracting cost savings (though not primary outcomes) from the costs of the regulation.[265] Effectiveness

253. *Id.* at 1702–03 (citing United Steelworkers of Am. v. Marshall, 647 F.2d 1189 (D.C. Cir. 1980); Bldg. & Constr. Trades Dep't. v. OSHA, 838 F.2d 1258 (D.C. Cir. 1988); Nat'l Cottonseed Prods. Ass'n v. Brock, 825 F.2d 482 (D.C. Cir. 1987)).
254. *See* Circular A-4 *supra* note 166, at 21-22.
255. *Id.* at 19.
256. *See* Exec. Order 12,866, 58 Fed. Reg. 51,735 §1(b)(6) (Sept. 30, 1993).
257. *See id.*
258. *See id.* § 1(a), (b)(5).
259. *See* Circular A-4, *supra* note 166, at 27.
260. *Id.*
261. *Id.* (Here, OMB specifically identifies situations where the "existence of a risk may be based on highly speculative assumptions, and the magnitude of the risk may be unknown" as circumstances where quantization may be difficult and qualitative description may be needed).
262. *Id.* at 11
263. *Id.*
264. *Id.*
265. *Id.*

measures are the final outcomes of the regulation.[266] Effectiveness measures should examine how a regulation reduces the severity and the duration of the problem it seeks to remedy.[267]

FCC analysis will likely require the use of both cost-benefit analysis and cost-effectiveness analysis. Cybersecurity and network reliability seem particularly amenable to cost-effectiveness analysis because different regulatory measures would have the same outcome of increased network reliability.

2. Application to Cybersecurity Standards

It may be difficult to quantify and account for all of the costs and benefits associated with increased reliability and decreased vulnerability to cyber-attacks that threaten network infrastructure. The FCC will need to devote time and resources to considering the various factors involved and providing appropriate opportunities for public comment. This subsection provides some initial considerations for this analysis.

Direct costs of cybersecurity regulation will likely include upgrade costs for service providers, wages for more security and network analysts who can determine vulnerabilities, and funds spent to ensure administrative compliance with regulations. Insofar as providers spend money to comply with cybersecurity regulation, those funds might have otherwise enabled other infrastructure upgrades, such as increased bandwidth and connection speeds. These costs could be passed down to consumers, so the analysis should account for ancillary costs such as decreased access to the network by lower income groups.

Tangible benefits of increased cybersecurity and network reliability include improved economic activity through decreased downtime and improved national security. Intangible benefits include increased trust in the communications system. Qualitative descriptions can sometimes replace exact cost-benefit monetization, especially for intangible aspects and for events that are low-probability but high-consequence occurrences. Here, a network failure due to cybersecurity vulnerabilities is an example of a low-probability, high-consequence event. As such, the FCC should ensure it addresses all of the considerations of qualitative description, such as the strengths and limitations of the qualitative information, and the reasons why the information cannot be quantified.[268]

Cost-benefit analysis suggests looking at market prices to determine the monetized values of the costs and benefits of cybersecurity and network reliability. However, utilizing consumer pricing may not reflect actual costs and benefits. Using market data to inform monetization of the value of reliability and cybersecurity may be inaccurate because of the lack of

266. *Id.*
267. *Id.* at 14.
268. *See* Circular A-4, *supra* note 166, at 27.

information in the market, both to consumers and to the government. This lack of information about reliability and cybersecurity arguably means that the market for secure access is not a competitive marketplace.

Market prices are difficult to ascertain in the areas of cybersecurity and network reliability because of the interconnectedness of the network. One provider upgrading its network to increase its reliability does not affect another provider who may not be reliable, and so traffic generated by the more reliable network may nevertheless be degraded by the lack of security of other service providers. Thus, the amount of money a provider earns owing to its superior reliability might not translate into greater overall reliability. On the other hand, in the last mile market, and within each provider's network, there might be a more workable measure of reliability. The FCC must account for these factors in its analysis.

The FCC will need to evaluate the cost-effectiveness of its various regulatory options against each alternative—and against the status quo, i.e., no regulatory action. The agency must show how the proposed action will provide the anticipated costs and benefits.[269] There are a number of different options available, with varying levels of regulatory burden and reliability benefits. The least costly regulatory option is requiring reporting of network disruption events and cybersecurity problems. Because there would be no mandatory network standards or performance requirements, service providers would only bear the burden of reporting their network conditions, a matter about which they presumably already keep records. However, this option would likely have limited effectiveness and was recently considered and rejected by the FCC in the *9-1-1 Reliability Order*.[270]

While performance standards have proven successful in other regulatory contexts, such as improving fuel efficiency for vehicles,[271] their efficacy regarding network vulnerabilities is questionable. If cyber-attacks are low-probability events, it may be trivial to meet performance standards for a given year if measured in network availability uptime. In this scenario, a provider could report high performance but still not adopt the network security that is desired.[272]

An intermediate option may be certification. Regulation to require certification of the use of industry best practices or reasonable alternative measures is the approach the FCC took in the *9-1-1 Reliability Order*.[273] The order requires 9-1-1 service providers to certify their implementation

269. *Id.* at 18.

270. *See 911 Reliability Order*, *supra* note 192, at paras. 66-67.

271. *See generally* Greenhouse Gas Emissions Standards and Fuel Efficiency Standards for Medium- and Heavy-Duty Engines and Vehicles, EPA & NHTSA, 76 Fed. Reg. 57106 (2011).

272. This method of regulation was recently considered and rejected by the Commission in the *911 Reliability Order*. *See 911 Reliability Order*, *supra* note 192, at paras. 71-72.

273. *See 911 Reliability Order*, *supra* note 192, at paras. 44-65.

of industry best practices for reliability.[274] The FCC noted that this form of regulation "is not 'heavy-handed' or overly prescriptive, but rather flexible and designed to encourage innovation."[275] A similar tack could be taken with cybersecurity for ISPs to ensure general network reliability through consensus-based industry best practices. NIST has already laid the groundwork for this option in the Cybersecurity Framework.

The most stringent regulatory option would be to mandate specific network protocols and practices that have improved cybersecurity and reliability outcomes as compared with current practices. This is the most costly option, and its effectiveness is unclear. This may be effective for universal network protocols utilized by all service providers, such as DNSSEC and BGP discussed in Part II.A above. However, technology changes quickly, and it would probably be less cost-effective to require specific hardware and software upgrades in lieu of more flexible industry best practices than other regulatory options.[276] The Office of Management and Budget would likely oppose this method of regulation as a type of command-and-control economic regulation.

Because of inadequate information in the market, the FCC should use implicit price estimates and revealed preference measures to conduct studies to determine the value of these costs and benefits. The FCC should address industry concerns about the feasibility of a proposed regulation, but only to the extent that regulation would significantly harm the industry—i.e., by causing a large number of businesses to fail or eliminate jobs. Because of the importance of network reliability and the transition away from the PSTN to IP-based communications, the FCC should not fall into paralysis by analysis. It should act. Given the above factors and considerations, as well as the recent 911 Reliability Order, the FCC should adopt a requirement for service providers to certify implementation of industry best practices and require providers to certify compliance.

V. CONCLUSION

As more communications services become Internet-dependent, and ultimately transition to an all-IP communications system, our communications system is increasingly vulnerable to cyber-attacks. The FCC has the legal authority to implement certain measures designed to increase the cybersecurity of broadband and our nation's telecommunications infrastructure. Because of the unique threat cyber-

274. *Id.*

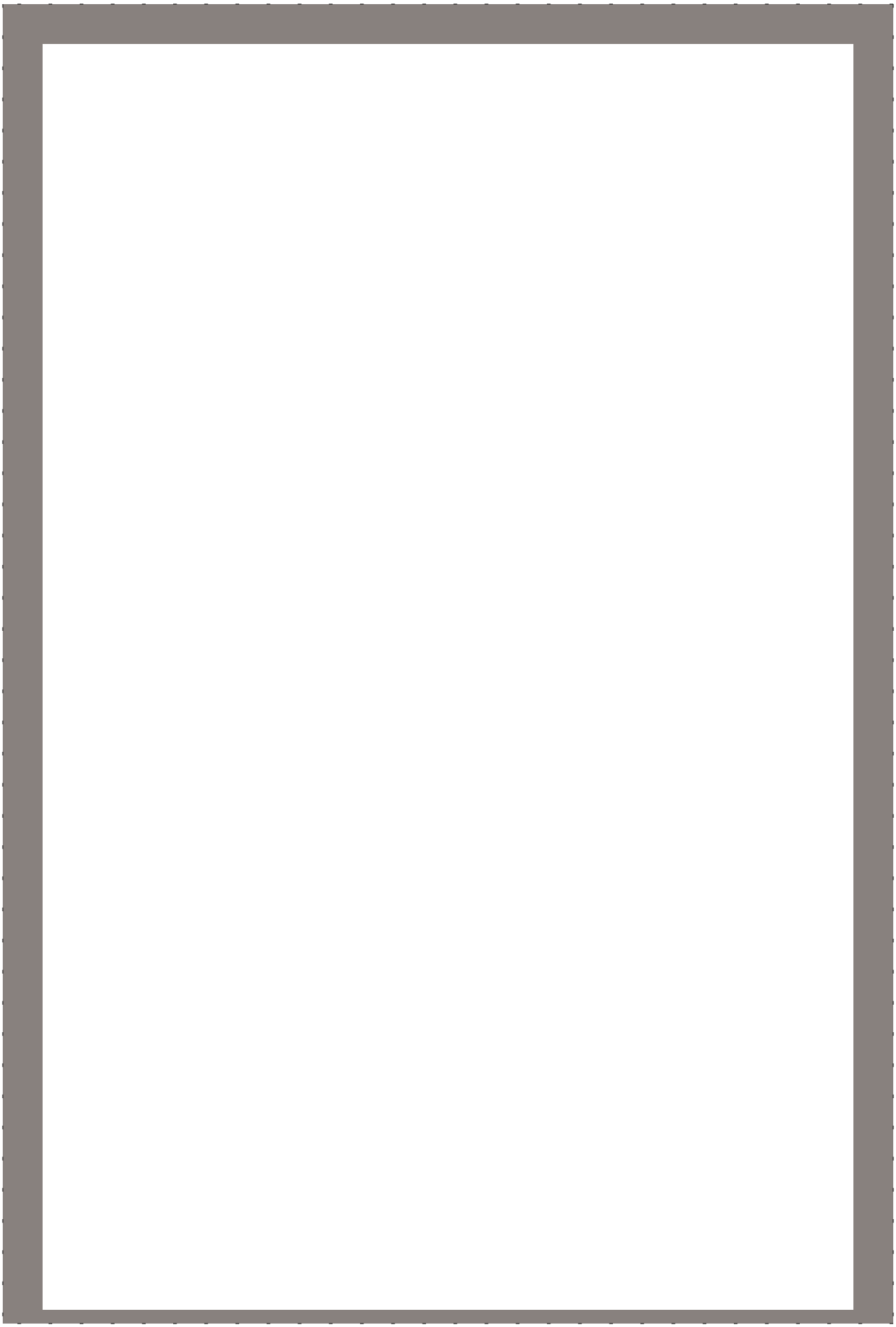
275. *Id.* at para. 30.

276. The FCC recognized this, and rejected tying regulations to specific technological standards in the *911 Reliability Order*. *See 911 Reliability Order*, *supra* note 192, para. 68; *see also* T. Randolph Beard, George S. Ford, Lawrence J. Spiwak & Michael Stern, *Wobbling Back to the Fire: Economic Efficiency and the Creation of a Retail Market for Set-Top Boxes*, 21 COMMLAW CONSPECTUS 1, 14 (2012).

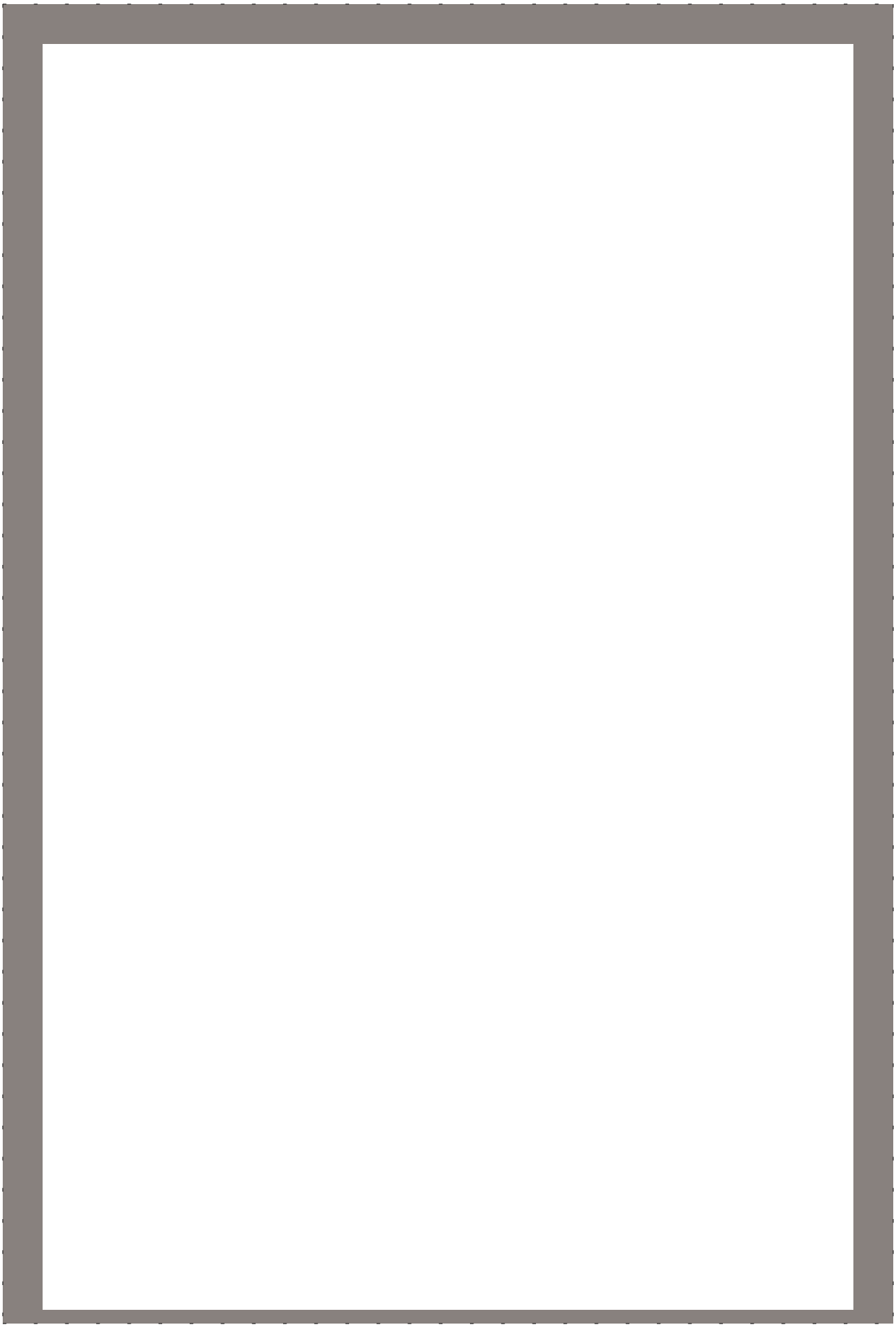
attacks pose to our telecommunications infrastructure, including jeopardizing network reliability, interconnection, and E-9-1-1 service, potential cybersecurity regulations would be reasonably ancillary to these congressionally mandated responsibilities, and thus amenable to regulation through the FCC's ancillary authority.

The FCC should exercise this authority because the market failure in information about vulnerabilities to cyber-attacks, together with the compelling need for a reliable communications system, both justifies government regulation. The specific type of regulation adopted must carefully balance costs and benefits, and should take the form of certification of industry best practices.

35573-fcl_66-3 Sheet No. 103 Side B 10/21/2014 10:02:02



35573-fcl_66-3 Sheet No. 104 Side A 10/21/2014 10:02:02



35573-fcl_66-3 Sheet No. 104 Side B 10/21/2014 10:02:02