EDITOR'S NOTE

Welcome to the third Issue of Volume 67 of the Federal Communications Law Journal, the nation's premier communications law journal and the official journal of the Federal Communications Bar Association.

This Issue features a timely article from Professor Rob Frieden of Pennsylvania State University, analyzing and critiquing the FCC's justification for reclassifying broadband Internet access as a common carrier, subject to Title II of the Communications Act of 1934.

Next, the Issue contains the inaugural Annual Review of Communications Law, from the Judicial Practice Committee of the Federal Communications Bar Association, to which the Journal owes many thanks. The Annual Review summarizes major communications law cases from 2014 and early 2015, providing an overview of recent jurisprudential developments in the field. The Annual Review covers: *T-Mobile South, LLC v. City of Roswell, Georgia*, No. 13-975 (U.S. Jan. 14, 2015); *CBS Corporation v. FCC*, 785 F.3d 699 (D.C. Cir. 2015); *Sorenson Communications, Inc. v. FCC* (Sorenson II), 765 F.3d 37 (D.C. Cir. 2014); *Spectrum Five LLC v. FCC*; 758 F.3d 254 (D.C. Cir. 2014); *Sorenson Communications, Inc. v. FCC* (*Sorenson I*), 755 F.3d 702 (D.C. Cir. 2014); *Illinois Public Telecommunications Association v. FCC*, 752 F.3d 1018 (D.C. Cir. 2014), and *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014).

In addition to those pieces, this Issue contains two student Notes. In the first Note, Anthony Glosson examines the Dormant Commerce Clause's impact on state data-privacy regulation. Employing the analytical framework of the district court's opinion in *American Library Association v. Pataki*, the Note presents several arguments for challenging state data-privacy laws and examines how modern geolocation technology changes this analysis, but concludes that geolocation does not cure the laws' constitutional ills. In the second Note, Anna Meyers presents a model for regulating online payment processors, which are attractive targets for criminals in a world of increasingly-common cyber-attacks. The Note examines the weaknesses of the now-prevailing territorial regulatory model and suggests that self-regulation, through industry-specific codes of conduct, paired with a comprehensive enforcement program, would be more effective.

The Journal is committed to providing its readership with substantive coverage of relevant topics in communications law, and we appreciate the continued support of contributions 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.

Tony Glosson
Editor-in-Chief

FEDERAL COMMUNICATIONS LAW JOURNAL

VOLUME 67 ISSUE 3

DECEMBER 2015

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 67 FED. COMM. L.J. ___ (2014).

FEDERAL COMMUNICATIONS LAW JOURNAL

GW | LAW

FCBA
FEDERAL COMMUNICATIONS BAR ASSOCIATION

VOLUME 67 ISSUE 3

DECEMBER 2015

ARTICLE

Professor Frieden assesses the current state of the FCC's Open Internet Order of 2015, which converted consumer broadband Internet access into a Title II service, as well as the potential outcomes of ongoing challenges to the lawfulness of its provisions. This article analyzes the likelihood that the FCC will succeed using their current theories of regulatory authority, and offers alternative prospects for lawful regulation of Internet access in the event that the Order is reversed or otherwise negatively affected by a judicial decision.

COMMUNICATIONS LAW: ANNUAL REVIEW

NOTES

States are enacting data privacy regulations at an ever-increasing pace. California led the way in 2013, enacting several new onerous data privacy laws that drew the ire of the technology sector.

This note addresses the Dormant Commerce Clause implications of statutes like California's new Do Not Track and Online Eraser laws. It overviews the Supreme Court's Dormant commerce clause jurisprudence, including the two primary

substantive doctrines constituting the cannon of Dormant Commerce Clause jurisprudence: extraterritoriality and Pike balancing.

Drawing on the above doctrines, along with the parallels between state data privacy laws and earlier statutes invalidated under the Dormant Commerce Clause, this note concludes that many state data privacy laws are unconstitutional regulations of interstate commerce because they impose burdens exceeding the putative benefits of their in-state effects.

Cross-Border Commerce without Constraint: Shifting from Territorial-Based Regulation to an Industry-Based Code of Conduct for the Online Payment Processing Industry

Data breaches are increasingly frequent and the data security standards promulgated to prevent those breaches are ineffective because they are based on a territorial regulation model. The regulations control based on where the data is located ignoring the modern reality of online global economies and commerce.

Online payment processors are particularly targeted in cyber-attacks because they collect personally identifiable information and sensitive financial information to facilitate online transactions. The regulation needs to shift from a territorial based model to an industry-based model that accounts for individual businesses' needs and is purposed for the information those businesses collect and maintain.

This objective is best achieved through a self-regulated industry code of conduct. The code of conduct should be based in sound principles adapted to the specific industry, should be flexible to adapt to emerging technologies and varying business practices, and should be enforceable through a comprehensive enforcement program.

Déjà vu All Over Again: Questions and a Few Suggestions on How the FCC Can Lawfully Regulate Internet Access

Rob Frieden*

TABLE OF CONTENTS

* Pioneers Chair and Professor of Telecommunications and Law, Penn State University, 102 Carnegie Bldg., University Park, PA 16802, http://www.personal.psu.edu/faculty/r/m/rmf5/

I. INTRODUCTION

In March, 2015 the Federal Communications Commission ("FCC") issued a comprehensive Report and Order on Remand and Declaratory Ruling, and Order, in the matter of *Protecting and Promoting the Open Internet* ("*2015 Open Internet Order*").[1] The FCC attempts to lawfully convert broadband Internet access[2] from a largely unregulated "information service,"[3] to a lightly regulated "telecommunications service."[4] In the *Order*, the Commission chose to classify Internet Service Providers ("ISPs")[5] as common carriers, subject to the telecommunications service regulations contained in Title II of the Communications Act,[6] as amended, based on changed circumstances necessitating more extensive government oversight.[7]

Having twice failed to convince a reviewing court that the Commission could impose conduit neutrality requirements without making the reclassification, the FCC took a different tack, subjecting ISPs to more

1. Protecting & Promoting the Open Internet, *Report & Order on Remand and Declaratory Ruling, & Order*, FCC 15-24, 30 FCC Rcd 17905 (2015) [hereinafter *2015 Open Internet Order*], http://www.fcc.gov/openinternet.

2. The FCC defines "broadband Internet access service" as: "A mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this Part." *Id*., para. 25.

3. An "information service" is "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and 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." 47 U.S.C. § 153(20).

4. A "telecommunications service" is "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used." 47 U.S.C. § 153(46) (2014).

5. The FCC emphasizes the need for regulatory safeguards applied to ISPs providing first and last mile links to and from the Internet. However, the reclassification of ISP-provided broadband Internet access also applies to upstream ISPs that perform an intermediary function between content providers and downstream ISPs. "The definition for broadband Internet access service includes the exchange of Internet traffic by an edge provider or an intermediary with the broadband provider's network. We note that anticompetitive and discriminatory practices in this portion of broadband Internet access service can have a deleterious effect on the open Internet, and therefore retain targeted authority to protect against such practices through sections 201, 202, and 208 of the Act (and related enforcement provisions), but will forbear from a majority of the other provisions of the Act." *2015 Open Internet Order*, para. 195.

6. *See generally* 47 U.S.C. §§ 201-276 (2014).

7. *2015 Open Internet Order*, para. 43 (explaining that "[a]s the record reflects, times and usage patterns have changed and it is clear that broadband providers are offering both consumers and edge providers straightforward transmission capabilities that the Communications Act defines as a "telecommunications service.").

muscular rules and regulations.[8] The *2015 Open Internet Order* has generated substantial controversy, several requests for a stay of the *Order*,[9] and an expedited appeal,[10] the latter of which questions whether the Commission has adequately justified its reclassification of broadband Internet access.[11]

This Article will assess whether and how the FCC can successfully defend its *2015 Open Internet Order* on appeal. In the *Order*, the FCC offered several justifications for its decision to apply its "light touch" approach to regulating broadband under Title II of the Communications Act, subject to extensive forbearing from Title II's common carrier regulatory safeguards.

While it is common in appellate advocacy to use multiple and alternative arguments, the FCC has presented contradictory legal rationales. On one hand, the FCC invokes the so-called *Chevron* Doctrine,[12] which requires courts to defer to the expertise of a regulatory agency when its authorizing statute lacks clarity and the agency reasonably interprets those statutory ambiguities.[13] However, elsewhere in its decision, the FCC

8. *See, e.g.*, Formal Complaint of Free Press & Public Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer Applications, *Memorandum Opinion and Order*, FCC 08-183, 23 FCC Rcd 13,028 (2008), *vacated*, *Comcast Corp. v. FCC*, 600 F.3d 642, 644 (D.C. Cir. 2010) (holding that imposing network neutrality rules under the FCC's "ancillary" authority exceeded its statutory authorization); 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 and remanded in part sub nom., Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014) (holding that because the FCC, under its prior regulatory regime, classified broadband providers as entities exempt from common carrier obligations, "the Communications Act expressly prohibits the [FCC] from . . . regulating them as such"), *on remand*, Protecting and Promoting the Open Internet, *Notice of Proposed Rulemaking*, FCC 14-61, 29 FCC Rcd 5561 (2014) [hereinafter *2014 Open Internet NPRM*].

9. *See, e.g.*, Joint Mot. Stay or Expedition at 1, *U.S. Telecom Ass'n*, No. 15-1063 (May 13, 2015), http://www.fhhlaw.com/1501063.net%20neutrality%20stay%20request.2015.05.13.PDF; Order Denying in Part & Granting in Part Joint Mot. Stay or Expedition at 1-2, *U.S. Telecom Ass'n*, No. 15-1063 (June 11, 2015); Protecting & Promoting the Open Internet, *Order Denying Stay Petitions*, DA 15-563, paras. 2-7 (May 8, 2015).

10. *See* Order Denying in Part & Granting in Part Joint Mot. Stay or Expedition at 1-2, *U.S. Telecom Ass'n*, No. 15-1063 (June 11, 2015); Joint Brief for Petitioners at 5, *U.S. Telecom Ass'n.*, No. 15-1063 (D.C. Cir. July 30, 2015), http://www.ustelecom.org/sites/default/files/documents/Joint%20Brief%20of%20Petitioners%20073015.pdf.

11. *See id.*

12. *See Chevron U.S.A. Inc. v. Natural Res. Def. Council*, 467 U.S. 837 (1984). In Chevron, the Supreme Court held that when reviewing an agency's implementation of its own authorizing statute, if "Congress has not directly addressed the precise question at issue," and the agency has acted pursuant to an express or implied delegation of authority, the agency's statutory interpretation is entitled to deference, as long as it is reasonable. *Id.* at 843-44. *See also United States v. Mead Corp.*, 533 U.S. 218, 226-27 (2001).

13. *2015 Open Internet Orde*r, para. 321 ("[W]e exercise the well-established power of federal agencies to interpret ambiguous provisions in the statutes they administer.") (citing *Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967, 980-81 (2005)).

confidently asserts that ISPs clearly provide essential telecommunications services,[14] evincing no difficulty with interpreting and applying existing service definitions created by Congress. Rather than having to remedy statutory ambiguity, the Commission appears to make the case that ISPs, once deemed to fit within the information service classification, now unambiguously fit within the telecommunications service category.[15]

This Article discusses how the FCC has come to understand the need to reclassify broadband Internet access as common carriage, leading the Commission to impose the regulatory safeguards it now considers essential. However, at the very time the Commission seeks to invoke lawful and sufficiently expansive statutory authority, ISPs need substantial flexibility to customize services meeting specific customer requirements, particularly demand for bandwidth intensive video services. Instead of according such flexibility, the Commission continues to apply an absolute, bright line regulatory dichotomy that does not work.

In this age of fast changing technologies and markets, the FCC ignores the fact that ventures readily offer both telecommunications and information services, as well as hybrids that combine elements that could trigger both regulatory classifications. Unlike reviewing courts, which have evidenced no difficulty in assessing how converging markets and technologies impact the FCC's jurisdiction,[16] the Commission continues to attempt the impossible: absolute and long term assessment of convergent services and assignment of them into single, mutually exclusive regulatory categories. Even as it already has attempted to reclassify broadband Internet access, the FCC wants reviewing courts, the public, and industry to think that it can shoehorn any existing or new service completely into one or the other service classification.

While stating its clear intent to forbear and streamline as never before, the FCC will have to convince a reviewing court that it considered all the facts and data in the record supporting the rational decision to reclassify ISP service. This Article concludes that the FCC's best appellate court strategy lies in emphasizing available direct statutory authority and changed circumstances in the Internet ecosystem, rather than ambiguity in the service definitions created by Congress, or alternatively that reviewing courts should defer to the Commission's expertise in assigning convergent

14. *Id.*, para. 59 ("[B]ased on a current factual record, we reclassify broadband Internet access service as a telecommunications service under Title II.").

15. *Id*., para. 413 n. 1207 ("[I]n reclassifying [broadband Internet access service] we simply acknowledge the reality of how it is being offered today.").

16. *Cellco P'ship v. FCC*, 700 F.3d 534, 547 (D.C. Cir. 2012) (reviewing court notes that wireless carriers offer both regulated voice, telecommunications service and unregulated data services classified as information services). The *Cellco* Court explained, "even if a regulatory regime is not so distinct from common carriage as to render it inconsistent with common carrier status, that hardly means it is so fundamentally common carriage as to render it inconsistent with private carrier status. In other words, common carriage is not all or nothing—there is a gray area in which although a given regulation might be applied to common carriers, the obligations imposed are not common carriage per se." *Id.*

services into unambiguous regulatory categories. This Article recommends that the FCC emphasizes its duty, established in Section 706 of the Communications Act,[17] to identify and remedy broadband market failures.

II. THE CHALLENGE OF CALIBRATING GOVERNMENT OVERSIGHT IN FAST CHANGING MARKETS

Even if the FCC could assert near complete independence from political parties, presidents, and Congress, it cannot avoid its duty to respond to fast changing markets and technologies and calibrate the proper scope of its regulatory oversight. Congress may have handicapped the FCC by constructing service definitions that the Commission must use to determine the scope of its oversight,[18] but the FCC exacerbates the situation by electing to make such category assignments based on the assumption that any existing or prospective service can and must fit solely into one classification, explaining:

> We agree with commenters that [telecommunications service and information service] are best construed as mutually exclusive categories, and our classification ruling appropriately keeps them distinct. In classifying broadband Internet access service as a telecommunications service, we conclude that this service is not a functionally integrated information service consisting of a telecommunications component "inextricably intertwined" with information service components. Rather, we conclude, for the reasons explained above, that broadband Internet access service as it is offered and provided today is a distinct offering of telecommunications and that it is not an information service.[19]

Over many generations of technologies, and despite vast changes in the telecommunications and information-processing marketplace, the FCC has opted to create and maintain an absolute dichotomy between regulated and largely unregulated services.[20] Notwithstanding its confidence in creating this dichotomy, the FCC has shown ambivalence about whether Congress created sufficiently clear statutory definitions, particularly when

17. 47 U.S.C. § 1302 (2014).

18.*See, e.g., id.* at §§ 153(43), 153(46), 153(20).

19. *2015 Open Internet Order*, para. 385. *See also* Federal-State Joint Board on Universal Service, *Report to Congress*, 13 FCC Rcd 11501, 11522 (1998) [hereinafter *1998 Universal Service Report*] ("[T]he language and legislative history of [the Communications Act of 1996] indicate that the drafters . . . regarded telecommunications services and information services as mutually exclusive categories."); Vonage Holdings Corp. v. Minnesota Pub. Utils. Comm'n, 290 F. Supp. 2d 993, 994, 1000 (D. Minn. 2003) (applying the FCC's dichotomy).

20. *See, e.g., 2015 Open Internet Order*, para. 385; *1998 Universal Service Report*, 13 FCC Rcd at 11522.

claimed ambiguity affords the Commission an opportunity to make its own clarifications, category assignments, and reclassifications.[21]

When determining which statutory classification applies to broadband Internet access, the FCC first refrained from making any determination at all,[22] but subsequently chose to apply the information service classification in 2002.[23] Now, the Commission has opted to change which classification applies[24] so that it can work around the judicial prohibition on applying common carrier nondiscrimination safeguards to non-common carriers.[25]

The FCC appears to have undertaken a strategy designed to accord it maximum flexibility in devising a new, ex ante regulatory regime. It uses statutory ambiguity as the basis for continual, but inconsistent regulatory classifications. This amounts to a once ambiguous, always ambiguous view of the Communications Act of 1934, as amended by the Telecommunications Act of 1996. By invoking statutory ambiguity, the FCC assumes it has largely unconditional authority to make different interpretations of the same, unchanged, legislatively-crafted definitions. Having previously considered statutory ambiguity as the basis for deeming broadband Internet access thoroughly fitting within the information service category created by Congress, the *2015 Open Internet Order*, changes its classification and now deems all types of Internet access to fit solely within the telecommunications service definition. The Commission reiterates its conclusion that the statutory definitions remain unclear,[26] but elsewhere in the *Order* the

21. *See, e.g.*, *2015 Open Internet Order*, para. 385.

22. Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities Internet Over Cable Declaratory Ruling, Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities, *Declaratory Rulemaking and Notice of Proposed Rulemaking*, FCC 02-77, 17 FCC Rcd 4798, para. 2. (2002) ("To date, however, the Commission has declined to determine a regulatory classification for, or to regulate, cable modem service on an industry-wide basis.").

23. Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities Internet Over Cable Declaratory Ruling, Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities, *Declaratory Rulemaking and Notice of Proposed Rulemaking*, FCC 02-77, 17 FCC Rcd 4798, para. 2. (2002) ("To date, however, the Commission has declined to determine a regulatory classification for, or to regulate, cable modem service on an industry-wide basis.").

24. *2015 Open Internet Order*, para. 29 ("[W]e find that broadband Internet access service is a 'telecommunications service' and subject to sections 201, 202, and 208.").

25. *See, e.g.*, *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014) (holding that because the FCC, under its prior regulatory regime, classified broadband providers as entities exempt from common carrier obligations, "the Communications Act expressly prohibits the [FCC] from . . . regulating them as such"); *Comcast Corp. v. FCC*, 600 F.3d 642, 644 (D.C. Cir. 2010) (holding that the FCC imposing network neutrality rules under its "ancillary" authority exceeded its statutory authority).

26. *See 2015 Open Internet Order*, para. 331 (explaining that when reclassifying services, the FCC is "exercise[ing] the well-established power of federal agencies to interpret ambiguous provisions in the statutes they administer."). *See also id*., para. 332. ("The Court's application of this *Chevron* test in *Brand X* makes clear our delegated authority to revisit our

Commission has no qualms about using the classifications, without adjustment, to specify into which single statutory category broadband Internet access fits.[27] Consistent with its insistence that any existing or prospective service fit solely within one category, the FCC decided that all types of broadband services constitute telecommunications services, regardless of the transmission technology.[28]

It appears that the FCC assumes that because Congress did not explicitly state into which service definition broadband access fits, the Commission can assume unfettered flexibility in making and changing the classification while referring to, and using, the service definitions. Apparently the FCC has no problem with the definitions crafted by Congress. However, the lack of specific statutory instructions provides the FCC with the assumed lawful authority to make ad hoc, and potentially inconsistent, determinations of which statutory definition solely applies to any and all types of broadband Internet access.

Adding complexity and uncertainty to the *2015 Open Internet Order*, the FCC maintains the preexisting telecommunications service/information service dichotomy for broadband by reaffirming that there are several types of services that remain information services.[29] Even though these information service providers may use the same broadband

---

prior interpretation of ambiguous statutory terms and reclassify broadband Internet access service as a telecommunications service.").

27. *See id*., para. 385 ("In classifying broadband Internet access service . . . [r]ather, we conclude, for the reasons explained above, that broadband Internet access service as it is offered and provided today is a distinct offering of telecommunications and that it is not an information service.").

28. *See id.*, para. 59 ("we reclassify broadband Internet access service as a telecommunications service under Title II"). The FCC previously determined that all forms of broadband Internet access constituted an information service. *See* Inquiry Concerning High-Speed Access to the Internet over Cable and Other Facilities, Declaratory Ruling and Notice of Proposed Rulemaking, 17 FCC Rcd 4798, paras. 13-15 (2002) (cable modem broadband), *aff'd sub nom*. *Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967, 977–78 (2005); Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, *Report and Order and Notice of Proposed Rulemaking*, 20 FCC Rcd 14,853, 14,863-64 (2005) (digital subscriber line broadband) [hereinafter *DSL Reclassification Order*], *petition for rev. denied*, *Time Warner Telecom, Inc. v. FCC*, 507 F.3d 205 (3d Cir. 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 13,281 (2006) (broadband via power lines); Appropriate Regulatory Treatment for Broadband Access to the Internet over Wireless Networks, *Declaratory Ruling*, 22 FCC Rcd 5901 (2007) (wireless broadband).

29. *Compare 2015 Open Internet Order*, para. 190 ("We adopt our tentative conclusion in the *2014 Open Internet NPRM* that broadband Internet access service does not include virtual private network (VPN) services, content delivery networks (CDNs), hosting or data storage services, or Internet backbone services (to the extent those services are separate from broadband Internet access service)."), *with*, *id*., para. 341 ("The record in this proceeding leads us to the conclusion that providers today market and offer consumers separate services that are best characterized as (1) a broadband Internet access service that is a telecommunications service; and (2) 'add-on' applications, content, and services that are generally information services.").

switching, routing, web address look up, and temporary storage technologies as ISPs now deemed telecommunications services, the FCC retained the information service classification for broadband service provided by Content Distribution Networks ("CDNs"),[30] such as Akamai and other ISPs operating as intermediaries upstream from "retail" ISPs providing first and last mile services to end users.[31] Bear in mind that CDNs and retail ISP interconnect their separate networks to provide consumers with speedy and seamless access to and from the Internet. Inconsistent regulatory classifications appear to differentiate the nature and function of CDNs vis a vis retail ISPs, but consumers expect both type carriers to cooperate fully to achieve a shared mission of ensuring high quality of service.

The FCC justifies the information service retention on grounds that CDNs and other intermediaries do not offer public services providing access to all or most Internet sites.[32] However, this rationale ignores the primary role of these intermediaries: to facilitate the kinds of traffic prioritization, for compensation, that downstream ISPs cannot offer.[33] Thus, while ISPs directly serving end users cannot initiate such non-neutral service,[34] they can

30. Alexander Reicher, *Redefining Net Neutrality After Comcast v. FCC*, 26 BERKELEY TECH. L.J. 733, 759 (2011) ("By manipulating routing protocols, network administrators can also route traffic to overlay networks, which are physical additions to the Internet in the form of servers deployed widely across the Internet. Content Distribution Networks (CDNs) are some of the most popular overlays on the Internet today. They consist of servers distributed geographically across the Internet that retain a cache of the most frequently demanded content and services from publishers and providers. CDNs work by shortening the physical distance between the end-user and the content, enabling CDNs to optimize content delivery based on different criteria, including faster response time or optimal bandwidth costs.").

31. *See 2015 Open Internet Order*, para. 373 ("[T]his caching function provided by broadband providers as part of a broadband Internet service, is distinct from third party caching services provided by parties other than the provider of Internet access service (including content delivery networks, such as Akamai), which are separate information services.").

32. *2015 Open Internet Order*, para. 190 ("The Commission has historically distinguished these services from 'mass market' services and, as explained in the 2014 Open Internet NPRM, they 'do not provide the capability to receive data from all or substantially all Internet endpoints.'") (quoting *2014 Open Internet NPRM*, 29 FCC Rcd, para. 58). *See also 2010 Open Internet Order*, 25 FCC Rcd, para. 47 ("These services typically are not mass market services and/or do not provide the capability to transmit data to and receive data from all or substantially all Internet endpoints.").

33. The FCC acknowledges that CDNs can enhance quality of service to broadband service subscribers by promoting greater certainty that they can access content without delay: "We do not seek to disrupt the legitimate benefits that may accrue to edge providers that have invested in enhancing the delivery of their services to end users. On the contrary, such investments may contribute to the virtuous cycle by stimulating further competition and innovation among edge providers, to the ultimate benefit of consumers." *2015 Open Internet Order*, para. 128.

34. *2015 Open Internet Order*, para. 135 ("[W]e adopt a rule setting forth a no-unreasonable interference/disadvantage standard, under which the Commission can prohibit, on a case-by-case basis, practices that unreasonably interfere with or unreasonably disadvantage the ability of consumers to reach the Internet content, services, and applications of their choosing or of edge providers to access consumers using the Internet.").

and do interconnect with other ventures whose business plans emphasize such non-neutrality.[35] By extension, retaining the information service classification for CDNs and other intermediaries constrains the FCC's ability to prevent the widespread operation of biased networks offering "better than best efforts" traffic enhancement for specific types of traffic generated by specific content providers and distributors.

Last mile ISPs cannot favor specific traffic, but upstream ventures can provide quality of service enhancements, so that certain types of traffic reach the last mile ISP with less latency, and little, if any, circuitous routing.[36] Having reached the last mile ISP using expedited and prioritized treatment, CDN traffic then travels on a "best efforts" routing link for the last mile without losing the likelihood of high quality transmission for the entire link from content source to consumer.[37]

The FCC chose to emphasize that last mile ISPs have the potential to degrade upstream traffic flows.[38] Support for this emphasis lies in the widely publicized disputes between CDNs and content sources, on one hand, and last mile ISPs, such as Comcast, on the other hand.[39] However, in the

35. The FCC does not consider "better than best efforts" services provided by CDNs as a form of paid prioritization that the Commission prohibits retails ISPs from providing: "We also clarify that the ban on paid prioritization does not restrict the ability of a broadband provider and CDN to interconnect." *2015 Open Internet Order*, para. 128.

36. "Today, Akamai has application delivery networks that can accelerate entire web or IP-based applications, media delivery networks that provide HD-quality delivery of live and on-demand media . . .." Erik Nygren, Ramesh K. Sitaraman and Jennifer Sun, *The Akamai Network: A Platform for High-Performance Internet Applications*, https://www.akamai.com/us/en/multimedia/documents/technical-publication/the-akamai-network-a-platform-for-high-performance-internet-applications-technical-publication.pdf. "Variants of Paid Peering, Deep Caching, Assured Delivery or Secure M2M are among the innovative IP Interconnection business models that could lay the foundation for an advanced Internet platform, based on assured end-to-end Quality of Service Internet Platform – complementary to 'Best Effort'." Arthur D. Little &Liberty Global, *The Future of the Internet, Innovation and Investment in IP Interconnection*, 5 (May, 2014), http://www.libertyglobal.com/pdf/public-policy/Liberty-Global-2014-Future-Of-The-Internet.pdf.

37. "CDNs that support dynamic content create a "super highway" to accelerate the delivery of content across a longer distance. An individual ISP cannot provide this." John McIlwain, *How Content Delivery Networks Work* (April 13, 2015), http://www.cdnetworks.com/blog/how-content-delivery-networks-work/.

38. *See 2015 Open Internet Order*, para. 196.

39. "Using Measurement Lab (M-Lab) data, and constraining our research to the United States, we observed sustained performance degradation experienced by customers of Access ISPs AT&T, Comcast, Centurylink, Time Warner Cable, and Verizon when their traffic passed over interconnections with Transit ISPs Cogent Communications (Cogent), Level 3 Communications (Level 3), and XO Communications (XO). "In a large number of cases we observed similar patterns of performance degradation whenever and wherever specific pairs of Access/Transit ISPs interconnected. From this we conclude that ISP interconnection has a substantial impact on consumer internet performance --sometimes a severely negative impact -- and that business relationships between ISPs, and not major technical problems, are at the root of the problems we observed." Measurement Lab Consortium, *ISP Interconnection and its Impact on Consumer Internet Performance, A Measurement Lab Consortium Technical*

more frequent instances where the last mile ISP does not meddle with upstream traffic, the FCC ignores the fact that plain vanilla delivery does not dilute the network management and traffic prioritization accruing to CDN traffic upstream.[40] Thus, retaining the information service classification for upstream traffic makes it nearly impossible for the FCC to intervene when problems arise, because the prohibition on common carrier remedies severely limits the remedial actions that the Commission can undertake.

Notwithstanding the tension among its statutory interpretations, the FCC will have to convince a panel of the D.C. Circuit that the *2015 Open Internet Order* reasonably responds to changed circumstances.[41] Historically, the FCC has achieved comparatively greater success in defending regulatory streamlining, or abandonment,[42] than when it has to convince an appellate courts that changed circumstances warrant regulatory modifications.[43] The *2015 Open Internet Order* could face an even more

Report, 5 (Oct. 28, 2014), http://www.measurementlab.net/static/observatory/M-Lab_Interconnection_Study_US.pdf.

40. Dirk Grunwald, *The Internet Ecosystem: The Potential for Discrimination*, 63 FED. COMM. L.J. 411, 413 (2011) ("[C]ommercial content distribution networks can effectively provide 'preferential access' to content provisioned on a CDN located within an ISP's network without actually violating 'neutral' access network policies.").

41. *See 2015 Open Internet Order*, paras. 43-48.

42. *See, e.g*., *Earthlink, Inc. v. FCC*, 462 F.3d 1 (D.C. Cir. 2006) (affirming the FCC's decision to forbear from imposing most local loop unbundling requirements on incumbent carriers); U.S. Telecom Ass'n v. FCC, 359 F.3d 554, 588 (D.C. Cir. 2004) (upholding the FCC's nationwide decision to refrain from requiring § 251 unbundling fiber broadband elements and reversing the Commission's decision not to eliminate other unbundling requirements in light if the adverse impact on carrier investment incentives); *In re* Inquiry Concerning High-Speed Access to the Internet over Cable and Other Facilities, 17 FCC Rcd. 4798, 4821 (Mar. 15, 2002) (declaratory ruling and notice of proposed rulemaking), *aff'd sub nom*. Nat'l Cable & Telecomm. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 977-78 (2005)(affirming FCC decision to apply a statutory service definition triggering limited regulation).

43. *See, e.g.*, *In re* Implementation of the Local Competition Provisions in the Telecommunications Act of 1996, 11 FCC Rcd. 15,499 (1996) (first report and order), *aff'd in part, rev'd in part, AT&T Corp. v. Iowa Utils. Bd*., 525 U.S. 366 (1999); *In re* Implementation of the Local Competition Provisions of the Telecommunications Act of 1996, 15 FCC Rcd. 3696 (1999) (third report and order and fourth further notice of proposed rulemaking), *rev'd and remanded*, United States Telecom Ass'n v. FCC, 290 F.3d 415 (D.C. Cir. 2002) (rejecting the FCC's local exchange network unbundling requirements as insufficiently calibrated); *In re* Review of the Section 251 Unbundling Obligations of Incumbent Local Exchange Carriers, 16 FCC Rcd. 22,781 (2001); *In re* Review of the Section 251 Unbundling Obligations of Incumbent Local Exchange Carriers, 18 FCC Rcd. 16,978 (2003) (report and order and order on remand and further notice of proposed rulemaking), *corrected by* Errata, 18 FCC Rcd 19,020 (2003), *vacated and remanded in part, aff'd in part*, *United States Telecom Ass'n v. FCC*, 359 F.3d 554 (D.C. Cir. 2004) (the FCC should not implement statutory requirements that incumbent carriers cooperate with market entrants when the Commission determines that adequate marketplace competition exist); *FCC v. Midwest Video Corp*., 440 U.S. 689 (1979)(FCC mandated public access channels on cable television networks constituted unlawful common carrier duties).

skeptical court review because the FCC has identified the need for re-regulation, which would result in more extensive government oversight.

A. The FCC's 2015 Open Internet Order

In the *2015 Open Internet Order*, the FCC substantially changed its regulatory approach to network neutrality.[44] Rather than act on a reviewing court's invitation to impose non-common carrier, network neutrality rules, the Democratic majority of the FCC opted for clearer and more muscular, ex ante rules on remand.[45] The FCC reclassified elements of Internet access as a Title II regulated, common carrier service with no distinction between wireline and wireless ISPs.[46] The FCC will have to convince a reviewing court that the decision to reclassify broadband service as common carriage resulted from rational decision-making based on a complete record

---

44. Network neutrality refers to government-mandated nondiscrimination, transparency, and other requirements on ISPs designed to foster a level competitive playing field among content providers and to establish consumer safeguards so that Internet users have unrestricted access, limited only by legitimate concerns such as ISP network management and national security. *See 2010 Open Internet Order*, n.48 (2010). *See also generally* Barbara van Schewick, *Network Neutrality and Quality of Service: What a Nondiscrimination Rule Should Look Like*, 67 STAN L. REV. 1 (Jan. 2015); James B. Speta, Unintentional Antitrust: *The FCC's Only (and Better) Way Forward With Net Neutrality After the Mess of Verizon v. FCC*, 66 FED COMM. L.J. 491 (June, 2014); Amanda Leese, Note, *Net Transparency: Post-*Comcast *FCC Authority to Enforce Disclosure Requirements Critical to "Preserving the Open Internet,"* 11 NW J. TECH. & INTELL. PROP. 81 (2013); Daniel A. Lyons, *Net Neutrality and Nondiscrimination Norms in Telecommunications*, 54 ARIZ. L. REV. 1029 (2012); Adam Candeub & Daniel McCartney, *Law and the Open Internet*, 64 FED COMM. L.J. 493 (2012); Rob Frieden, *Rationales for and Against Regulatory Involvement in Resolving Internet Interconnection Disputes*, 14 YALE J.L. & TECH. 266 (2012); Dirk Grunwald, *The Internet Ecosystem: The Potential for Discrimination*, 63 FED COMM. L.J 411 (2011); Rob Frieden, *Assessing the Merits of Network Neutrality Obligations at Low, Medium and High Network Layers*, 115 PENN. ST. L. REV. 49 (2010); Christopher S. Yoo, *Innovations in the Internet's Architecture that Challenge the Status Quo*, 8 J. ON TELECOMM. & HIGH TECH. L. 79 (2010) Marvin Ammori, *Beyond Content Neutrality: Understanding Content-Based Promotion of Democratic Speech*, 61 FED COMM. L.J 273 (2009); Sascha D. Meinrath & Victor W. Pickard, *Transcending Net Neutrality: Ten Steps Toward an Open Internet*, 12 J. INTERNET L., Dec. 2008, at 1; Christopher S. Yoo, *Would Mandating Broadband Network Neutrality Help or Hurt Competition? A Comment on the End-To-End Debate*, 3 J. ON TELECOMM. & HIGH TECH. L. 23 (2004); Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. ON TELECOMM. & HIGH TECH. L. 141 (2003).

45. Regulatory agencies contemplating the potential for future conflicts and harm to competition and consumers create ex ante rules and regulations. Regulatory agencies and courts applying ex post remedies respond to complaints and law suits claiming harm that already has occurred. *SeeS* Rob Frieden, *Ex Ante Versus Ex Post Approaches to Network Neutrality: A Comparative Assessment*, BERKELEY TECH. L. J. (2015).

46. *See 2015 Open Internet Order*, para. 49. The FCC previously imposed less stringent rules on wireless carriers in light of spectrum use, greater potential for congestion and recent entry in broadband markets. The *2015 Open Internet Order*, however, treats wireless ISPs no differently than wireline ISPs. *See id.*, para. 88 (" conclude[ing] that it would benefit the millions of consumers who access the Internet on mobile devices to apply the same set of Internet openness protections to both fixed and mobile networks").

evidencing substantially changed circumstances occurring since 2002 when the FCC first classified Internet access as an information service.[47]

The *Order* emphasized the need for narrowly crafted rules designed to "prevent specific practices we know are harmful to Internet openness—blocking, throttling, and paid prioritization—as well as a strong standard of conduct designed to prevent the deployment of new [anticompetitive] practices that would harm Internet openness."[48] The Commission emphasized that ISPs have both the incentive and ability to leverage access in ways that can reduce incentives to innovate and invest in the Internet ecosystem:

> The key insight of the virtuous cycle is that broadband providers have both the incentive and the ability to act as gatekeepers standing between edge providers and consumers. As gatekeepers, they can block access altogether; they can target competitors, including competitors to their own video services; and they can extract unfair tolls.[49]

The FCC emphasized that while subjecting ISPs to Title II common carrier oversight, the Commission will use its statutory authority quite narrowly as evidenced by the decision to forbear50 from applying "27 provisions of Title II of the Communications Act, and over 700 Commission rules and regulations."[51] The Commission recognized the need to explain

---

47. "It is also well settled that we may reconsider, on reasonable grounds, the Commission's earlier application of the ambiguous statutory definitions of 'telecommunications service' and 'information service.'" *Id*. at para. 334. "The [Supreme] Court's application of . . . [the] *Chevron* test in *Brand X* makes clear our delegated authority to revisit our prior interpretation of ambiguous statutory terms and reclassify broadband Internet access service as a telecommunications service. The Court upheld the Commission's prior information services classification because 'the statute fails unambiguously to classify the telecommunications component of cable modem service as a distinct offering. This leaves federal telecommunications policy in this technical and complex area to be set by the Commission . . . .' Where a term in the Act 'admit[s] of two or more reasonable ordinary usages, the Commission's choice of one of them is entitled to deference.' The Court concluded, given the 'technical, complex, and dynamic' questions that the Commission resolved in the *Cable Modem Declaratory Ruling*, '[t]he Commission is in a far better position to address these questions than we are.'" *Id*. at para. 332 (citations omitted).

48. *Id*., para. 4. The FCC prohibits broadband Internet access providers from blocking the delivery of lawful traffic to consumers. Additionally ISPs cannot slow down traffic absent congestion and other compelling circumstances. ISPs also cannot create fast lanes with "better than best efforts" available at premium rates and slow lanes using best efforts routing likely to result in degraded service.

49. *Id*., para. 20.

50. 47 U.S.C § 160(a) authorizes the FCC to streamline the scope of its Title II oversight by forbearing from applying many common carrier requirements.

51. *Id.* at para. 5. The major provisions of Title II that the Order will apply are: nondiscrimination and no unjust and unreasonable practices under Sections 201 and 202; authority to investigate complaints and resolve disputes under section 208 and related enforcement provisions, specifically sections 206, 207, 209, 216 and 217; protection of

how the new requirements satisfy pressing needs, but in the most narrow and well-calibrated matter, in light of virulent opposition from most ISPs and the two Republican Commissioners. The *Order* reports that:

> [T]here will be fewer sections of Title II applied than have been applied to Commercial Mobile Radio Service (CMRS), [the regulatory classification for wireless voice telecommunications service] where Congress expressly required the application of Sections 201, 202, and 208, and permitted the Commission to forbear from others. In fact, Title II has never been applied in such a focused way.[52]

In addition to the specific prohibitions on blocking, throttling, and paid prioritization, the FCC established a general prohibition on ISP practices that unreasonably interfere with, or disadvantage downstream consumers and upstream edge providers of content, applications and services.[53] The Commission will consider, on a case-by-case basis, whether an ISP has engaged in a practice "that unreasonably interfere[s] with or unreasonably disadvantage[s] the ability of consumers to reach the Internet content, services, and applications of their choosing or of edge providers to access consumers using the Internet."[54] The Commission opted to apply more open-ended evaluative criteria than the legal standard it previously proposed, which would have prohibited commercially unreasonable practices.[55] The Commission concluded that, instead, it would "adopt a governing standard that looks to whether consumers or edge providers face unreasonable interference or unreasonable disadvantages, and makes clear that the standard is not limited to whether a practice is agreeable to commercial parties."[56]

---

consumer privacy under Section 222; fair access to poles and conduits under Section 224, protection of people with disabilities under Sections 225 and 255; and providing universal funding for broadband service, but not the requirement to collect contributions to such funding through partial application of Section 254.

52. *Id.* at para. 38.

53. *See id.*, para. 21.

54. *Id.* at para. 135.

55. *2014 Open Internet NPRM*, para. 10 ("[W]here conduct would otherwise be permissible under the no-blocking rule, we propose to create a separate screen that requires broadband providers to adhere to an enforceable legal standard of commercially reasonable practices, asking how harm can best be identified and prohibited and whether certain practices, like paid prioritization, should be barred altogether.").

56. *Id*., para. 150. The FCC identified a number of factors it will consider in future evaluations. These include an assessment whether a practice allows end-user control and is consistent with promoting consumer choice, its competitive effect, whether consumers and opportunities for free expression are promoted or harmed, the effect on innovation, investment, or broadband deployment, whether the practice hiders the ability of end users or edge providers to use broadband access to communicate with each other and whether a practice conforms to best practices and technical standards adopted by open, broadly

The FCC stated that it will use the "no-unreasonable interference/disadvantage" standard to evaluate controversial subjects including the lawfulness of "sponsored data" arrangements where an ISP accepts advertiser payment in exchange for an agreement not to meter and debit the downstream traffic delivery.[57] The FCC also will use this standard to consider the lawfulness of data caps that tier service by the amount of permissible downloading volume.[58] In both instances, the FCC sees the potential for an ISP to create artificial scarcity to extract higher revenues, to favor corporate affiliates and third parties willing to pay a surcharge, as well as the potential for disadvantaging competitors, e.g., using data caps to harm new vendors of video programming that compete with an ISP service.[59] On the other hand, the Commission also recognizes that service tiering can promote innovation and new, customized services.[60]

The *2015 Open Internet Order* expresses the view that reclassifying Internet access as a telecommunications service provides the strongest legal foundation for enforceable regulations, coupled with a secondary reference to Section 706 of the Telecommunications Act of 1996[61] and Title III,[62] which addresses the use of radio spectrum and applies common carriage regulation to wireless voice carriers.[63] By using the stronger Title II foundation, the FCC asserts that it can establish clear and unconditional statutory authority, but also use the flexibility to forbear[64] from applying

representative, and independent Internet engineering, governance initiatives, or standards-setting organization. *Id.*, paras. 139-145.

57. *See id.* paras. 151-53.

58. *See id.* para. 122.

59. *2015 Open Internet Order*, para. 82 ("Broadband providers may seek to gain economic advantages by favoring their own or affiliated content over other third-party sources. Technological advances have given broadband providers the ability to block content in real time, which allows them to act on their financial incentives to do so in order to cut costs or prefer certain types of content. Data caps or allowances, which limit the amount and type of content users access online, can have a role in providing consumers options and differentiating services in the marketplace, but they also can negatively influence customer behavior and the development of new applications.").

60. *Id*., para. 351 ("Furthermore, fixed broadband providers use transmission speeds to classify tiers of service offerings and to distinguish their offerings from those of competitors.").

61. 47 U.S.C. § 1302 (2014).

62. 47 U.S.C. § 301-399B (2014).

63. *See 2015 Open Internet Order*, paras. 273-74; *see also* Mobile Services, 47 U.S.C. § 332 (2014). "We ground the open Internet rules we adopt today in multiple sources of legal authority—section 706, Title II, and Title III of the Communications Act. We marshal all of these sources of authority toward a common statutorily-supported goal: to protect and promote Internet openness as platform for competition, free expression and innovation; a driver of economic growth; and an engine of the virtuous cycle of broadband deployment. We therefore invoke multiple, complementary sources of legal authority. As a number of parties point out, our authority under section 706 is not mutually exclusive with our authority under Titles II and III of the Act."

64. 47 U.S.C. § 160(a)(1)-(3) ("Notwithstanding section 332(c)(1)(A) of this Act, the Commission shall forbear from applying any regulation or any provision of this Act to a telecommunications carrier or telecommunications service . . . if the Commission determines

unnecessary common carrier requirements, as has occurred for wireless telephone service.[65] With a Title II regulatory foundation, the *Order* also makes it possible for the FCC to create an open Internet conduct standard that ISPs cannot harm consumers or edge providers with enforcement tools available to sanction violations.66

The FCC's decision to treat Internet access as common carriage triggered petitions for judicial review, asking the courts to decide whether the reclassification constitutes a reasonable decision based on a complete evidentiary record. By opting for the reclassification option, the FCC underscores the riskiness in imposing ex ante regulation without an explicit legislative mandate.[67]

III. THE VARIABLE BURDENS OF APPELLATE REVIEW FOR FCC REGULATIONS

The FCC achieves greater success on judicial review when it reduces its regulatory wingspan as compared to instances where it changes the nature of regulation, or imposes new and more burdensome regulations. This section will examine case precedent addressing FCC decisions that change the scope and reach of its oversight. A deregulatory decision typically passes judicial muster unless explicit statutory language requires specific action.[68]

---

that (1) enforcement of such regulation or provision is not necessary to ensure that the charges, practices, classifications, or regulations by, for, or in connection with that telecommunications carrier or telecommunications service are just and reasonable and are not unjustly or unreasonably discriminatory; (2) enforcement of such regulation or provision is not necessary for the protection of consumers; and (3) forbearance from applying such provision or regulation is consistent with the public interest.").

65. 47 U.S.C. § 332 (c)(1)(A) ("A person engaged in the provision of a service that is a commercial mobile service shall, insofar as such person is so engaged, be treated as a common carrier for purposes of this Act, except for such provisions of title II as the Commission may specify by regulation as inapplicable to that service or person.").

66. With an eye toward providing timely, certain and flexible enforcement of its open Internet rules, the FCC announced its intention to use advisory opinions similar to those issued by the Department of Justice's Antitrust Division. *See generally 2015 Open Internet Order*, paras. 229-239 (discussing the advisory opinion process). Advisory opinions will enable companies to seek guidance on the propriety of certain open Internet practices before implementing them, enabling them to be proactive about compliance and avoid enforcement actions later. The FCC may use advisory opinions to explain how it will evaluate certain types of behavior and the factors that will be considered in determining whether open Internet violations have occurred. Because these opinions will be publicly available, we believe that they will reduce the number of disputes by providing guidance to the industry." *See id.* para. 229.

67. *See* Rob Frieden, *Ex Ante Versus Ex Post Approaches to Network Neutrality: A Comparative Assessment*, xx BERKLEY TECH. L.J. xx (2015).

68. "[I]n examining rulemaking and transitions in all three branches of government from the agency's perspective, it may be most helpful to consider how the agency analyzes the costs and benefits of rulemaking. This cost-benefit calculation is quite different than the one typically discussed in administrative law—whether a particular regulation has net benefits to society. Instead, the calculation considers the net benefits of a rulemaking, both in terms of

When the FCC changes regulatory requirements of ventures already subject to oversight, appellate courts typically affirm the decision absent evidence that the Commission failed to generate a complete evidentiary record,[69] when it chose to ignore relevant information,[70] or when it devised unreasonable rules and regulations.[71] The FCC's *2015 Open Internet Order* creates a new category where the FCC seeks to re-regulate, an outcome likely to trigger very close scrutiny of the factual and legal rationales used by the Commission.

A. Streamlining and Deregulation

When the FCC reduces, streamlines, or eliminates regulation, it likely receives the benefit of the doubt from reviewing courts based on reasonably anticipated competitive and consumer benefits.[72] Prevailing

---

substance and process, to an agency in light of the particular costs to the agency. On the benefit side, the agency may care about the regulatory outcome; budgetary, political, and status rewards; and judicial deference. On the cost side, the agency may worry about regulatory outcome; budgetary, political, and status fallout; and reversal by the courts. Anne Joseph O'Connell, *Agency Rulemaking and Political Transitions*, 105 NW. U. L. REV. 471, 487 (2011). Even though regulatory agencies arguably have identical statutory obligations when regulating and deregulating, *see* Motor Vehicles Manufacturers Association v. State Farm, 463 U.S. 29 (1983)(subjecting reduced seat belt requirements to same arbitrary standard as one that would have imposed greater requirements), they likely accrue dividends with the public, Congress and the courts when showing how deregulation will promote efficiency, possibly lead to lower consumer costs and stimulate competition.

69. "When an agency departs from past practice, it 'must provide a reasoned analysis indicating that prior policies and standards are being deliberately changed, not casually ignored.'" CBS Corp. v. FCC, 785 F.3d 699, 708 (D.C. Cir. 2015) (quoting Ramaprakash v. FAA, 346 F.3d 1121, 1124 (D.C. Cir. 2003)).

70. *See, e.g.*, Am. Radio Relay League, Inc. v. FCC, 524 F.3d 227, 231 (2008) (FCC "failed to satisfy the notice and comment requirement of the Administrative Procedure Act ('APA') by redacting studies on which it relied in promulgating the rule and failed to provide a reasoned explanation for its choice of the extrapolation factor

for" predicting how quickly broadband over powerline (BPL) emissions attenuate or weaken); *see also* Administrative Procedure Act, 5 U.S.C. § 553(b)-(c) (2014).

71. In *Schurz Commc'ns, Inc. v. FCC*, 982 F.2d 1043 (7th Cir. 1992), the Seventh Circuit rejected the FCC's attempt to modify rules designed to limit broadcast networks' control of programming aired by affiliates, including a rule limiting to 40 percent how much of a network's own prime-time entertainment schedule may consist of programs produced by the network itself. The court strongly admonished the FCC:

The Commission's articulation of its grounds is not adequately reasoned. Key concepts are left unexplained, key evidence is overlooked, arguments that formerly persuaded the Commission and that time has only strengthened are ignored, contradictions within and among Commission decisions are passed over in silence. The impression created is of unprincipled compromises of Rube Goldberg complexity among contending interest groups viewed merely as clamoring suppliants who have somehow to be conciliated. . . . The Commission must do better in articulating

their justification. *Id.* at 1050.

72. *Ad Hoc Telecomms. Users Comm. v. FCC*, 572 F.3d 903, 908 (D.C. Cir. 2009) (citing EarthLink, Inc. v. FCC, 462 F.3d 1, 12 (D.C. Cir. 2006)) ("Our task on review is therefore limited. We review the FCC's action in this case only to ensure that it is not 'arbitrary,

political and economic doctrine typically support the reduction of government oversight based on the view that this will reduce market distortions, place greater reliance on marketplace self-regulation, promote innovation, stimulate investment, and benefit consumers. [73]

Opposition to reduced or eliminated regulation sometimes occurs when disputes arise whether public benefits will actually accrue and when a stakeholder determines that it would achieve higher revenues under the status quo. For example, incumbent local and long distance telephone carriers opposed an FCC plan to remove the requirement that all carriers file and adhere to tariffs, which are public contracts specifying, in painstaking detail, the terms and conditions of every type of service.[74] While tariff filing reduced the speed and flexibility in which carriers specified service terms, incumbent carriers benefitted from the insulation from liability that these public contracts accorded as well as the ability to standardize service into a small number of tariffs.[75]

In the case, *MCI Telecommunications Corp. v. FCC*,[76] the District of Columbia Circuit overturned the FCC's deregulatory decision, reasoning that the Commission lacked explicit statutory authority to eliminate the tariff-filing requirement contained in Section 203(b)(2) of the

---

capricious, an abuse of discretion, or otherwise not in accordance with law.' 5 U.S.C. § 706(2)(A). That standard is particularly deferential in matters such as this, which implicate competing policy choices, technical expertise, and predictive market judgments."); *see also Time Warner Telecom, Inc. v. FCC*, 507 F.3d 205, 221 (3d Cir. 2007).

73. For example, the D.C. Circuit Court of Appeals rejected FCC-imposed caps on cable television national market share on grounds that the FCC did not fully consider the extent of current competition:

> [T]he Commission has failed to demonstrate that allowing a cable operator to serve more than 30 percent of all cable subscribers would threaten to reduce either competition or diversity in programming. First, the record is replete with evidence of ever increasing competition among video providers: Satellite and fiber optic video providers have entered the market and grown in market share since the Congress passed the 1992 Act, and particularly in recent years. Cable operators, therefore, no longer have the bottleneck power over programming that concerned the Congress in 1992. Second, over the same period there has been a dramatic increase both in the number of cable networks and in the programming available to subscribers.

Comcast Corp. v. FCC, 579 F.3d 1,7 (D.C. Cir. 2009).

74. Policy & Rules Concerning Rates for Competitive Common Carrier Services & Facilities Authorizations Therefor, *First Report and Order*, 85 F.C.C. 2d 1(1980), *Second Report and Order*, 91 F.C.C. 2d 59 (1982), *Fourth Report and Order*, 95 F.C.C. 2d 554 (1983), *Sixth Report and Order*, 99 F.C.C. 2d 1020 (1985), *reversed sub nom*.,. *MCI Telecommunications Corp. v. AT & T*, 512 U.S. 218 (1994).

75. *See Am. Tel. & Tel. Co. v. Cent. Office Tel., Inc.*, 524 U.S. 214 (1998)(filed rate doctrine bars claims against a utility that conflict with its tariff or claims that would vary or enlarge a party's rights as defined by the tariff).

76. *MCI Telecomm. Corp. v. FCC* , 765 F.2d 1186 (D.C. Cir. 1985), *aff'd*, MCI Telecommn's Corp. v. AT&T 512 U.S. 218 (1994).

Communications Act.[77] The Supreme Court affirmed the lower court, holding that the FCC cannot ignore a clear and unambiguous statutory requirement:

> The dispute between the parties turns on the meaning of the phrase "modify any requirement" in § 203(b)(2). Petitioners argue that it gives the Commission authority to make even basic and fundamental changes in the scheme created by that section. We disagree. The word "modify"—like a number of other English words employing the root "mod-" (deriving from the Latin word for "measure"), such as "moderate," "modulate," "modest," and "modicum"—has a connotation of increment or limitation. Virtually every dictionary we are aware of says that "to modify" means to change moderately or in minor fashion.[78]

B. New or Revised Regulation When the Statutory Mandate Contains Ambiguities

Many appellate cases involving the FCC address the lawfulness of a new or revised regulatory regime.[79] The standard of review turns, in large part, on whether the FCC can demonstrate that it reasonably interpreted and applied ambiguous statutory language, compiled a complete evidentiary record, and generated a decision that does not appear arbitrary, capricious or an abuse of discretion.[80] For instances where the FCC can show ambiguity exists in the statutory language, the review standard, commonly referred to

77. *See* MCI Telecomm. Corp. v. FCC, 765 F.2d 1186 (D.C. Cir. 1985); *see also* 47 U.S.C. § 203(b)(2) (2013).

78. *MCI Telecommunications Corp. v. FCC* , 512 U.S. 218, 225 (1994).

79. "[A regulatory] agency must examine the relevant data and articulate a satisfactory explanation for its action including a rational connection between the facts found and the choice made." Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983). Qwest Corp. v. FCC, 258 F.3d 1191, 1198-99 (10th Cir. 2001) (citing Olenhouse v. Commodity Credit Corp., 42 F.3d 1560, 1575 (10th Cir. 1994) (determining that the FCC failed to provide adequate justifications to prove rational decision making in calculating subsidy mechanism for promoting universal service in high cost areas) ("If the agency has failed to provide a reasoned explanation for its action, or if limitations in the administrative record make it impossible to conclude the action was the product of reasoned decision-making, the reviewing court may supplement the record or remand the case to the agency for further proceedings. It may not simply affirm.")).

80. Under the Administrative Procedure Act ("APA"), federal courts have an obligation to set aside an agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A) (2013). *See also* Caroline Cecota & W. Kip Viscusi, *Judicial Review of Agency Benefit-Cost Analysis*, 22 GEO. MASON L. REV.. 575, 575 (2015) [hereinafter Cecota & Viscusi] ("In essence, the APA tasks courts with ensuring that federal agency action is reasonable--or rather, that agencies base their actions on relevant and reliable data and articulate a rational connection between the evidence and their actions.").

as the *Chevron* Doctrine,[81] requires the FCC to demonstrate that its interpretation is reasonable.[82]

An appellate court may affirm the FCC even when a rule change results in an expansion of its regulatory wingspan, or prevents states and localities from creating their own regulations.[83] For example, the FCC successfully defended its decision to subject Voice over the Internet Protocol ("VoIP")[84] telephone services to substantial regulation, despite never stating that VoIP constitutes a telecommunications service.[85] The FCC avoided stating that VoIP constituted the functional equivalent of common carrier voice telephone service[86] because doing so probably would have qualified VoIP providers to receive universal service subsidies and other entitlements

---

81. *See Chevron v. Natural Resources Defense Council, Inc*., 467 U.S. 837 (1984).

82. "First, Chevron directed courts to determine whether the relevant statutory language was clear and on point using traditional tools of statutory interpretation. If the statutory language were clear, the agency would have to follow Congress's unambiguously expressed instruction. If Congress's intentions were unclear and the language were open to multiple interpretations, then in step two the court would defer to the agency's interpretation as long as the interpretation was permissible and not foreclosed by the statutory language. The Chevron method was to give more leeway to the agency, acknowledging its interpretative mandate from Congress to implement the statute and its relative expertise in regulatory affairs as compared to the courts." Cecota & Viscusi, *supra*, at 585.

83.

84. VoIP is the real-time carriage and delivery of data packets that correspond to voice. VoIP services range in quality, reliability, and price and can link both computers and ordinary telephone handsets. For technical background on how VoIP works, see Susan Spradley & Alan Stoddard, *Tutorial on Technical Challenges, Associated with the Evolution to VoIP*, FCC (Sept. 22, 2003), http://www.fcc.gov/events/ tutorial-technical-challenges-associated-evolution-voip. *See also generally*, Charles J. Cooper & Brian Stuart Koukoutchos, *Federalism and the Telephone: The Case for Preemptive Federal Deregulation in the New World of Intermodal Competition*, 6 J. TELECOM & HIGH TECH. L.293 (2008).

85. Vonage Holdings Corp.'s Petition for Declaratory Ruling Concerning an Order of the Min. Pub. Utils. Comm'n, *Memorandum Opinion & Order*, FCC 04-267, 19 FCC Rcd 22404 (2004), *aff'd. sub nom*, *Minn. Pub. Utils. Comm'n v. FCC*, 483 F.3d 570 (8th Cir. 2007). "Today, interconnected VoIP providers must contribute to universal service,78 offer access to law enforcement subject to legitimate wiretaps, provide E911 emergency service, support users with disabilities, protect the privacy of customer information they use to complete calls, offer number portability, and report service outages. The FCC has adopted all these requirements, which have been relatively uncontroversial, without ever having to decide whether certain forms of VOIP fall under the definition of "telecommunications service" subject to Title II of the Communications Act." Kevin Werbach, *Reflections on Network Transitions and Social Contracts for the Broadband World*, 13 COLO. TECH. L.J. 45, 65 (2015).

86. "Vonage Holdings is an interesting example of the FCC's continuing refusal to classify VoIP as either a telecommunications service or an information service. Extrapolating from the FCC argument accepted by the D.C. Circuit leads to the conclusion that offerors of either telecommunications or information services may provide telecommunications as one component of services offered. As such, other Title II requirements also using the verb 'provide' may be applied to interconnected VoIP without having to define its type of service. In effect, the FCC has established a means of regulating VoIP implementations outside of the telecommunications/information services dichotomy in addition to exercises of its ancillary Title I authority." Marc Elzweig, *D, None of the Above: On the FCC Approach to VoIP Regulation*, 2008 U. CHI. LEGAL F. 489, 503 (2008)[hereinafter cited as Elzweig].

reserved for telephone companies.[87] The FCC also avoided applying the information service classification, because this attribution would have limited the scope of regulatory safeguards it could apply,[88] just as has occurred for broadband Internet access.[89]

The FCC invoked its "ancillary jurisdiction"[90] to justify regulation, based on its determination that VoIP could adversely impact existing voice telephone service subscribers as well as carriers already subject to common carrier regulation.[91] Not only did the FCC convince the Eighth Circuit that

87. "The FCC has in the past relied upon its ancillary authority under Title I of the Act to create universal service contribution obligations for interconnected VoIP providers, but has not made VoIP services eligible for funding for universal service. Although the FCC applied contribution obligations on interconnected VoIP providers for calls that did not actually touch the PSTN, it based its decision on the fact that interconnected VoIP services in general still offer the capability of reaching the PSTN." Jodie Griffin, *Universal Service in an All-IP World*, 23 COMMLAW CONSPECTUS 346, 351 (2015).

88. By avoiding classifying VoIP as either an information service or a telecommunications service, the FCC has flexibility to determine the proper mix of regulatory duties and freedoms. "With VoIP, the FCC has differentiated among implementations, determining some to be telecommunications services and some to be information services, while others remain unclassified. Some VoIP implementations are heavily regulated, while others are not regulated at all. For VoIP services not yet placed in either category, the FCC has imposed incremental, targeted regulations through a series of orders. This treatment is a notable departure from past FCC regulatory actions, and responses are varied. Some argue that the FCC should declare VoIP an information service and leave it unregulated. Other commentators have criticized the regulations that have been applied, and still others have taken this departure as a signal that markedly different regulation regimes should be applied." Elzweig, 2008 U. CHI. LEGAL F. at
490-91.

89. *See generally*, *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014) (holding that because the FCC, under its prior regulatory regime, classified broadband providers as entities exempt from common carrier obligations, "the Communications Act expressly prohibits the [FCC] from . . . regulating them as such").

90. The FCC relies on a claim of ancillary jurisdiction when the Commission lacks explicit statutory authority. The FCC successfully invoked ancillary jurisdiction to regulate cable television even before the Commission received a statutory mandate to do so. "The FCC needed a hook to assert jurisdiction over cable. To reach that goal, it used a two-step process. First, the Commission found that cable was within its primary statutory grant of authority under section 152(a) of the [Communications] Act, which allows the FCC to regulate 'all interstate and foreign communication by wire or radio.' Second, the FCC invoked section 303(r) of the Act, which allows the Commission to issue 'such rules and regulations and prescribe such restrictions and conditions, not inconsistent with law,' as 'public convenience, interest, or necessity requires.' The FCC also referenced section 154(i), which provides that '[t]he Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with [the Communications Act], as may be necessary in the execution of its functions.' Kevin Werbach, *Off the Hook*, 95 CORNELL L. REV. 535, 572 (2010) (citations omitted).

91. *See Nuvio Corp. v. FCC*, 473 F.3d 302 (D.C. Cir. 2006) (requiring interconnected VoIP service providers to supply 911 emergency calling capabilities); Vonage Holdings Corp. v. F.C.C., 489 F.3d 1232 (D.C. Cir. 2007) (affirming the FCC's decision to require VoIP operators to contribute to universal service funds); In re Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007)

the Commission should have jurisdiction over VoIP service, the court also upheld the FCC's preemption of state regulation that could interfere with formation of a single, national regulatory policy.[92]

A successful claim of ancillary jurisdiction allows the FCC to apply existing, direct statutory authority to new technologies and ventures.[93] The FCC first applied this strategy in defending cable television regulations, which it argued were necessary to prevent economic harm to incumbent, regulated television broadcasters, despite the lack of explicit statutory authority to regulate cable television operators.[94]

In the recent case of *Cellco Partnership v. FCC*,[95] the FCC succeeded in convincing the District of Columbia Circuit that it has the jurisdiction and the power to impose rules requiring wireless carriers to provide Internet access to visitors, despite the fact that the service in question constituted an information service and not regulated voice telephone service.[96] In its Order, the FCC mandated that all cellphone companies interconnect their wireless data networking capabilities, so that users temporarily located outside their home service territory can continue to access Internet services.[97] The Court accepted the FCC's rationale for requiring wireless carriers to provide data service to "roaming" subscribers of another company because the FCC previously had ordered these companies to provide roaming for their voice telephone services, a common carrier service, so that roamers could continue to make and receive calls.[98] Even though the FCC lacked statutory authority to regulate information services, which at the time included wireless data service, the Court agreed that ensuring the continuity of attendant data services was ancillary to its voice-roaming requirement.[99] In so holding, the Court accepted the rationale

(extending customer proprietary network information obligations to interconnected VoIP service providers), aff'd sub nom. Nat'l Cable & Telecom. Assoc. v. FCC, 555 F.3d 996 (D.C. Cir. 2009); Matters of Local Number Portability Porting Interval and Validation, Report and Order, 25 FCC Rcd 6953 (2010) (establishing fast deadlines for migrating a telephone service subscriber to and from VoIP service); The Proposed Extension of Part 4 of the Commission's Rules Regarding Outage Reporting to Interconnected Voice Over Internet Protocol Service Providers and Broadband Internet Service Providers, Report and Order, 27 FCC Rcd 2650 (2012) (requiring VoIP carriers to report service outages).

92. *See Minn. Pub. Utils. Comm'n*, 483 F.3d at 581 ("After carefully considering the positions presented by both sides of this dispute, we conclude the FCC did not arbitrarily or capriciously determine state regulation of VoIP service would interfere with valid federal rules or policies.").

93. *See, e.g.*, *Vonage Holding Corp. v. FCC*, 489 F.3d 1232 (D.C. Cir. 2007) (affirming FCC regulatory oversight of VoIP and preempting state deregulation or inconsistent regulation).

94. *See* United States v. Sw. Cable Co., 392 U.S. 157 (1968); *see also* United States v. Midwest Video Corp. (Midwest Video I), 406 U.S. 649 (1972).

95. *Cellco P'ship v. FCC*, 700 F.3d 534 (D.C. Cir. 2012).

96. *See id.*

97. *See id.*

98. *See id.*

99. *See id.* at 544 ("[G]iven the 'high level of deference due to an agency in interpreting its own orders and regulations,' we have little difficulty concluding that the Commission's

that the FCC's ancillary jurisdiction enables the Commission to leverage existing statutory authority over incumbent technologies to regulate related new technologies that would otherwise be exempt from common carrier regulation.[100] In this case, because the FCC had direct statutory authority to mandate wireless voice roaming interconnection under Titles II and III of the Communications Act, the FCC could impose a duty to deal between wireless carriers, so long as the requirements did not rise to the level of common carriage.[101]

Under *Chevron*, the can FCC change the scope and emphasis of its regulatory mission based on changed circumstance and a new evidentiary record.[102] For example, in *In re FCC 11–161* (Universal Service Reform Affirmance),[103] the Tenth Circuit upheld a substantially revised and refocused universal service regime that establishes surcharges on voice telephone service subscribers to subsidize carrier voice and broadband services in high cost areas.[104] This case provides strong validation of judicial deference to regulatory agency expertise when the applicable statutes either lack specificity, provide multiple objectives, or contemplate changed circumstances necessitating revised implementation.[105] In this case, the court

---

classification of the voice roaming rule as a common carrier obligation does not amount to a conclusion that automatic-roaming requirements necessarily entail common carriage.") (citing *MCI Worldcom Network Servs v. FCC*, 274 F.3d 542, 548 (D.C. Cir. 2001)). The Court also noted that, "the data roaming rule imposes obligations that differ materially from the kind of requirements that necessarily amount to common carriage," *id*. at 547, and "the data roaming rule leaves substantial room for individualized bargaining and discrimination in terms." *Id.* at 548.

100. *See id.*

101. *See id.*

102. *2015 Open Internet Order*, para. 332 ("[The] *Chevron* test in *Brand X* [which affirmed the information service classification to cable modem, Internet access] makes clear our delegated authority to revisit our prior interpretation of ambiguous statutory terms and reclassify broadband Internet access service as a telecommunications service.").

103. *In re FCC 11–161* (*Universal Service Reform Affirmance*), 753 F.3d 1015 (10th Cir. 2014),

104. *In re FCC 11–161* (*Universal Service Reform Affirmance*), 753 F.3d 1015 (10th Cir. 2014). *See also* Connect America Fund, A National Broadband Plan for Our Future, Establishing Just and Reasonable Rates for Local Exchange Carriers, High-Cost Universal Service Support; Developing a Unified Inter carrier Compensation Regime; Federal-State Joint Board on Universal Service; Lifeline and Link-Up, and Universal Service Reform Mobility Fund, *Report and Order and Further Notice of Proposed Rulemaking*, 26 FCC Rcd 17663 (2011), *affirmed sub nom*., *In re* FCC 11–161, 753 F.3d 1015 (10th Cir. 2014). *See also* Connect America Fund, *Report and Order and Further Notice of Proposed Rulemaking*, 26 FCC Rcd 17663, 27 FCC Rcd 4040 (2011); Connect America Fund, *Report and Order*, 28 FCC Rcd 15060 (2013); Universal Service Implementation Progress Report, WC 10-90 (Wireline Comp. Bur. Mar. 24, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-326217A1.pdf.

105."Instead, as the FCC suggests, it is reasonable to conclude that Congress left a gap to be filled by the FCC, i.e., for the FCC to determine and specify precisely how USF funds may or must be used. And, as the FCC explained in the Order, carriers 'that benefit from public investment in their networks must be subject to clearly defined obligations associated with

deferred to the FCC's interpretation of its statutory authority, finding that the statute was ambiguous and the Commission acted reasonably in its interpretation of the statute.

The court affirmed the FCC decision to expand the USF mission to include fixed line and wireless broadband services without having qualified these ventures as conventional common carriers solely providing telecommunications services.[106] For example, the court closely examined the FCC's use of Section 254 of the Communications Act to grant it authority to redirect the USF mission largely to broadband information services:

> [I]t is beyond dispute that subsection (c)(1) expressly authorizes the FCC to define "periodically" the types of telecommunications services that are encompassed by "universal service" and thus "supported by Federal universal service support mechanisms." Further, there is no question that the FCC, to date, has interpreted the term "telecommunications services" to include only telephone services and not VoIP or other broadband internet services. All that said, however, nothing in the language of subsection (c)(1) serves as an express or implicit limitation on the FCC's authority to determine what a USF recipient may or must do with those funds. More specifically, nothing in subsection (c)(1) expressly or implicitly deprives the FCC of authority to direct that a USF recipient, which necessarily provides some form of "universal service" and has been deemed by a state commission or the FCC to be an eligible telecommunications carrier under 47 U.S.C. § 214(e), use some of its USF funds to provide services or build facilities related to services that fall outside of the FCC's current definition of "universal service." In other words, nothing in the

---

the use of such funding.'" *In re FCC 11–161 (Universal Service Reform Affirmance)*, 753 F.3d at 1046, quoting JA at 418 (Order Id. 74).

106. "The fact remains, however, that in order to obtain USF funds, a provider must be designated by the FCC or a state commission as an "eligible telecommunications carrier" under 47 U.S.C. § 214(e). See 47 U.S.C. § 254(e) ('only an eligible telecommunications carrier designated under section 214(e) ... shall be eligible to receive specific Federal universal service support.'). And, under the existing statutory framework, only 'common carriers,' defined as 'any person engaged as a common carrier for hire ... in interstate or foreign communication by wire or radio or in interstate or foreign radio transmission of energy,' 47 U.S.C. § 153(10), are eligible to be designated as 'eligible telecommunications carriers,' 47 U.S.C. § 214(e). Thus, under the current statutory regime, only ETCs can receive USF funds that could be used for VoIP support. Consequently, there is no imminent possibility that broadband-only providers will receive USF support under the FCC's Order, since they cannot be designated as 'eligible telecommunications carriers.' As a result, we agree with the FCC that the petitioners' argument 'will not be ripe for judicial review unless and until a state commission (or the FCC) designates ... an entity' that is not a telecommunications carrier as "an 'eligible telecommunications carrier' " under § 214(e). *In re FCC 11–161 (Universal Service Reform Affirmance)*, 753 F.3d at 1048-49, quoting FCC Br. 3 at 5.

> statute limits the FCC's authority to place conditions, such as the broadband requirement, on the use of USF funds.[107]

The court accepted the view that the Commission can allocate universal service funds for both services and facilities, the latter including advanced broadband facilities used by carriers to provide both telecommunications services, e.g., voice telephony and advanced services, including broadband Internet access that might fit into either telecommunication services or information services:

> The FCC also, in our view, reasonably concluded that Congress's use of the terms "facilities" and "service" in the second sentence of § 254(e) afforded the FCC "the flexibility not only to designate the types of telecommunications services for which support would be provided, but also to encourage the deployment of the types of facilities that will best achieve the principles set forth in section 254(b). [108]

The court also examined whether and how Section 706(b) of the Communications Act granted the FCC an independent grant of authority to revise the USF mission to include broadband services without having to invoke other sections of the Act. The court confirmed that the FCC could use this authority, established in the Telecommunications Act of 1996, to make reasonable recalibrations of the universal service mission in light of the new mandate to promote timely access to advanced telecommunications capabilities[109] which the FCC has interpreted to include broadband Internet access:

---

107. *Id*. 753 F.3d at 1046. The court concluded that "the FCC's interpretation of § 254(e) is not 'arbitrary, capricious, or manifestly contrary to the statute.' (citing *Chevron*, 467 U.S. at 844). Congress clearly intended, by way of the second sentence of § 254(e), to mandate that USF funds be used by recipients 'only for the provision, maintenance, and upgrading of facilities and services for which the support is intended.' And it seems highly unlikely that Congress would leave it to USF recipients to determine what "the support is intended" for. Instead, as the FCC suggests, it is reasonable to conclude that Congress left a gap to be filled by the FCC, i.e., for the FCC to determine and specify precisely how USF funds may or must be used. And, as the FCC explained in the Order, carriers 'that benefit from public investment in their networks must be subject to clearly defined obligations associated with the use of such funding.' *Id*. (citations omitted).

108. *Id*. 753 F.3d at 1046-47; *see also* Am. Family Ass'n, Inc. v. FCC, 365 F.3d 1156, 1166 (D.C. Cir. 2004). "We must defer to the Commission's expert judgment in the absence of record evidence indicating that the Commission's assumption is a clear error of judgment, or a showing that the empirical assumption is facially implausible or inconsistent." Id. at 1165 (FCC's method for assigning noncommercial educational broadcast licenses among competing applicants deemed valid).

109. The term 'advanced telecommunications capability' is defined, without regard to any transmission media or technology, as high-speed, switched, broadband telecommunications

> In contrast, section 706(b) requires the FCC to perform two related tasks. First, the FCC must conduct an annual inquiry to "determine whether advanced telecommunications capability is being deployed to all Americans in a reasonable and timely fashion." Second, and most importantly for purposes of this appeal, if the FCC's annual "determination is negative," it is required to "take immediate action to accelerate deployment of such capability by removing barriers to infrastructure investment and by promoting competition in the telecommunications market." Unlike section 706(a), section 706(b) does not specify how the FCC is to accomplish this latter task, or otherwise refer to forms of regulatory authority that are afforded to the FCC in other parts of the Act. As the FCC concluded in the Order, section 706(b) thus appears to operate as an independent grant of authority to the FCC "to take steps necessary to fulfill Congress's broadband deployment objectives," and "it is hard to see what additional work section 706(b) does if it is not an independent source of authority."[110]

The court sequentially examined the numerous changes in universal service funding and in each instance affirmed the FCC's actions. These actions include the Commission's determination of USF support amounts, the decision to limit ongoing voice telephony subsidies to incumbent carriers, but to eliminate all support in locations, previously deemed high cost areas, where an unsubsidized competitor offers voice and broadband throughout the specified service area. The court also affirmed the FCC's decision to use reverse auctions to determine which carrier will receive USF funding and how much it will receive.

In contrast to the FCC's perceived need to make an explicit regulatory reclassification in its *2015 Open Internet Order*, the 10th Circuit Court of Appeals affirmed the FCC without requiring it to provide reasons for including information services to the array of services, qualifying for universal service subsidization. The FCC was able to mandate surcharges of basic telecommunications services to generate funds used to expand the reach and affordability of both voice and data service without any question whether the Commission had statutory authority to subsidize information service for which it then lacked jurisdiction to regulate.[111]

---

capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology. 47 U.S.C. § 1302.

110. *Universal Service Reform Affirmance*, 753 F.3d at 1053-54.

111. The FCC also has established a subsidy mechanism to promote universal broadband access in schools and libraries. *See* Modernizing the E-rate Program for Schools and Libraries, WC Docket No. 13-184, Order and Further Notice of Proposed Rulemaking, 29 F.C.C. R. 8870 (2014); Modernizing the E-rate Program for Schools and Libraries, WC Docket No. 13-

On the other hand, the FCC twice failed to convince an appellate court that ancillary jurisdiction should apply to broadband Internet access, because the reviewing court considered the requirements as imposing illegal common carrier duties. While the Commission could readily demonstrate that unregulated broadband operators could harm competition and consumers, the appellate court rejected the nature and scope of the proposed safeguards. The D.C. Circuit Court of Appeals held that the FCC could not lawfully impose common carrier regulations on broadband service providers having previously determined that these ventures operate as private carriers offering information services.[112]

The FCC fails to pass muster with appellate courts when advocates can demonstrate a lack of reasonableness, point to flaws in the Commission's rationale, or show how it failed to comply with its administrative rules. Until the FCC reclassified broadband Internet access as a telecommunications service, the FCC could not stretch the largely unregulated information service classification to impose common carrier, nondiscrimination and neutrality requirements.[113]

Earlier, the FCC failed to convince appellate courts that a revised, more extensive regulatory regime made sense even if doing so would have protected children from coarse and potentially harmful content. In *FCC v. Fox Television Stations, Inc.*,[114] the Supreme Court held that FCC violated broadcast networks' due process rights by failing to give them fair notice

---

184, Connect America Fund, WC Docket No. 10-90, Second Report and Order and Order on Reconsideration, 29 FCC Rcd 15538 (2014).

Recently the FCC proposed to revise its Lifeline universal service subsidy program to include access to wireless broadband services and handsets, for which the FCC has limited jurisdiction primarily focused on technical compatibility issues. *See* Lifeline and Link Up Reform and Modernization, Telecommunications Carriers Eligible for Universal Service Support, Connect America Fund, WC Docket Nos. 11-42, 09-197, 10-90, *Second Further Notice of Proposed Rulemaking, Order on Reconsideration, Second Report and Order, and Memorandum Opinion and Order*, FCC 15-71, WL 3884807 (rel. June 22, 2015).

112. "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.' In requiring broadband providers to serve all edge providers without 'unreasonable discrimination,' this rule by its very terms compels those providers to hold themselves out 'to serve the public indiscriminately.'" *Verizon v. FCC*, 740 F.3d at 655-56 (citations omitted); *see also FCC v. Midwest Video Corp.*, 440 U.S. 689, 99 S.Ct. 1435 (1979) (deeming as the functional equivalent of common carriage mandatory public access to cable television channels); *Nat'l Ass'n of Regulatory Util Comm'rs v. FCC*, 525 F.2d 630, 642 (D.C.Cir.1976) (identifying the basic characteristic that distinguishes common carriers from "private" carriers); *National Association of Regulatory Utility Commissioners v. FCC*, 533 F.2d 601, 608 (1976)(common carriers must have a quasi-public character arising out of the undertaking to carry for all people indifferently).

113. The FCC's ancillary jurisdiction of cable television operators does not extend to rules and regulations that impose the functional equivalent of common carriage. In FCC v. Midwest Video Corp., 440 U.S. 689 (1979), the Supreme Court determined that compulsory public access to cable television channel capacity constituted common carriage unlike the limited carriage rights available only to broadcasters.

114. *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307 (2012).

that, in contrast to prior policy, a fleeting expletive, or a brief shot of nudity, could be deemed indecent and trigger regulatory sanctions.

In *American Radio Relay League, Inc. v. FCC*,[115] the District of Columbia Circuit determined that even for complex technological issues regarding the potential for radio spectrum interference the FCC did not qualify for deference.[116] The court agreed with arguments that the FCC selectively chose empirical research data to support a specific technical standard, despite evidence supporting an alternative summarily rejected by the Commission.[117]

A series of cases addressing interconnection of carrier competitors offered insights on how courts may first defer to FCC expertise, but eventually sided with stakeholders frustrated by the length of time in implementation, complexity and lack of narrowing application as competitive conditions improved. When Congress enacted the Telecommunications Act of 1996,[118] it gave the FCC explicit statutory authority to require incumbent local exchange carriers to interconnect with market entrants.[119] However, the law lacked specificity on how the FCC should proceed to maximize the potential for competition without micromanaging carriers' operations and removing incentives for both types of carriers to invest in new infrastructure. Predictably, incumbent operators grew weary of having to cooperate with market entrants,[120] particularly after having made significant accommodations that the '96 Act required as preconditions before these carriers could enter new markets such as long distance telephone service.[121]

The FCC initially achieved success in its policies and strategies to promote local telephone service competition. The Supreme Court validated the FCC's overall policy agenda including the requirement that incumbents use a pricing methodology that made access to their networks extraordinarily cheap.[122] Eventually lower courts chided the FCC for the lack of follow through, particularly in light of the passage of time and the lack of a strategy for streamlining and reducing cooperation as competitive access alternatives became available, e.g., the ability to use cable television network facilities to

115. *American Radio Relay League, Inc. v. FCC*, 524 F.3d 227 (D.C. Cir. 2008),

116. *See id.*

117. *See id.*

118. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, *codified in scattered sections of* Title 47 of the United States Code.

119. *See* 47 U.S.C. §251, Interconnection.

120. *See e.g.,* 47 U.S.C. §251 (interconnection) 47 U.S.C. §252 (procedures for negotiation, arbitration, and approval of agreements); 47 U.S.C. § 253 (removal of barriers to entry).

121. *See* 47 U.S.C. §251(c) (additional obligations of incumbent local exchange carriers).

122. *See AT&T Corp. v. Iowa Utils. Bd*., 525 U.S. 366 (1999); *see also* Implementation of the Local Competition Provisions in the Telecommunications Act of 1996, *First Report and Order*, 11 FCC Rcd 15499 (1996).

reach end users.[123] These courts rejected the FCC's rules that mandated access to incumbent telephone company plants on financial terms well below wholesale and on an unbundled basis so that competitors could pick and use only those network elements they needed.[124] The courts criticized the FCC for failing to calibrate rules so that compulsory infrastructure access was limited only to localities still lacking competition and to network elements for which no alternative option was available.[125]

On balance, appellate courts appear willing to defer to agency expertise, particularly for quite complex technical and economic issues.[126] However the reluctance to second guess regulatory expertise wanes when stakeholders can assert, but not necessarily prove, that the agency's chosen course of action would create regulatory uncertainty, disincentives to additional investments, and other marketplace harms.[127] Eventually, courts held that the FCC lacked authority to require unbundled access to incumbent carrier facilities[128] and later the Commission abandoned any effort to

123. *See United States Telecom Ass'n v. FCC*, 290 F.3d 415 (D.C. Cir. 2002) (FCC failed to determine when competition would be impaired absent affirmative regulatory efforts); *see also* Implementation of the Local Competition Provisions of the Telecommunications Act of 1996, *Third Report and Order and Fourth Further Notice of Proposed Rulemaking*, 15 FCC Rcd 3696 (1999).

124. *See U.S. Telecomm. Ass'n v. FCC*, 359 F.3d 554 (D.C. Cir. 2004); *see also* Review of the Section 251 Unbundling Obligations of Incumbent Local Exchange Carriers, 18 FCC Rcd 16978, 16983 (2003); Unbundled Access to Network Elements, 20 FCC Rcd 2533, 2534 (2005) (order on remand).

125. "[A] rule is irrational in this context if a party has presented to the agency a narrower alternative that has all the same advantages and fewer disadvantages, and the agency has not articulated any reasonable explanation for rejecting the proposed alternative.

We therefore vacate the FCC's determination that ILECs must make mass market switches available to CLECs as UNEs, subject to the stay discussed in Part VI below, and remand to the Commission for a re-examination of the issue." *U.S. Telecomm. Ass'n v. FCC*, 359 F.3d at 571.

126. *See City of Arlington v. FCC*, 133 S. Ct. 1863 (2013) (upholding Chevron deference to FCC decisions that identify the boundaries of its jurisdiction over wireless tower site authorization vis a vis state and local authorities);

"Agencies, as specialists in particular fields, possess superior expertise as compared to generalist courts." Claire R. Kelly, *The Brand X Liberation: Doing Away with Chevron's Second Step as Well as Other Doctrines of Deference*, 44 U.C. DAVIS L. REV. 151, 164 (Nov. 2010); *see also* J. Brad Bernthal, *Procedural Architecture Matters: Innovation Policy at the Federal Communications Commission*, 1 TEX. A&M L. REV. 615 (Spring, 2014).

127. "Chevron is so indeterminate that lower courts have plenty of room to tailor their interpretive approach to varied facts, using contractual interpretation as a familiar guidepost. This approach could make a real difference for agencies and interested parties. They might find Chevron more predictable at the court of appeals level where most cases end. It is even possible the Supreme Court will incorporate Chevron developments from lower courts." Christine Kexel Chabota, *Selling Chevron*, 67 ADMIN. L. REV. 481, 549 (Summer, 2015).

128. *Covad Communications Co. v FCC*, 450 F.3d 528, 548 (D.C. Cir. 2006) ("The plain text of § 251(d)(2) permits unbundling *only* where the Commission receives evidence that UNEs are 'necessary' to prevent 'impair[ment]' of the CLECs' competitive aspirations. Thus, the 1996 Act does not obligate the ILECs to prove non-impairment—it forces the CLECs to prove impairment.").

stimulate local telephone service competition despite its statutory mandate to do so.[129]

C. Re-Regulation

The FCC reclassification of broadband Internet access from a largely unregulated information service to a significantly regulated telecommunications service has the effect of reversing the Commission's prior decision not to regulate Internet access. The Commission will bear an extraordinarily high burden to prove the lawfulness of its decision, because re-regulation runs counter to prevailing economic and political doctrine supporting less government intervention, particularly in the telecommunications marketplace where technological innovations have the potential to support more competition in some segments even as it can favor market concentration in others.[130] Opponents of network neutrality and other types of muscular FCC regulatory oversight claim that such intervention harms the national interest, generates regulatory uncertainty, reduces

129. *See* Petition of AT&T Inc. for Forbearance Under 47 U.S.C. § 160(c) from Title II and Computer Inquiry Rules with Respectto Its Broadband Services, WC Docket No. 06-125, Memorandum Opinion and Order, 22 FCC Rcd 18705 (2007), *aff'd sub nom. Ad Hoc Telecom. Users Comm. v. FCC*, 572 F.3d 903 (D.C. Cir. 2009) (granting AT&T forbearance from rules applicable to enterprise broadband services); Unbundled Access to Network Elements, Review of the Section 251 Unbundling Obligations of Incumbent Local Exchange Carriers, WC Docket No. 04-13, CC Docket No. 01-338, Order on Remand, 20 FCC Rcd 2533 (2005) (eliminating unbundled switching and significantly scaling back unbundling of other network elements); Review of the Section 251 Unbundling Obligations of Incumbent Local Exchange Carriers. Implementation of the Local Competition Provisions of the Telecommunications Act of 1996, Deployment of Wireline Services Offering Advanced Telecommunications Capability, CC Docket Nos. 01-338, 96-98, and 98-147, Report and Order and Notice of Proposed Rulemaking, 18 FCC Rcd 16978 (2003) (eliminating line-sharing).

130. "Faced with the advent of new technologies, cheaper equipment and distribution methods, and an increasingly dynamic marketplace, federal policymakers responded at first by relaxing the rules that had long insulated the telephone monopoly. In addition, influential FCC proceedings like the Computer Inquiries would set a deregulatory precedent for "enhanced" services (i.e., communications services that were more advanced and interactive in nature than traditional telephony) by freeing them from common-carrier regulation in an effort to support continued experimentation in their development." Charles M. Davidson & Michael J. Santorelli, *Federalism in Transition: Recalibrating the Federal-State Regulatory Balance for the All-IP Era*, 29 BERKELEY TECH. L.J. 1131, 1149-50 (Fall. 2014); "The reconstitution of integrated local and long distance companies through mergers by firms that also dominate wireless and have joint-ventures with their closest cable rivals bears no resemblance to the 'sweet spot' that the pre-divestiture theory identified as the place where quasi-competition might produce 'voluntary' integration between independent networks. Special access services, which allow competitors to interconnect with the wireline telecommunications network, have been a source of constant complaint about abuse since the industry was deregulated." Mark Cooper, *The Long History and Increasing Importance of Public-Service Principles for 21st Century Public Digital Communications Networks*, J. on Telecomm. & High Tech. L. 1, 31 (2014).

incentives for investment, stifles innovation and offers a remedy where no problem exists.[131]

While Congress forces the FCC to interpret and apply statutory definitions, such as telecommunications and information service, the Commission unilaterally decided that these classifications are mutually exclusive.[132] Nothing in the Telecommunications Act, or case precedent requires the FCC to establish an absolute dichotomy and shoe horn any existing or new Internet service into one category or the other.[133] In the

131. See, e.g., Babette E.L. Boliek, *FCC Regulation versus Antitrust: How Net Neutrality is Defining the Boundaries*, 52 B.C. L. REV. 1627 (2011); Shanika Chapman, *Hands Off My Internet! Why the FCC Should Refrain from Regulating the Internet*, 67 CONSUMER FIN. L. Q. REP. 375 (2013); Thomas W. Hazlett & Joshua D. Wright, *The Law and Economics of Network Neutrality*, 45 IND. L. REV. 767, 798 (2012); Hon. Maureen K. Ohlhausen, *Net Neutrality vs. Net Reality: Why an Evidence-Based Approach to Enforcement, and Not More Regulation, Could Protect Innovation on the Web*, 14 ENGAGE: J. FEDERALIST SOC'Y PRAC. GROUPS 81 (2013); J. Gregory Sidak & David J. Teece, *Innovation Spillovers and the "Dirt Road" Fallacy: The Intellectual Bankruptcy of Banning Optional Transactions for Enhanced Delivery Over the Internet*, 6 J. COMP. L. & ECON. 521 (2010); Dennis L. Weisman & Robert B. Kulick, Price Discrimination, Two-Sided Markets, and Net Neutrality Regulation, 13 TUL. J. TECH. & INTELL. PROP. 81 (2010); Christopher S. Yoo, *Network Neutrality and the Economics of Congestion*, 94 GEO L. J. 1847, 1901 (2006); Christopher S. Yoo, *Beyond Network Neutrality*, 19 HARV. J.L. & TECH. 1 (2005).

132. Federal-State Joint Board on Universal Service, Report to Congress, 13 FCC Rcd 11501, 11522 (1998) ("[T]he language and legislative history of [the Communications Act of 1996] indicate that the drafters . . . regarded telecommunications services and information services as mutually exclusive categories."). *See also Vonage Holdings Corp. v. Minnesota Pub. Utils. Comm'n* , 290 F. Supp. 2d 993, 994, 1000 (D. Minn. 2003) (applying the FCC's dichotomy).

The telecommunications service/information service classifications "are best construed as mutually exclusive categories, and our classification ruling appropriately keeps them distinct. In classifying broadband Internet access service as a telecommunications service, we conclude that this service is not a functionally integrated information service consisting of a telecommunications component 'inextricably intertwined' with information service components. Rather, we conclude, for the reasons explained above, that broadband Internet access service as it is offered and provided today is a distinct offering of telecommunications and that it is not an information service." *2015 Open Internet Order*, para. 385. ""To the extent that broadband Internet access service is offered along with some capabilities that would otherwise fall within the information service definition, they do not turn broadband Internet access service into a functionally integrated information service. To the contrary, we find these capabilities either fall within the telecommunications systems management exception or are separate offerings that are not inextricably integrated with broadband Internet access service, or both." *Id.* para. 365.

133. Both the Telecommunications Act of 1996 and the Communications Act of 1934 provide service definitions that are not identified as mutually exclusive, nor do these laws prohibit a single operator from provider more than one service. The D.C. Circuit Court of Appeals underscored the lack of mutually exclusivity between the classification of services provided by the various ventures that cooperate in the creation, distribution and delivery of Internet-mediated content that ultimately reaches end users:

To pull the whole picture together with a slightly oversimplified example: when an edge provider such as YouTube transmits some sort of content—say, a video of a cat—to an end user, that content is broken down into packets of information, which are carried by the edge provider's local access provider to the backbone network, which transmits these packets to the

telecommunications marketplace, ventures embrace converging technologies and markets and offer consumers an inventory of services that fall within the telecommunications service and information service classifications while others combine the two.[134]

Even the District of Columbia Circuit, which handled both prior appeals of FCC network neutrality orders, accepts the reality that convergence forecloses a bright line distinction between what the FCC can lawfully regulate and what it cannot:

> [E]ven if a regulatory regime is not so distinct from common carriage as to render it inconsistent with common carrier status, that hardly means it is so fundamentally common carriage as to render it inconsistent with private carrier status. In other words, common carriage is not all or nothing—there is a gray area in which although a given regulation might be applied to common carriers, the obligations imposed are not common carriage per se."[135]

By assuming the obligation to make an either/or determination of regulatory status, the FCC limited itself to binary decision-making when it could no longer avoid having to make the call.[136] It could declare Internet access an information service and abandon statutory authority to regulate, regardless of changed circumstances. Alternatively it could declare Internet access a telecommunications service as it did when initially assigning Digital Subscriber Line access to the telecommunications service category.[137] On grounds that it should avoid creating regulatory asymmetry, the FCC opted

---

end user's local access provider, which, in turn, transmits the information to the end user, who then views and hopefully enjoys the cat.

These categories of entities are not necessarily mutually exclusive." Verizon v. FCC, 740 F.3d at 629.

134. For example, Voice over the Internet Protocol ("VoIP") services combine software and broadband Internet access to offer functional equivalents of and competitive alternatives to conventional, common carrier regulated voice telephone service. Internet Protocol Television uses a similar combination to provide an increasingly viable alternative to broadcast, cable and satellite television.

135. *Cellco P'ship v. FCC*, 700 F.3d 534, 547 (D.C. Cir. 2012).

136. The FCC avoided having to make a definite regulatory classification of where broadband Internet fits until 2002. "To date, however, the Commission has declined to determine a regulatory classification for, or to regulate, cable modem service on an industry-wide basis." Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, Internet Over Cable Declaratory Ruling, GN Docket No. 00-185, Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities, 17 FCC Rcd 4798, 4800-01 (2002), *vacated in part, National Cable & Telecommunications Ass'n v. Brand X Internet Servs.*, 545 U.S. 967 (2005). Subsequently, the FCC established binding rules treating cable modem service as an information service. Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, 20 FCC Rcd 14853 (2005), *petition for rev. den.*, Time Warner Telecom, Inc. v. F.C.C., 507 F.3d 205 (3rd Cir. 2007).

137. *2015 Open Internet Order*, para. 39 ("[W]ireline DSL was regulated as a common-carrier service until 2005.").

to treat all forms of broadband Internet access as information services, including DSL, which it reclassified.[138]

Having classified all forms of broadband Internet access as information services, the FCC voluntarily relinquished the option of applying just about all regulatory safeguards, even if it came to realize that self-regulation would not suffice. The FCC received complaints detailing instances where unregulated ISPs appeared to operate in ways that harmed both competitors and consumers. Rather than acknowledge its mistake in eliminating the option of applying any common carrier nondiscrimination requirement, the Commission embarked on a twice-failed strategy of devising regulatory safeguards designed to achieve the same outcomes as common carrier oversight without reclassifying them and expressly regulating under Title II regulations.

In *Comcast v. FCC*, the District of Columbia Circuit rejected the FCC's attempts as unlawful.[139] The court first held that the FCC could not sanction Comcast for using software to disable peer-to-peer file sharing by subscribers, even though the company did not need to remedy congestion and had financial incentives to prevent subscribers from sharing movies it might otherwise lease on a pay per view basis.[140] The court then held that the FCC had no express statutory authority to impose network neutrality obligations on information service providers, nor could the Commission assert ancillary jurisdiction based on its duty to ensure that new technologies do not adversely impact regulated services.[141]

When reviewing the FCC's second attempt to establish jurisdiction over ISPs, the District of Columbia Circuit again rejected common-carrier style rules, mandating nondiscrimination and prohibiting traffic blocking.142 However, the court agreed with the FCC that it could impose non-common

---

138. *Id.*, para. 323 ("Following *Brand X*, the Commission issued the *Wireline Broadband Classification Order* [20 FCC Rcd 14853 (2005)], which applied the 'information services' classification at issue in the *Cable Modem Declaratory Ruling* [17 FCC Rcd 4798 2005)] to facilities-based wireline broadband Internet access services as well and eliminated the resulting regulatory asymmetry between cable companies and telephone companies offering wired Internet access service via DSL and other facilities.").

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

140. *See id.*

141. *See id.* at 644 ("The Commission may exercise this 'ancillary' authority only if it demonstrates that its action—here barring Comcast from interfering with its customers' use of peer-to-peer networking applications—is 'reasonably ancillary to the ... effective performance of its statutorily mandated responsibilities.") (citing *Am. Library Ass'n v. FCC*, 406 F.3d 689, 692 (D.C. Cir. 2005).

142. *Verizon v. FCC*, 740 F.3d at 628 **(**"[E]ven though the Commission has general authority to regulate in this arena, 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. Because the Commission has failed to establish that the anti-discrimination and anti-blocking rules do not impose *per se* common carrier obligations, we vacate those portions of the *Open Internet Order*.").

carrier rules based on the FCC's reading of Section 706 of the Communications Act,143 which authorizes the Commission to promote nationwide access to advanced telecommunications services such as the Internet.[144]

Now, rather than find a way to achieve non-common carrier regulatory safeguards, the FCC has opted to reclassify broadband Internet access as common carriage.[145] The Commission could have bolstered its defense on appeal had it acknowledged its two prior classification mistakes: (1) its belief that anything Internet-related must be treated as either an information service or a telecommunications service and (2) its determination that all Internet broadband access fits squarely within the information service category.

Instead, the FCC offers multiple and conflicting justifications. At various points within the *2015 Open Internet Order*, the Commission appears to use the ancillary jurisdiction rationale, as least insofar as considering its statutory instructions to be ambiguous and therefore open to its expert interpretation.[146] In other places, the FCC has no problem using the statutory classifications to categorize broadband Internet access solely as common carriage.[147] By doing so, rather than bolstering the weight and rationale of its argument, the FCC offers conflicting, inconsistent, and not complementary justifications.

---

143. "As we explain in this opinion, the Commission has established that section 706 of the Telecommunications Act of 1996 vests it with affirmative authority to enact measures encouraging the deployment of broadband infrastructure. The Commission, we further hold, has reasonably interpreted section 706 to empower it to promulgate rules governing broadband providers' treatment of Internet traffic, and its justification for the specific rules at issue here—that they will preserve and facilitate the "virtuous circle" of innovation that has driven the explosive growth of the Internet—is reasonable and supported by substantial evidence." *Id.* at 628.

144. 47 U.S.C. § 1302 (2014).

145. 2015 Open Internet Order at ¶29.

146. "To be sure, with the Commission's exercise of both section 706 and ancillary authority, regulations must be within the Commission's subject matter jurisdiction. Indeed, this is the first prong of the test for ancillary jurisdiction. American Library Ass'n v. FCC, 406 F.3d 689, 703–04 (D.C. Cir. 2005). But we do not read the Verizon decision as applying the second prong—which requires that the regulation be sufficiently linked to another provision of the Act—to our exercise of section 706 authority. Section 706 "does not limit the Commission to using other regulatory authority already at its disposal, but instead grants it the power necessary to fulfill the statute's mandate." See Verizon, 740 F.3d at 641 (citing 2010 Open Internet Order, 25 FCC Rcd at 17972, para. 123)." 2015 Open Internet Order at n. 721.

147. "Based on this updated record, this Order concludes that the retail broadband Internet access service available today is best viewed as separately identifiable offers of (1) a broadband Internet access service that is a telecommunications service (including assorted functions and capabilities used for the management and control of that telecommunication service) and (2) various "add-on" applications, content, and services that generally are information services." 2015 *Open Internet Order* at ¶47.

IV. WHETHER AND HOW THE FCC CAN DEFEND THE 2015 OPEN INTERNET ORDER

By opting to reclassify broadband Internet access as common carriage, the FCC has imposed upon itself a challenging burden in securing judicial affirmance. Had the Commission opted solely to impose non-common carrier regulations, it would have enhanced the odds of affirmance by using less muscular regulation that did not necessitate reclassifying broadband Internet access as a telecommunications service. Arguably the FCC could have achieved its public policy goals by combining enhanced transparency requirements on ISPs with a complaint-resolution process for addressing problems as they arise. Additionally, the Commission could have bolstered its link to statutory authority by emphasizing its jurisdiction based on Section 706, Title III for wireless broadband, and the incremental extension of private carrier oversight, as recommended by the District of Columbia Circuit.[148] By seeking to maintain a bright line distinction between telecommunications services and information services, with ISPs reassigned to the former category, the FCC substantially added to its appellate woes. Ostensibly to remove uncertainty, the Commission opted to convert any and all types of broadband Internet access as telecommunications services, a category that links a new generation of technology and service with legacy technologies and services much more akin to public utility, monopoly service such as voice telephony. Additionally, the Commission muddied the logic and consistency of its legal rationale by offering multiple and contradicting tracks of case precedent.[149]

A. Extensive Reliance on Chevron Deference to Interpret Statutory Ambiguity

The *2015 Open Internet Order* heavily relies on case law endorsing flexibility in regulatory agencies' interpretations and subsequent

148. "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." Christopher S Yoo, *Wickard for the Internet? Network Neutrality After Verizon v. FCC*, 66 Fed. Comm. L.J. 415, 417 (June, 2014). The court appeared to suggest some requirements on ISPs are lawful provided they do not constitute common carriage, as was the case when the FCC ordered wireless carriers to negotiate data roaming on commercially based terms and conditions specific to each type of individual interconnection arrangement. The court also emphasized that absolute mutual exclusivity between the offering of telecommunications services and information services is not statutorily mandated: "Since it is clearly possible for a given entity to carry on many types of activities, it is at least logical to conclude that one may be a common carrier with regard to some activities but not others." *Verizon v. FCC*, 740 F.3d at 653 (quoting *Nat'l Ass'n. Regl. Util. Comm'nrs v. FCC*, 533 F.2d 601, 608 (D.C. Cir. 1976)).

reinterpretations of their statutory authority.150 Because it previously was unsuccessful in asserting ancillary jurisdiction over information services,[151] the FCC instead opted to rely on repeated assertions of statutory ambiguity to achieve its new goal of justifying the reclassification of broadband Internet access as a telecommunications service.[152] The FCC emphasizes how ambiguous statutory definitions in the Communications Act,[153] and even in the meaning of common words like "offer,"[154] "just," "unjust," "reasonable," "unreasonable,"[155] "necessary,"156 and "points specified by the user,"[157] justify its reclassification of broadband Internet access.

The FCC heavily relies on the *Chevron* deference to support its reclassification of broadband Internet access from an information service to a telecommunications service.[158] While agency expertise is owed no deference "if the intent of Congress is clear,"[159] courts should defer to reasonable exercises of regulatory agency expertise "if the statute is silent or

---

150. *2015 Open Internet Order*, para. 331 ("We both revise our prior classifications of wired broadband Internet access service and wireless broadband Internet access service, and classify broadband Internet access service provided over other technology platforms. In doing so, we exercise the well-established power of federal agencies to interpret ambiguous provisions in the statutes they administer.").

151. *Comcast v. FCC*, 600 F.3d 642, 643 (D.C. Cir. 2010) ("The Commission may exercise this 'ancillary' authority only if it demonstrates that its action—here barring Comcast from interfering with its customers' use of peer-to-peer networking applications—is 'reasonably ancillary to the ... effective performance of its statutorily mandated responsibilities.' The Commission has failed to make that showing.") (quoting *Am. Library Ass'n v. FCC*, 406 F.3d 689, 692 (D.C. Cir. 2005)).

152. We "conclude that the application of sections 201 and 202 is appropriate to remove any ambiguity regarding our authority to enforce strong, clear open Internet rules." *2015 Open Internet Order*, para. 448.

153. *2015 Open Internet Order*, para. 334 & n.868 (citing *Virgin Islands Tel. Comp. v. FCC*, 198 F.3d 921, 925-26 (D.C. Cir. 1999) (holding that "telecommunications service" is an ambiguous term)).

The FCC provides case law supporting its determination that telecommunications service and information service are ambiguous terms: "It is also well settled that we may reconsider, on reasonable grounds, the Commission's earlier application of the ambiguous statutory definitions of 'telecommunications service' and 'information service.'" *Id.* The Commission also provides case precedent supporting its determination that Sec. 706 is ambiguous: "Finding that provision ambiguous, the court [in *Verizon v. FCC*,] upheld the Commission's interpretation as consistent with the statutory text, legislative history, and the Commission's lengthy history of regulating Internet access." *Id*., para. 276 (citation omitted).

154. *2015 Open Internet Order*, n. 868. *See also id*., para. 322 & n.983 (discussing ambiguity in "offering").

155. *Id*., n.1493 (citing *Capital Network Sys., Inc., v. FCC*, 28 F.3d 201, 204 (D.C. Cir. 1994)).

156. *Id*., n.1493 (citing *Cellco P'ship v. FCC*, 357 F.3d 88 (D.C. Cir. 2004)).

157. *Id*., para. 361.

158. "[W]e exercise the well-established power of federal agencies to interpret ambiguous provisions in the statutes they administer." *Id*., para. 331. "The [Supreme] Court's application of this *Chevron* test in *Brand X* makes clear our delegated authority to revisit our prior interpretation of ambiguous statutory terms and reclassify broadband Internet access service as a telecommunications service." *Id*., para. 332.

159. *Id.* 467 U.S. at 842.

ambiguous with respect to the specific issue, [. . .] [provided] the agency's answer is based on a permissible construction of the statute."[160]

The *2015 Open Internet Order* also heavily relies on the Supreme Court's application of *Chevron* Doctrine in *Brand X*,[161] where the Court affirmed the Commission's decision to classify cable modem Internet access as an information service:

> In *Chevron*, this Court held that ambiguities in statutes within an agency's jurisdiction to administer are delegations of authority to the agency to fill the statutory gap in reasonable fashion. Filling these gaps, the Court explained, involves difficult policy choices that agencies are better equipped to make than courts. If a statute is ambiguous, and the implementing agency's construction is reasonable, *Chevron* requires a federal court to accept the agency's construction of the statute, even if the agency's reading differs from what the court believes is the best statutory interpretation.[162]

The FCC links its invocation of statutory ambiguity with changed circumstances in the Internet ecosystem to justify its reclassification of broadband Internet access.[163] The Commission appears to assume that, having properly identified statutory ambiguity as the basis for taking on the task of statutory interpretation, it also can consider whether changed circumstances warrant reclassification of broadband Internet access.[164] In the absence of congressional action to clarify and remove statutory ambiguity,

---

160. *Id*. at 843. *See also United States v. Mead Corp.*, 533 U.S. 218, 226–27 (2001); John Blevins, *Jurisdiction as Competition Promotion: A Unified Theory of the FCC's Ancillary Jurisdiction*, 36 FLA. ST. U. L. REV. 585 (2009); Andrew Gioia, Note, *FCC Jurisdiction Over ISPs in Protocol-Specific Bandwidth Throttling*, 15 MICH. TELECOMM. & TECH. L. REV. 517 (2009); James B. Speta, *The Shaky Foundations of the Regulated Internet*, 8 J. ON TELECOMM. & HIGH TECH. L. 101 (2010).

161. "The Court's application of this *Chevron* test in *Brand X* makes clear our delegated authority to revisit our prior interpretation of ambiguous statutory terms and reclassify broadband Internet access service as a telecommunications service." 2015 Open Internet Order at para. 332.

162. *Id*., para. 331 (quoting *Brand X*, 545 U.S. at 980) (citations omitted).

163. "As the record reflects, times and usage patterns have changed and it is clear that broadband providers are offering both consumers and edge providers straightforward transmission capabilities that the Communications Act defines as a 'telecommunications service.'" *Id*., para. 43.

164. *Id*., para. 47 ("Based on this updated record, this Order concludes that the retail broadband Internet access service available today is best viewed as separately identifiable offers of (1) a broadband Internet access service that is a telecommunications service (including assorted functions and capabilities used for the management and control of that telecommunication service) and (2) various "add-on" applications, content, and services that generally are information services. This finding more than reasonably interprets the ambiguous terms in the Communications Act, best reflects the factual record in this proceeding, and will most effectively permit the implementation of sound policy consistent with statutory objectives, including the adoption of effective open Internet protections.").

nothing has changed in terms of the nature, type and existence of the ambiguities in the Communications Act. What has changed is the nature, scope and reach of regulatory authority based on the persistence of statutory ambiguity.

To achieve its desired reclassification of broadband Internet access, the FCC undertakes a broad-ranging reassessment of the need for regulatory safeguards due to changes in the marketplace.[165] The Commission acknowledges this game plan:

> Exercising our delegated authority to interpret ambiguous terms in the Communications Act, as confirmed by the Supreme Court in *Brand X*, today's Order concludes that the facts in the market today are very different from the facts that supported the Commission's 2002 decision to treat cable broadband as an information service and its subsequent application to fixed and mobile broadband services.[166]

B. The FCC Applies the Statutory Classifications Without Modification

The *2015 Open Internet Order* explicitly identifies what types of broadband transmitting, switching, routing, caching and addressing functions fit solely within the telecommunications service and information service dichotomy. The Commission applies the existing statutory language contained in the service classifications and identifies no flaws that it believes Congress should remedy by amending the Communications Act. On the contrary, the FCC painstakingly explains why changed circumstances warrant its reclassification, not that these changes make it more difficult or impossible to interpret and apply the existing classifications.[167] The FCC explicitly reclassifies broadband Internet access:

> Having determined that Congress gave the Commission authority to determine the appropriate classification of broadband Internet access service—and having provided sufficient justification of changed factual circumstances to warrant a reexamination of the Commission's prior classification—we find, upon interpreting the relevant statutory terms, that broadband Internet access service, as offered today,

165. *Id*., para. 43.

166. *Id*.,para. 43.

167. "Changed factual circumstances cause us to revise our earlier classification of broadband Internet access service based on the voluminous record developed in response to the *2014 Open Internet NPRM*." *Id*. at para. 330.

> includes "telecommunications," and falls within the definition of a "telecommunications service."[168]

To justify its reclassification, the FCC reexamined the nature of what a retail ISP does and how it uses techniques it previously used to support the information service classification, but now support the provisioning of telecommunications services. The FCC simplifies its conceptualization of the work performed. Instead of providing complex and multifaceted information services, "broadband providers are offering both consumers and edge providers [which offer content, software and applications] straightforward transmission capabilities that the Communications Act defines as a 'telecommunications service.'"[169] The Commission reverses its previous determination that ISP transmission capabilities are "inextricably intertwined" with various proprietary applications and services and now concludes that "it is more reasonable to assert that the 'indispensable function' of broadband Internet access service is 'the connection link that in turn enables access to the essentially unlimited range of Internet-based services.'"[170]

The FCC simplifies the role of retail ISPs to primarily acting as a conduit for access to and from the Internet,[171] even though the technologies used rely on sophisticated data processing, temporary storage (caching)[172] and address creation, lookup and resolution using the Domain Numbering System ("DNS"),[173] a mechanism far more complicated than processing telephone numbers. The Commission justifies this simplification based on:

---

168. *Id*. at para. 335. The FCC also provided a new definition for broadband Internet access, "[T]oday's Order applies its rules to the consumer-facing service that broadband networks provide, which is known as 'broadband Internet access service' (BIAS) and is defined to be: A mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this Part." *Id*., para. 25.

169. *Id*., para. 43.

170. *Id.*, para. 330 (citations omitted).

171. *See* William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under The Stored Communications Act*, 98 GEO L.J. 1195, 1199 (2010) ("The increasing functionality of the Internet is decreasing the role of the personal computer. This shift is being led by the growth of 'cloud computing'--the ability to run applications and store data on a service provider's computers over the Internet, rather than on a person's desktop computer."); *see also* Jake Vandelist, *Status Update: Adapting the Stored Communications Act to a Modern World*, 98 MINN. L. REV. 1536 (2014).

172. *2015 Open Internet Order*, n. 973 ("Caching is the storing of copies of content at locations in a network closer to subscribers than the original source of the content. This enables more rapid retrieval of information from websites that subscribers wish to see most often.") (citing Cable Modem Declaratory Ruling, 17 FCC Rcd at 4810, n.76).

173. "DNS is most commonly used to translate domain names, such as 'nytimes.com,' into numerical IP addresses that are used by network equipment to locate the desired content.

> (1) consumer conduct, which shows that subscribers today rely heavily on third-party services, such as email and social networking sites, even when such services are included as add-ons in the broadband Internet access provider's service; (2) broadband providers' marketing and pricing strategies, which emphasize speed and reliability of transmission separately from and over the extra features of the service packages they offer; and (3) the technical characteristics of broadband Internet access service.[174]

Here, the FCC appears to understand the need to explain why certain technical functions performed by ISPs now support the telecommunications service classification having previously been considered by the Commission as integral to, and inseparable from the information service these technologies supported. It emphasizes that caching and DNS management now fit within the telecommunications systems management exception to the definition of information service,[175] because these are now considered separate,[176] standalone functions, or at least not "inextricably integrated with broadband Internet access service."[177]

The FCC appears to state that caching and DNS management are supportive technologies that might be used by ISPs to provide access to a wide variety of services, but for regulatory purposes snugly fit within the telecommunications systems management exception to the information service definition. To achieve this new assignment, the FCC has to place far greater emphasis on a clause contained in the information service definition that the Commission hardly noticed before. Additionally, it has to give far greater credence to Justice Scalia's dissent in *Brand X*.

Bear in mind, when the FCC bore the incentive to justify its information service classification before appellate courts and to secure necessary judicial deference in light of statutory ambiguity, the Commission had every reason to ignore the telecommunications systems management

---

Id., n. 972 (citing Cable Modem Declaratory Ruling at 4810, n.74; *Brand X*, 545 U.S. at 987, 999).

174. *2015 Open Internet Order*, para. 330.

175. *Id.*, para. 356 ("We also find that domain name service (DNS) and caching, when provided with broadband Internet access services, fit squarely within the telecommunications systems management exception to the definition of 'information service.' Thus, when provided with broadband Internet access services, these integrated services do not convert broadband Internet access service into an information service."). The statutory definition of information service, 47 U.S.C. § 153(24), states that this category "does not include any use of any such capability for the management, control, or operation of a telecommunications system of the management of a telecommunications service." The FCC refers to this exclusion as the "telecommunications systems management" exception.

176. *Id.*, para. 370 ("Although we find that DNS falls within the telecommunications systems management exception, even if did not, DNS functionality is not so inextricably intertwined with broadband Internet access service so as to convert the entire service offering into an information service.").

177. *Id.*, para. 365.

exception[178] and to emphasize the tight integration of caching and DNS management with the provisioning of an information service. Suddenly the FCC can view caching and DNS management functions as standalone functions, even though the definitions of telecommunications service and information service have not changed.

In the *2015 Open Internet Order*, the FCC embraces Justice Scalia's view that a telecommunications function can be decoupled from other functions. However, Justice Scalia referred to the FCC's refusal to identify and decouple a telecommunications service as evidence that regulatory agencies can and will seek unconditional judicial deference to create new regulatory, deregulatory or re-regulatory schemes at the agency's discretion:

> In other words, what the Commission hath given, the Commission may well take away—unless it doesn't. This is a wonderful illustration of how an experienced agency can (with some assistance from credulous courts) turn statutory constraints into bureaucratic discretions. The main source of the Commission's regulatory authority over common carriers is Title II, but the Commission has rendered that inapplicable in this instance by concluding that the definition of "telecommunications service" is ambiguous and does not (in its current view) apply to cable-modem service. It contemplates, however, altering that (unnecessary) outcome, not by changing the law (*i.e.*, its construction of the Title II definitions), but by reserving the right to change the facts. . . . Such Möbius–strip reasoning mocks the principle that the statute constrains the agency in any meaningful way.[179]

In a nutshell, Justice Scalia has predicted what the FCC now seeks from appellate courts: maximum flexibility to regulate, deregulate, or re-regulate largely free of having to convince a skeptical judiciary that statutory authority exists, or ambiguity warrants such deference. A clever regulatory agency could exploit such flexibility to achieve welcomed deregulation, but it could just as easily seek to expand its regulatory "wingspan."

C. The FCC Can Generate a Persuasive Empirical Record of New Facts and Changed Circumstances

The FCC did not need to reclassify broadband Internet access to secure lawful authority to remedy existing and future problems that harm broadband consumers and competitors. The Commission could have

178. The FCC acknowledges that when it made its information services classification, it undertook no analysis on whether and how the telecommunications systems management exception applied. *See Id*. at 166 n. 1028.

179. *Brand X*, 545 U.S. at 1013-14; *see also* Rob Frieden, *What Do Pizza Delivery and Information Services Have in Common? Lessons From Recent Judicial and Regulatory Struggles with Convergence* 32 RUTGERS COMPUTER & TECH. L. J. 247 (2006).

followed the roadmap created by the D.C. Circuit Court of Appeals in *Verizon* case that supports limited private carrier oversight based primarily on direct statutory authority. Rather than to resurrect a "top-down" Title II regulatory regime, only to remove substantial portions as unnecessary and politically unpalatable, the Commission could have used a less aggressive "bottom up" strategy. The FCC could have combined already approved transparency requirements and Title III regulation of spectrum use with the direct statutory authority available from Section 706 of the Communications Act that authorizes the Commission to assess whether Americans have access to affordable and widespread broadband service and to impose safeguards designed to achieve these legislatively identified goals.

1. Curious Reluctance to Emphasize Direct Statutory Authority Conferred by Section 706

Section 706(a) of the Communications Act requires the FCC and state PUCs to "encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans . . .."[180] Section 706(b) of the Communications Act requires the Commission to conduct an annual inquiry "concerning the availability of advanced telecommunications capability" and if it determines that access is not available on "a reasonable and timely fashion" "to take immediate action to accelerate deployment of such capability by removing barriers to infrastructure investment and by promoting competition in the telecommunications market."[181]

The FCC initially stated that Section 706 did not confer a direct statutory conferral of statutory authority to enact measures encouraging the deployment of broadband infrastructure.[182] It subsequently reversed itself [183] and the *Verizon* court accepted the Commission's new rationale:

180. 47 U.S.C. § 1302(a) (2012).

181. 47 U.S.C. § 1302(b) (2012).

182. Deployment of Wireline Services Offering Advanced Telecommunications Capability, *Memorandum Opinion and Order and Notice of Proposed Rulemaking*, 13 FCC Rcd 24012, 24044, ¶69 (1999) ("After reviewing the language of section 706(a), its legislative history, the broader statutory scheme, and Congress' policy objectives, we agree with numerous commenters that section 706(a) does not constitute an independent grant of forbearance authority or of authority to employ other regulating methods."). ** quote is at 24044

183. "Section 706(a) accordingly provides the Commission a specific delegation of legislative authority to promote the deployment of advanced services, including by means of the open Internet rules adopted today. Our understanding of Section 706(a) is, moreover, harmonious with other statutory provisions that confer a broad mandate on the Commission." 2010 Open Internet Order, 25 FCC Rcd at 17971, *vacated on other grounds sub nom*., Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014). "To the extent that the Advanced Services Order can be construed as having read Section 706(a) differently, we reject that reading of the statute for the reasons discussed in the text." *2010 Open Internet Order*, 25 FCC Rcd at 17969, n.370.

> As we explain in this opinion, the Commission has established that section 706 of the Telecommunications Act of 1996 vests it with affirmative authority to enact measures encouraging the deployment of broadband infrastructure. The Commission, we further hold, has reasonably interpreted section 706 to empower it to promulgate rules governing broadband providers' treatment of Internet traffic, and its justification for the specific rules at issue here—that they will preserve and facilitate the "virtuous circle" of innovation that has driven the explosive growth of the Internet—is reasonable and supported by substantial evidence.[184]

The FCC can lawfully interpret Section 706 as requiring an ongoing assessment of the broadband ecosystem and action to remedy market failure that has resulted in insufficient competition and infrastructure investment. With judicial approval, the Commission has invoked Section 706 as the statutory basis for requiring ISPs to operate with transparency and disclosure of specialized service arrangements. The Commission overstepped the bounds of its Section 706 authority only when it sought to create and enforce common carrier rules prohibiting unreasonable discrimination and blocking lawful content.

The District of Columbia Circuit has affirmed the FCC's lawful authority under Section 706 to take affirmative steps, short of imposing common carrier regulations, to remedy broadband market failure.[185] The options available to the Commission appear widespread as evidenced by its decision to increase what constitutes broadband transmission speeds that satisfy the legislative goal of widespread access to advanced services[186] and

184. *Verizon*, 740 F.3d at 628.

185. Equally important, the Commission has adequately supported and explained its conclusion that, absent rules such as those set forth in the Open Internet Order, broadband providers represent a threat to Internet openness and could act in ways that would ultimately inhibit the speed and extent of future broadband deployment. First, nothing in the record gives us any reason to doubt the Commission's determination that broadband providers may be motivated to discriminate against and among edge providers. The Commission observed that broadband providers—often the same entities that furnish end users with telephone and television services—'have incentives to interfere with the operation of third-party Internet-based services that compete with the providers' revenue-generating telephone and/or pay-television services.'" *Verizon*, 740 F.3d at 645, (citing *2010 Open Internet Order*, 25 FCC Rcd 17916, para. 22).

186. "We can no longer conclude that broadband at speeds of 4 megabits per second (Mbps) download and 1 Mbps upload (4 Mbps/1 Mbps)—a benchmark established in 2010 and relied on in the last three Reports—supports the "advanced" functions Congress identified. Trends in deployment and adoption, the speeds that providers are offering today, and the speeds required to use high-quality video, data, voice, and other broadband applications all point at a new benchmark. . . . With these factors in mind, we find that, having 'advanced telecommunications capability' requires access to actual download speeds of at least 25 Mbps and actual upload speeds of at least 3 Mbps (25 Mbps/3 Mbps)." Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans

by proposals to allocate a larger percentage of universal service fund subsidies to broadband access.[187]

In light of the tremendous opposition to the FCC reclassification of broadband Internet access as unlawful, the "mission creep" in expanding the Section 706 and broadband development mission comes across as both justifiable and prudent. Remarkably, the FCC has opted for a far more controversial and aggressive posture, despite having a less provocative strategy that could have provided the Commission with the regulatory reach and flexibility it considered necessary.

2. VoIP Regulation Presents a Workable and Legally Defensible Model

Despite wanting to maintain an absolute, bright line dichotomy between regulated telecommunications services and unregulated information services, the FCC already has confronted the consequences of marketplace and technological convergence that prevents mutual exclusivity. The Commission has developed a track record of first avoiding having to make a regulatory classification for as long as possible. However, during this period of classification uncertainty, the Commission can and does assert jurisdiction, respond to complaints and make incremental decisions that apply regulatory burdens.

For example, even as the FCC continues to avoid classifying most types of VoIP, [188] it has imposed a number of regulatory burdens on ventures that provide access to and from conventional wired and wireless telephone networks, commonly referred to as the Public Switched Telephone Network ("PSTN"). With unconditional judicial approval, the FCC has imposed a number of requirements previously borne only by common carrier, telecommunications service providers. Even though the FCC does not explicitly treat VoIP operators as telephone companies, it considers them as

---

in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act, GN Docket No. 14-126, 2015 Broadband Progress Report and Notice of Inquiry on Immediate Action to Accelerate Deployment, FCC 15-10, 2015 WL 477864 (Rel. Feb. 4, 2015).

187. *See, e.g.*, FCC, Fact Sheet, *Chairman Wheeler Seeks Comment on Modernizing Lifeline for Broadband* (May 28, 2015), https://www.fcc.gov/document/chairman-seeks-comment-modernizing-reforming-lifeline-broadband; Connect America Fund ETC Annual Reports and Certifications, 29 FCC Rcd 8769 (2014)(implementing the Connect America Fund to advance the deployment of voice and broadband-capable networks in rural, high-cost areas); Connect America Fund, *Report and Order and Further Notice of Proposed Rulemaking*, 26 FCC Rcd 17663, 27 FCC Rcd 4040 (2011)(reforming and updating universal service funding), *aff'd sub nom*. In re FCC 11-161, 753 F.3d 1015 (10th Cir. 2014).

188. The FCC has classified only one type of VoIP service: computer-to-computer voice connections that do not have access to or from the PSTN. *See* Petition for Declaratory Ruling That Pulver.Com's Free World Dialup is Neither Telecommunications Nor a Telecommunications Service, Memorandum Opinion and Order, 19 FCC Rcd 3307 (2004).

competitive alternatives and functional equivalents regardless of which regulatory classification applies.

The FCC convinced an appellate court that the Commission did not first have to classify VoIP carriage before asserting exclusive jurisdiction and preempting state regulation.[189] Another court affirmed the FCC's direct statutory authority to require VoIP operators to contribute to universal service funding based on an interpretation of Section 254 of the Communications Act as requiring such payments from ventures that offer services that include a telecommunications component, even if the composite does not necessarily constitute a telecommunications service.[190]

Additionally, VoIP operators with PSTN access must provider subscribers with the same type of emergency 911 access as conventional telephone companies.[191] VoIP and conventional carriers must cooperate so that subscribers of a new service can retain their existing telephone number.[192] Further, VoIP operators have similar FCC reporting requirements on service outages,[193] the same limits on using subscriber information for

189. "The first issue is whether the FCC arbitrarily or capriciously failed to classify VoIP service as either an "information service" or a "telecommunications service." The FCC concluded state regulation of VoIP service should be preempted regardless of its regulatory classification because it was impossible or impractical to separate the intrastate components of VoIP service from its interstate components. . . . The impossibility exception, if applicable, is dispositive of the issue whether the FCC has authority to preempt state regulation of VoIP services. It was therefore sensible for the FCC to address that question first without having to determine whether VoIP service should be classified as a telecommunication service or an information service." *Minnesota Public Utilities Com'n. v. FCC*, 483 F.3d 570. 577-78 (8th Cir. 2007)(affirming FCC preemption of state VoIP regulation) (*citing* See *Nat'l Cable & Telecomms. Ass'n v. Gulf Power Co*., 534 U.S. 327, 338, 122 S.Ct. 782, 151 L.Ed.2d 794 (2002)(affirming FCC jurisdiction of pole-attachment rates for Internet traffic without having to determine whether such service constitutes a cable, telecommunications, or information service).

190. "The Commission's application of section 254(d) to interconnected VoIP providers involved two discrete decisions: (1) that, unlike the verb "offer," the verb "provide" may apply to the act of supplying a component of an integrated product, and (2) that VoIP providers supply telecommunications as a component of their service. . . . Finding that the Commission has section 254(d) authority to require interconnected VoIP providers to make USF contributions, we have no need to decide whether the Commission could have also done so under its Title I ancillary jurisdiction. *Vonage Holding Corp. v. FCC*, 489 F.3d 1232, 1240-41 (D.C. Cir. 2007)(affirming direct statutory authority for the FCC to required regulatory VoIP with PSTN access to contribute to universal service funds).

191. Nuvio Corp. v. FCC, 473 F.3d 302 (D.C. Cir. 2006).

192. Local Number Portability Porting Interval and Validation, *Report and Order*, 25 FCC Rcd 6953 (2010)(establishing fast deadlines for migrating a telephone service subscriber to and from VoIP service).

193. The Proposed Extension of Part 4 of the Commission's Rules Regarding Outage Reporting to Interconnected Voice Over Internet Protocol Service Providers and Broadband Internet Service Providers, Report and Order, 27 FCC Rcd 2650 (2012); *see also* Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications, New Part 4 of the Commission's Rules Concerning Disruptions to Communications Notice of Proposed Rulemaking, *Second Report and Order and Order on Reconsideration*, PS Docket No. 15-80, ET Docket No. 04-35, FCC 15-39, WL 1442082 (rel. March 30, 2015).

marketing purposes,[194] obligations to make service available to people with hearing and speech disabilities,[195] and the duty to cooperate with law enforcement officials.[196]

The FCC has found lawful ways to regulate VoIP without having to classify it as a telecommunications service. It appears that the Commission will use the same strategy to retain regulatory oversight of new voice telephone services that incumbent telephone companies will use as complete and total substitutes for common carrier, PSTN services.

The FCC likely will confront other instances of changed circumstances, triggered by convergence, which do not necessitate the use of common carrier regulation. For example, the Commission understands that broadband networks increasingly will become the primary media for all types of information, commerce, and entertainment ("ICE"). Leading trends show growing migration from old media, such as broadcasting, cable television and direct broadcast satellites, to new Over the Top[197] applications, including Internet Protocol Television ("IPTV").[198] Despite this growing trend, the FCC knows better than to subject new video service providers as regulated carriers, or the functional equivalent of regulated cable television systems.

---

194. Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (extending customer proprietary network information obligations to interconnected VoIP service providers), *aff'd sub nom*. *Nat'l Cable & Telecom. Assoc. v. FCC*, 555 F.3d 996 (D.C. Cir. 2009).

195. Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities; E911 Requirements for IP-Enabled Service Providers, CG Docket No. 03-123, WC Docket No. 05-196, Report and Order, 23 FCC Rcd 5255 (2008).

196. Communications Assistance for Law Enforcement Act and Broadband Access and Services, First Report and Order and Further Notice of Proposed Rulemaking, ET Docket No. 04-295, RM-10865, 20 FCC Rcd 14989 (2005), Second Report and Order and Memorandum Opinion and Order, 21 FCC Rcd 5360 (2006).

197. "Over-the-top VoIP [and other] services require the end user to obtain broadband transmission from a third-party provider, and providers of over-the-top . . . [services] can vary in terms of the extent to which they rely on their own facilities." 2010 Open Internet Order, n. 48.

198. "IPTV offers consumers with broadband connections options to download video files or view (streaming) video content on an immediate 'real time' basis." Sky Angel U.S., LLC, Emergency Petition for Temporary Standstill, DA 10-679, 25 FCC Rcd 3879 (2010). Some of the available content duplicates what cable television subscribers receive therein triggering disputes over whether cable operators can secure exclusive distribution agreements and prevent an IPTV service provider from distributing the same content. "Sky Angel has been providing its subscribers with certain Discovery networks for approximately two and a half years, including the Discovery Channel, Animal Planet, Discovery Kids Channel, Planet Green, and the Military Channel. Sky Angel submits that these channels are a significant part of its service offering." *Id*. at 3879-80; *see also* In-Sung Yoo, *The Regulatory Classification of Internet Protocol Television: How the Federal Communications Commission Should Abstain From Cable Service Regulation and Promote Broadband Deployment*, 18 COMMLAW CONSPECTUS 199 (2009).

The FCC also has adjusted its universal service programs to include Internet access even through telecommunications service subscribers and VoIP customers provide the funds for subsidies.[199] It does not need to establish regulatory parity, or apply the same regulatory classification of broadband and telecommunications carriers to justify significant changes as to who pays and who receives universal service subsidies. In a nutshell, the FCC understands that the future Internet ecosystem will grow increasingly essential and versatile, largely free of the conventional old media regulation.

An additional decision by the District of Columbia Circuit supports an FCC strategy short of reclassification. In *Cellco Partnership v. FCC*,[200] the court affirmed the FCC's decision requiring wireless carriers to negotiate commercial "roaming agreements," making it possible for subscribers located outside their local service area to access Internet services. The court reasoned that although wireless data access clearly constitutes an

199. "We begin by adopting support for broadband-capable networks as an express universal service principle under section 254(b) of the Communications Act, and, for the first time, we set specific performance goals for the high-cost component of the USF that we are reforming today, to ensure these reforms are achieving their intended purposes. The goals are: (1) preserve and advance universal availability of voice service; (2) ensure universal availability of modern networks capable of providing voice and broadband service to homes, businesses, and community anchor institutions; (3) ensure universal availability of modern networks capable of providing advanced mobile voice and broadband service; (4) ensure that rates for broadband services and rates for voice services are reasonably comparable in all regions of the nation; and (5) minimize the universal service contribution burden on consumers and businesses." In the Matter of Connect America Fund, WC Docket No. 10-90, A National Broadband Plan For Our Future, GN Docket No. 09-51, Report and Order and Further Notice of Proposed Rulemaking, 26 FCC Rcd. 17663, 17672 (2011), *aff'd sub nom*., *In re*: FCC 11-161, 753 F.3d 1015 (10th Cir. 2014).

"All telecommunications service providers and certain other providers of telecommunications must contribute to the federal Universal Service Fund (USF) based on a percentage of their interstate and international end-user telecommunications revenues. These companies include wireline phone companies, wireless phone companies, paging service companies and certain Voice over Internet Protocol (VoIP) providers."

Some consumers may notice a "Universal Service" line item on their telephone bills. This line item appears when a company chooses to recover its USF contributions directly from its customers by billing them this charge. The FCC does not require this charge to be passed on to customers. Each company makes a business decision about whether and how to assess charges to recover its Universal Service costs. Companies that choose to collect Universal Service fees from their customers cannot collect an amount that exceeds their contribution to the USF." FCC, FCC ENCYCLOPEDIA, *Contribution Methodology & Administrative Filings, Who Pays for Universal Service?*,

https://www.fcc.gov/encyclopedia/contribution-methodology-administrative-filings.

200. Cellco Partnership v. FCC, 700 F.3d 534, 541 (D.C. Cir. 2012),

information service provided by private carriers,[201] the FCC nevertheless can impose reasonable, non-common carrier duties to deal.[202]

The court noted that the FCC only required wireless carriers to negotiate commercially reasonable terms, meaning that terms and conditions need not be uniform and roaming need not be even offered if technically infeasible.[203]

V. CONCLUSION.

The FCC's decision to reclassify broadband Internet access as a telecommunications service significantly reduced the odds for affirmance by the District of Columbia Circuit. Rather than frame its regulatory intervention as non-common carriage safeguards needed to implement Section 706 of the Communications Act, the Commission opted for a more aggressive posture: reclassification of Internet access to qualify the service for a wide array of regulatory safeguards, many of which the Commission acknowledged as unnecessary. While the invocation of direct Title II statutory authority offers clarity and provides a large arsenal of available regulatory tools, the FCC increased the odds for reversal by going "all in" with such a forceful approach.

A. A Cascade of Strategic Miscalculations.

The decision to reclassify broadband Internet access as a telecommunications service adds to a sizeable list of flawed strategies and market assessments that began on or before 1988 and continue to the present. In 1988, the FCC submitted a Report to Congress that expressed the view that telecommunications services and information services constituted

201. *Cellco P'shipv. FCC*, 700 F.3d at 538 (D.C. Cir. 2012) ("The Commission has previously determined and here concedes that wireless internet service both is an "information service" and is not a [common carrier] 'commercial mobile service.' [citing Broadband Classification Order, 22 FCC Rcd at 5915–21 paras. 37–56] Accordingly, mobile-data providers are statutorily immune, perhaps twice over, from treatment as common carriers").

202. *Id.* at 537 ("[A]lthough the rule bears some marks of common carriage, we defer to the Commission's determination that the rule imposes no common carrier obligations on mobile-internet providers. In response to Verizon's remaining arguments, we conclude that the rule does not effect an unconstitutional taking and is neither arbitrary nor capricious. We therefore reject Verizon's challenge to the data roaming rule").

203. *Id.* at 548 ("The Commission has thus built into the 'commercially reasonable' standard considerable flexibility for providers to respond to the competitive forces at play in the mobile-data market. Although the rule obligates Verizon to come to the table and offer a roaming agreement where technically feasible, the 'commercially reasonable' standard largely leaves the terms of that agreement up for negotiation").

mutually exclusive, standalone services.[204] As it had done so previously,[205] the Commission sought the apparent ease and simplicity in establishing of a "bright line"[206] difference between regulated and unregulated services.

The FCC could consider the two services mutually exclusive and completely separate at a time when telephone companies, traditionally regulated as Title II common carriers, offered dial tone voice service that subscribers could retrofit for Internet access using analog modems.[207] The Commission could draw a plausible line of demarcation between conventional, basic service such as telephony and the enhancements achieved using dial tone. Before enactment of the Telecommunications Act of 1996, the FCC's *Computer Inquiry* policy also established mutual exclusivity between basic and enhanced services with the former deemed common carriage and the later unregulated. [208] The dichotomy worked,

---

204. Federal-State Joint Board on Universal Service, Report to Congress, 13 FCC Rcd 11,501, 11,522–23 (1998) ("The language and legislative history of [the Communications Act of 1996] indicate that the drafters . . . regarded telecommunications services and information services as mutually exclusive categories"); *see also Vonage Holdings Corp. v. Minn.Pub. Utils. Comm'n*, 290 F. Supp. 2d 993, 994, 1000-01 (D. Minn. 2003) (applying the FCC's dichotomy).

205. Statement of Commissioner Anne P. Jones Reconsideration of the Final Decision in the Second Computer Inquiry, Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry), Order on Reconsideration, 84 F.C.C.2d 50 (1980) ("I believe that our Basic/Enhanced definitional structure draws a bright line in the correct place between basic services, which we may continue to regulate, and enhanced services, which will be provided on an unregulated basis. Since I believe that competition should be relied upon to the fullest extent possible to meet the telecommunication needs of this country, I believe that a heavy burden of proof should be placed upon any carrier which wishes to modify any of the separation requirements imposed on the provision of enhanced services because such modifications would result in more services being subjected to varying degrees of regulation rather than being subjected to the test of the marketplace").

206. 2015 Open Internet Order at para.288 ("[W]e have ample legal bases on which to adopt the three bright-line rules against blocking, throttling, and paid prioritization"). 2015 Open Internet Order at para.288.

207. 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 Telecommunications Act of 1996, CC Docket 98-146, Notice of Inquiry, 13 FCC Rcd 15280, 15286-87 (1998) ("The incumbent LECs possess wire facilities that go the last mile to nearly every home and business in the United States. The last part of these last miles generally consists of copper that, as now used, lacks advanced telecommunications capability. . . .This collection of facilities we have just described, as it is now used, is capable of providing 'plain old telephone service' (POTS) and data communications and Internet access via dial-up modems. They are the only facilities that go to almost every home in this country and now provide POTS. For these facilities to provide certain advanced services, they would need either expensive improvement by new last miles, probably consisting of fiber or wireless connections, or new software or technology that will derive increased bandwidth from the existing twisted pair copper cable").

208. *See* Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry), Final Decision, 77 F.C.C.2d 384 (1980), aff'd sub nom. *Computer and Commc'ns Indus. Ass'n. v. FCC*, 693 F.2d 198 (D.C. Cir. 1982); Amendment of Sections 64.702 of the Commission's Rules & Regulations (Third Computer Inquiry), Report and Order, 104 F.C.C.2d 958 (1986), vacated sub nom. *California v. FCC*, 905 F.2d

because common carrier telephone companies operated bottleneck facilities needed by ventures seeking to offer unregulated information services.[209] The FCC could apply nondiscriminatory requirements solely on the access link provider without regulation of service providers using the link.

Technological innovation soon augmented and all but replaced dial up access to the Internet.[210] Broadband access became available from ventures lacking a history of common carrier operations, e.g., cable television companies. Recognizing the heritage of non-common carriage in cable television company-provided Internet access, the FCC opted to classify cable modem access as an information service in 2002.[211] Whatever political and public relations benefits the FCC accrued from its deregulatory posture quickly evaporated when it quickly realized that marketplace self-regulation would not resolve all disputes and foreclose harm to consumers. Unlike its strategic avoidance of making a definitive regulatory classification for VoIP, one of the "killer applications" of that time, the FCC willingly abandoned regulatory oversight.

The FCC clearly wants to reverse its 2002 mistake, but it has failed to come up with acceptable legal and factual rationales. In many instances, the Commission assumes the legal right—if not obligation—to use its expertise in fleshing out congressional intent and the interpretation of ambiguous statutory definitions. But when advantageous, the FCC has no problem interpreting the meaning of unmodified, service definitions, such as telecommunications service and information service. The problem lies in changed circumstances that the FCC considers the justification for switching,

---

1217 (9th Cir. 1990), on remand, Computer III Remand Proceedings: Bell Operating Co. Safeguards, Notice of Proposed Rulemaking & Order, 6 FCC Rcd 174 (1990), rule modification, 6 FCC Rcd 7571 (1991), vacated in part and remanded, California v. F.C.C., 39 F.3d 919 (9th Cir. 1994), on remand, Computer III Further Remand Proceedings: Bell Operating Co. Provision of Enhanced Servs., Order, 10 FCC Rcd 5692 (1995).

209. NTCA v. Brand X, 545 U.S. 967, 996 (2005) ("In the Computer II rules, the Commission subjected facilities-based providers to common-carrier duties not because of the nature of the 'offering' made by those carriers, but rather because of the concern that local telephone companies would abuse the monopoly power they possessed by virtue of the 'bottleneck' local telephone facilities they owned").

210. "Cable modem service typically includes many and sometimes all of the functions made available through dial-up Internet access service, including content, e-mail accounts, access to news groups, the ability to create a personal web page, and the ability to retrieve information from the Internet, including access to the World Wide Web. Because of the broadband capability of the cable plant, however, cable modem service subscribers can access the Internet at speeds that are significantly faster than telephone dial-up service. As a result of that faster access, subscribers can often send and view content with much less transmission delay than would be possible with dial-up access, utilize more sophisticated 'real-time' applications, and view streaming video content at a higher resolution and on a larger portion of their screens than is available via narrowband." Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, Internet Over Cable Declaratory Ruling, GN Docket No. 00-185, Declaratory Ruling and Notice of Proposed Rulemaking, 17 FCC Rcd 4798, 4805 (2002); *aff'd in part and vacated in part sub nom. Brand X Internet Services v. FCC*, 345 F.3d 1120 (9th Cir. 2003), *reversed and remanded sub nom.*, *National Cable & Telecommunications Ass'n v. Brand X Internet Services*, 545 U.S. 967 (2005).

211. *Id.*

some but not all service classifications. For example, the *2015 Open Internet Order* prevents last mile ISPs from paid enhancements without extraordinary proof that such a quality of service option would cause no harm. Yet the Order evidences no similar concerns for paid prioritization from upstream ISPs and CDNs. Curiously, the FCC maintains the information service classification for CDNs, despite the fact that these ventures, operating upstream from last mile ISPs, work on an integrated basis with last mile ISPs to achieve a complete and seamless link from content source to content consumer. CDNs can offer premium "better than best efforts" traffic management for "mission critical," "must see" video content, for any and all links until it reaches the last mile ISP. Apparently, information service providers and some yet unclassified ISPs, upstream from the last mile ISP, can provide enhancements consumers may want, but last mile ISPs cannot provide similar accommodations. The FCC does not adequately explain why paid prioritization for most of the Internet ecosystem would result in no harm to competition or consumers, but last mile enhancement all but guarantees it.

B. Handicapping the Odds for Affirmance.

The FCC nevertheless may succeed in convincing a reviewing court that circumstances have so changed that it needed to take radical steps to prevent calamity. Bear in mind that a reviewing court may affirm a regulatory agency's action even if the court could identify better alternatives, including ones that do not require as much deference. The Supreme Court chose not to second guess the FCC's initial classification of cable modem, broadband access even though some, or all of the justices might have considered the FCC's "reading [of the Communications Act service classifications as] differ[ing] from what the court believes is the best statutory interpretation."[212]

On two prior occasions, the FCC received clear messages from the judiciary: 1) the Commission should not have classified broadband access an information service initially unless it had ample empirical evidence that the Internet access was a robustly competitive ecosystem capable of self-regulating forever; and 2) having learned that such self-regulation was not feasible, the Commission could not finesse its voluntary abandonment of direct statutory authority to impose the safeguards it now considered necessary.

The FCC compounded the harm from its first mistake, by making the second mistake which has generated over a decade of regulatory uncertainty. Notwithstanding the FCC's mistake, the Internet has evolved and thrived with ample investment in software, applications and infrastructure. Competitors and consumers might have been better off had the FCC not committed these two mistakes, but these errors do not appear to have caused significant and measureable harm both in terms of consumer welfare and carrier profitability.

212. *Brand X*, 545 U.S. at 980.

Arguably, if an underestimation of the need for regulatory intervention has caused little harm, then the possibility exists that an overestimate of the need might have similarly negligible results. The state of FCC regulation of the wireless industry supports this premise as the Commission has available a large array of regulatory safeguards greater than what it claims it has reserved for broadband oversight.[213] No one can credibly assert that the actual degree of FCC oversight has reduced incentives for wireless common carriers to bid on spectrum and to make infrastructure investments. Perhaps the same real, or perceived, benign environment will continue in the Internet ecosystem.

The possibility exists that one or more reviewing courts will give the FCC the benefit of the doubt and refrain, this time, from second guessing the Commission. If the appellate court shows a willingness to ignore specious and counterproductive rationales, it might opt to concentrate on the Commission's direct statutory responsibilities created by Section 706 of the Communications Act. The court would have to ignore the warning given by Justice Scalia, in his *Brand X* dissent, that regulatory agencies regularly seek judicial deference based on superior skills in assessing changed circumstances. The court also would have to tolerate the FCC's new found ability to extract and regulate telecommunications services from services it previously considered as not worth regulating, even with an inseparable telecommunications component.

Put another way, the FCC has acted in a manner predicted by Justice Scalia in 2002. The Commission succeed in convincing a majority that it needed to ignore the telecommunications component to support a deregulatory regime. Now the Commission needs to convince an appellate court that the telecommunications component has become so important that it must be pulled from the deregulated safe harbor the FCC previously created. The Commission may not have sufficient persuasive power to finesse a changed regulatory classification based on a collection of conflicting factual and legal rationales.

213. *See supra*, n.24.

Communications Law:
Annual Review
The Judicial Practice Committee of the FCBA

TABLE OF CONTENTS

T-MOBILE SOUTH, LLC V. CITY OF ROSWELL, GEORGIA

No. 13-975 (U.S. Jan. 14, 2015)

In *T-Mobile South, LLC v. City of Roswell*,[1] the Supreme Court held that the Telecommunications Act of 1996 requires localities denying a cell-phone tower construction permit to provide or make available their reasons for doing so. The needn't, however, include those reasons in the formal denial letter; rather, "the locality's reasons may appear in some other written record so long as the reasons are sufficiently clear and are provided or made accessible to the applicant essentially contemporaneously with the written denial letter or notice."

Under the Telecommunications Act of 1996, "[a]ny decision by a State or local government or instrumentality thereof to deny a request to place, construct, or modify personal wireless service facilities shall be in writing and supported by substantial evidence contained in a written record."[2] In *T-Mobile*, the Court addressed "whether, and in what form, localities must provide reasons when they deny" such a request.[3]

This case arose from T-Mobile's application to build a new cell-phone tower in a residential area of Roswell, Georgia.[4] To build a cell-phone tower in a residential area, Roswell requires companies to use an "alternative tower structure," meaning "an artificial tree, clock tower, steeple, or light pole," which is "compatible with the natural setting and surrounding structures" and effectively camouflages the tower, as judged by the City Council.[5] In accord with this requirement, T-Mobile proposed to build a 108-foot-tall tower in the form of an artificial tree, termed a "monopine."[6]

Roswell's Planning and Zoning Division considered the application first and, finding it complied with the city's ordinances, recommended its approval.[7] The City Council, the ultimate arbiters of the issue, then scheduled a 2-hour public hearing during which it heard from the Planning and Zoning Division, T-Mobile, and local

1. T-Mobile South, LLC v. City of Roswell, No. 13-975 (U.S. Jan. 14, 2015).
2. Telecommunications Act of 1996,110 Stat. 151, 47 U. S. C. §332(c)(7)(B)(iii).
3. *T-Mobile*, slip op. at 1.
4. *See id.* at 1-2.
5. *See id.*
6. *See id.*
7. *See id.*

residents.[8] After each council member shared his thoughts on the tower issue, the Council unanimously rejected the application.[9]

Two days after the hearing, the Planning and Zoning Division issued a brief rejection letter, which provided no explanation of the decision but referred T-Mobile to the formal meeting minutes.[10] The meeting minutes, which contained the Councilmembers' remarks, were not available for another twenty-six days. Three days later, T-Mobile filed suit in federal court, alleging that the city violated the Telecommunications Act of 1996 when denying its application without the support of substantial evidence in the record.[11]

On cross-motions for summary judgment, the District Court held that Roswell, when denying T-Mobile's application, violated the Telecommunications Act, which the court interpreted to require a written notice explaining the reasons for denial in a manner sufficient to evaluate them against the written record.[12] The Eleventh Circuit reversed, holding that ""to the extent that the decision must contain grounds or reasons or explanations, it is sufficient if those are contained in a different written document or documents that the applicant is given or has access to."[13]

With the circuits split on whether and in what form a localities must provide its reasons for denial, the Supreme Court granted cert. In an opinion written by Justice Sotomayor, the Court answered the former in the affirmative and crafted a permissive standard for the latter.

First, the Court held that the Telecommunications Act "requires localities to provide reasons when they deny applications to build cell phone towers."[14] The Court explained that the Act "preserves 'the traditional authority of state and local governments to regulate the location, construction, and modification" of . . . cell phone towers, but imposes 'specific limitations' on that authority."[15] Among these limits is the requirement that denials must be in writing and supported by substantial evidence in the written record and that a denied applicant may seek judicial review. To give effect to these limits and others, "courts must be able to identify the reason or reasons

8. *See id.* at 2-3.
9. *See id.* at 13.
10. *See id.* at 4.
11. *See id.* at 4.
12. *See id.* at 5.
13. *See id.*
14. *See id.* at 6.
15. *Id.* (quoting Rancho Palos Verdes v. Abrams, 544 U.S. 113, 115 (2005)).

why the locality denied the application."[16] This conclusion is buttressed by Congress's use of "substantial evidence," a term of art that incorporates an existing body of administrative law requiring "that the grounds upon which the administrative agency acted to be clearly disclosed."[17] From this, the Court concludes that "localities must provide reasons when they deny cell phone tower siting applications . . . these reasons need not be elaborate or even sophisticated, but rather . . . simply clear enough to enable judicial review."[18]

Next, the Court held that these reasons need not "appear in the same writing that conveys the locality's denial of an application."[19] The text of the Act imposes several limitations on localities' power to turn down cell phone tower applications and its savings clause reserves the balance of power to state and local governments.[20] These factors suggest that the Act's enumerated limitations should be read as an exhaustive list.[21] Because the text of the Act does not proscribe a particular form in which the reasons must appear, it should not be read to impose one. Thus, "Congress imposed no specific requirement . . . but instead permitted localities to comply with their obligation to give written reasons so long as the locality's reasons are stated clearly enough to enable judicial review."[22] The Court did advise localities that, although detailed minutes are sufficient under the Act, providing a separate statement of reasons for the denial can help avoid prolonged litigation over the permissibility of its reasons.

Finally, the Court noted that "a locality cannot stymie or burden the judicial review contemplated by the statute by delaying the release of its reasons for a substantial time after it conveys its written denial."[23] Because aggrieved parties have only 30 days from the denial to seek judicial review and need time to make a reasoned decision, which they cannot do without knowing the reasons, the locality "must provide . . . its written reasons at essentially the same time as it communicates its denial."[24] "If a locality is not in a position to provide its reasons promptly, the locality can delay the issuance of its denial within this 90- or 150-day window, and instead release it along with its reasons once those reasons are ready to be provided. Only once the

16. *Id.*
17. *Id.* at 7-8.
18. *Id.* at 8.
19. *Id.* at 8-9.
20. *See id.* at 9.
21. *See id.*
22. *See id.*
23. *See id.* at 10
24. *See id.*

denial is issued would the 30-day commencement-of-suit clock begin."[25]

Thus, the Court held that "localities [must] provide reasons when they deny cell phone tower siting applications, but that the Act does not require localities to provide those reasons in written denial letters or notices themselves. A locality may satisfy its statutory obligations if it states its reasons with sufficient clarity in some other written record issued essentially contemporaneously with the denial."[26] Here, Roswell provided its reasons to T-Mobile for denying its application, and it did so in a permissible form – detailed minutes of the City Council meeting.[27] It did not, however, provide its reasons "essentially contemporaneously" with the written denial because the minutes were not available until 26 days after its issuance.[28] Because the 26-day delay rendered Roswell non-compliant with its statutory obligations, the Court reversed the judgment of the Eleventh Circuit and remanded the case for consideration of questions of harmless error or remedy.[29]

25. *See id.* at 11.
26. *See id.* at 14.
27. *See id.*
28. *See id.*
29. *See id.*

CBS CORPORATION V. FCC

785 F.3d 699 (D.C. Cir. 2015)

In *CBS Corporation v. FCC*,[1] the District of Columbia Circuit vacated an FCC order expediting disclosure of commercially-sensitive program-pricing information and documents to third parties in the course of a pre-merger review.[2] The Court held that the FCC failed to make the showing required by its own regulations to justify disclosure and failed to provide a reasoned explanation for changing its policy governing pre-disclosure judicial review.[3]

I. BACKGROUND

The Communications Act of 1934, requires the FCC to review cable company mergers and determine whether they serve "the public interest, convenience, and necessity."[4] This pre-merger review requires parties to submit information to the FCC, some of which is of a sensitive and proprietary nature.[5] To enhance its understanding of these materials, the FCC sometimes shares them with knowledgeable third parties.[6] When doing so, the FCC's Media Bureau ordinarily issues a protective order limiting, *inter alia*, access by merger-applicants' competitors and allowing merger applicants to challenge its disclosure decisions.[7]

The instant dispute arose during FCC review of the proposed AT&T/DirecTV and Comcast/Time Warner mergers, the latter of which has since been abandoned.[8] Because it was simultaneously reviewing merger proposals involving five[9] out of the world's seven largest video-programming distributors, the FCC requested sensitive documents, some relating to program-pricing negotiations and

1. CBS Corp. v. FCC, 785 F.3d 699 (D.C. Cir. 2015).
2. *See id.* at 710.
3. *See id.* at 700-702.
4. *See id.* at 700 (citing & quoting 47 U.S.C. § 310).
5. *See id.*
6. *See id.*
7. *See id.* at 701-02.
8. *See id.* at 700-01.
9. The fifth participant was Charter Communications, which was then involved in the Comcast/Time Warner proposal through a partial divestiture agreement. *See id.* at 701. The Comast/Time Warner merger has since been abandoned. *See id.* at 700-01 (citing Shalini Ramachandran, *Comcast Kills Time Warner Cable Deal*, WALL ST. J. (Apr. 24, 2015), http://goo.gl/vPG1hh).

agreements, which "it believed would help it evaluate these important corporate marriages."[10]

These merging parties, however, did not object to the required disclosures; rather, the instant case was brought by content producers—CBS, Viacom, Disney, *et al.*—who have program-distribution contracts with the merging entities, the terms of which they would like to keep confidential.[11] These content-producer Petitioners, seek to protect their Video Programming Confidential Information (VPCI), which includes negotiations, agreements, and pricing terms between the cable companies and content providers.[12]

At the Commission level, the Petitioners opposed allowing any third-party access to VPCI, contending the agency should review the materials itself, in secret.[13] In response, the Media Bureau maintained third-party access to VPCI but augmented its traditional protective order by expanding the disclosure restrictions to include content producers' competitors and empowering content producers to lodge pre-disclosure objections.[14] With these new rights in hand, Petitioners broadly objected to all VPCI access requests, concerned that many filers were their direct competitors.[15]

The Media Bureau, worrying that objections' pre-disclosure resolution would substantially delay merger review, issued the *November Bureau Order*,[16] truncating review of Media Bureau disclosure determinations.[17] The Order allowed disclosure to "individuals seeking to view VPCI . . . just five days after the Bureau—not the [FCC] or a court—rejects any objections."[18] Over the Petitioners' objections, the FCC affirmed the *November Bureau Order* and adopted its reasoning in the *November Commission Order*.[19] The FCC did, however, delay access, allowing Petitioners to seek judicial

10. *See id.* at 701.

11. *See id.*

12. *See id.*

13. *See id.* at 702.

14. *See id.* (citing Applications of Comcast Corp. et al. for Consent to Assign or Transfer Control of Licenses and Authorizations, Bureau Order, DA 14-1463, paras. 2, 7–8, 10 (MB October 7, 2014)).

15. *See id.*

16. Applications of Comcast Corp. et al. for Consent to Assign or Transfer Control of Licenses and Authorizations, Order, Order on Reconsideration, DA 14-1605 (MB Nov. 4, 2014). *See also* Applications of Comcast Corp. et al. for Consent to Assign or Transfer Control of Licenses and Authorizations, Amended Modified Joint Protective Order, DA 14-1602, 14-1604 (MB Nov. 4, 2014).

17. *See CBS*, 785 F.3d at 703.

18. *Id.*

19. *See id.* (citing Applications of Comcast Corp. et al. for Consent to Assign or Transfer Control of Licenses and Authorizations, Order, 29 FCC Rcd ___, FCC 14-202 (Nov. 10, 2014)).

review, upon which the a special panel of the District of Columbia Circuit stayed disclosure of the VPCI.[20] On review, Petitioners argued that the FCC's determination violated the Trade Secrets Act[21] and the FCC's own Confidential Information Policy[22] and that it departed from past practice without explanation.[23]

II. ANALYSIS

In *CBS v. FCC*, the Court considered whether the FCC may "disclose petitioners' confidential information to third parties and may it do so on a timeline so swift as to effectively preclude judicial review?"[24] Answering this question entailed two inquiries: whether the confidential information disclosures were consistent with the FCC's own requirements and whether its policy change was arbitrary and capricious.

A. Substantive Challenge to the FCC's Decision to Disclose the Trade Secrets in the Course of Its Pre-Merger Review.

The Court first considered whether disclosure was proper, under FCC regulations and policy.[25] FCC regulations require a party seeking disclosure of private information to make a "persuasive showing."[26] Assuming without deciding that, under the circumstances, the FCC is required to make the requisite showing, the Court faced two questions: "what exactly does that persuasive showing entail, and has the [FCC] made its case?"[27] After grappling with substantial confusion over the meaning of the FCC's disclosure policies,[28] the Court ultimately concluding that the FCC had impermissibly ignored part of its own requirements.[29]

To determine what a "persuasive showing" entails, the Court turned to the FCC's *Confidential Information Policy*.[30] Paragraph 8 of

20. *See id.*

21. 18 U.S.C § 1905 (2014). The Court did not reach the issue of consistency with § 1905.

22. 47 C.F.R. § 0.457 (2015)). *See also* Examination of Current Policy Concerning the Treatment of Confidential Information, 13 FCC Rcd 24816 (1998) [hereinafter *Confidential Information Policy*].

23. *CBS*, 785 F.3d at 703.

24. *Id.*

25. *See id.*

26. *See id.* at 704.

27. *Id.*

28. *See id.* at 703-05.

29. *See id.* at 708.

30. *See id.* at 704.

the *Policy* sets forth a clear test, balancing the interests of disclosure and nondisclosure and requiring the contested information be a "necessary link" to resolution of an issue.[31] But later, in Paragraph 17, the *Policy* explains that "'[b]ecause [the FCC] believe[s] that a case-by-case determination is most appropriate . . . [it] decline[d] to adopt a blanket rule requiring the requester to demonstrate that access is 'vital' to the conduct of a proceeding [or] necessary to the 'fundamental integrity' of the Commission process at issue.'"[32] As the Court explained, these provisions are contradictory—the former requiring a "necessary link" and the latter disavowing any necessity requirement.[33] Ultimately, the Court found that Paragraph 17's ambiguity did not negate the clear requirements of Paragraph 8 and held that "to make the persuasive showing necessary to disclose petitioners' confidential documents, [the proponent] must explain (1) why disclosure is in the public interest, (2) why it is a good idea on balance, and (3) why the information serves as a ''necessary link in a chain of evidence.'"[34]

Next, the Court applied this standard, finding that the *November Bureau Order* adequately explained why disclosure was in the public interest and a good idea on balance, but failed to show it was a necessary link in its pre-merger review.[35] First, it accepted that obtaining "different perspective on materials that the [FCC] is considering" in the course of its pre-merger review responsibilities "facilitates informed decision making," which is in the public interest.[36] Second, it accepted that, in light of the governing protective orders' limits on access to and use of VPCI, the benefits of disclosure outweigh the potential competitive harms feared by Petitioners.[37]

But, finally, the Court found insufficient the Bureau's finding that VPCI is "'highly relevant . . . to the pending transactions'—even 'central'" because neither rises to the level of "necessary."[38] Although the documents "'provide what is likely the best evidence available to test the validity of allegations'" about how the proposed mergers would change the market and the FCC "would . . . be derelict if it *failed* to consider VPCI as it evaluates the proposed mergers," disclosure was

31. *See id.*
32. *Id.* at 705 (quoting *Confidential Information Policy*, para. 17) (some alterations in original).
33. *See id.* at 704-05.
34. *See id.* at 705.
35. *See id.* at 705-06.
36. *Id.* at 705.
37. *See id.*
38. *Id.* at 706 (quoting *November Bureau Order*, para. 23).

still prohibited without a showing of necessity.[39] In sum, the Court explained: "Are the documents relevant? Absolutely. Important? Sure. Central? Probably. . . But to justify disclosure, the information must be 'necessary,'" and here they were not.[40]

B. Procedural Challenge to the FCC's Departure from Prior Agency Practice

Next, the Court considered whether the FCC's action was procedurally invalid because it failed to explain its change of policy on pre-disclosure review of Bureau determinations.[41] Under prior FCC policy, disputed information remained confidential until objectors' concerns were resolved by the Commission and/or judiciary,[42] while the new policy effectively eliminated this pre-disclosure review by allowing disclosure five days after a Bureau determination.[43]

The Court found that this "amounts to a substantive and important departure from prior [FCC] policy," which Petitioners argued the FCC "failed entirely to acknowledge . . . much less to explain."[44] Under the APA, "[w]hen an agency departs from past practice, it 'must provide a reasoned analysis indicating that prior policies and standards are being deliberately changed, not casually ignored.'"[45] The Court found that while the Bureau had acknowledged it was modifying the protective order "nowhere [did it acknowledge] that the new rule departs from longstanding practice," and the mere addition of the five-day rule to the protective order (the departure from past practice itself) is "completely insufficient" to serve as acknowledgement.[46]

Next, the Court considered whether, by acknowledging alteration of the protective orders, the Bureau recognized a larger policy shift.[47] The Court held that "admitting to a technical change in the *governing documents* is a far cry from acknowledging a fundamental departure from longstanding *policy*. Instead, it seems like the old policy is being casually ignored."[48] It further found the FCC's

39. *Id.* at 707.
40. *Id.*
41. *See id.* at 708.
42. *See id.*
43. *See id.*
44. *See id.*
45. *Id.* at 708 (quoting Ramaprakash v. Federal Aviation Administration, 346 F.3d 1121, 1124 (D.C. Cir. 2003)).
46. *Id.* at 709.
47. *See id.*
48. *See id.* (internal quotation marks omitted).

rationales for the departure "exceedingly thin."[49] First, it was unclear whether or how pre-disclosure review of a Bureau determination actually slowed down pre-merger review because the FCC could still review the VPCI internally. Second, concerns over abuse of the objection process "rest[ed] on a flawed premise" because, although Petitioners challenged all of the 266 access requests, most were challenges to VPCI disclosure generally and "the objection process represented the only administrative avenue open to petitioners to protect their right to meaningful pre-disclosure review."[50]

Finally, in *dicta* the Court offered a "cautionary observation," without pre-judging the issue, that "should [the FCC] choose to retain the five-day rule, it must not only come forward with a 'reasoned analysis' for this dramatic break from the past, but also explain why speed is so important as to justify limiting one of the fundamental principles of administrative law—judicial review." [51]

II. CONCLUSION

In sum, the Court vacated the *November Commission Order* for both substantive and procedural infirmity.[52] Substantively, the FCC's non-compliance with its own disclosure requirements rendered its action unlawful.[53] Procedurally, the FCC failed to acknowledge or explain its departure from past practice.[54]

49. *Id.*
50. *Id.* at 709-710.
51. *Id.* at 710
52. *See id.* at 710.
53. *See id.* at 707.
54. *See id.* at 709.

Sorenson Communications v. FCC (Sorenson II)

765 F.3d 37 (D.C. Cir. 2014)

In *Sorenson Communications Inc. v. FCC* (*Sorenson II*),[1] the District of Columbia Circuit largely upheld the FCC's *2013 VRS Rate Order*[2] against a service provider's challenge that it was arbitrary and capricious.[3] The Court upheld the *Order*'s set rates and tiered rate structure but vacated and remanded the agency's enhanced speed-of-answer requirements for further consideration.[4]

I. BACKGROUND

The Americans with Disabilities Act of 1990 requires the FCC to make available telecommunications relay services (TRS), providing hearing or speech impaired individuals with service 'functionally equivalent" to non-disabled Americans.[5] Costs of these services are covered by the TRS Fund, which is funded by communications industry contributions and pays TRS providers a per-minute rate, which reflects the provider's costs.[6]

One such resource is video relay service (VRS), which "works much like a video call that any caller might make using a digital platform such as Skype or Apple FaceTime."[7] In the course of VRS, "[t]he video call is placed to an American Sign Language interpreter, employed by the VRS provider, who then makes a standard voice call to the video caller's hearing recipient. The interpreter signs with the caller via the visual connection and speaks with the recipient via the voice connection, translating messages back and forth."[8]

With respect to VRS, although, "[t]he per-minute rate is supposed to approximate the cost incurred to provide VRS, . . . for much of the past decade the rate has generated revenues well in excess of that cost."[9] The FCC sought to remedy that imbalance and "more

1. Sorenson Comm'ns, Inc. v. FCC (*Sorenson II*), 765 F.3d 37 (D.C. Cir. 2014)

2. *In re* Structure & Practices of the Video Relay Serv. Program, Telecomms. Relay Servs. & Speech–to–Speech Servs. for Individuals with Hearing & Speech Disabilities, Report & Order & Further Notice of Proposed Rulemaking, 28 FCC Rcd 8618, 8661, ¶ 107, 8706–07, ¶ 217 (2013) [hereinafter *VRS Rate Order*].

3. *See Sorenson II*, 765 F.3d at 40 (citing 5 U.S.C. § 706(2)(a)).

4. *See id.* at 52.

5. *See id.* at 41.

6. *See id.*

7. *Id.* at 40.

8. *See id.*

9. *See id.* at 40.

accurately to reflect cost[s] until it could develop a new approach to reimbursement," by "lower[ing] the per-minute rates first in its *2010 Rate Order* and again in its *2013 Rate Order*."[10]

Petitioner Sorenson Communications, Inc., the leading provider of VRS, incurred voluntary costs under the pre-2010 reimbursement rates which are unsustainable at the current rate.[11] Unhappy with the new regime, Sorenson brought suit under the Administrative Procedure Act (APA), arguing that the *2013 Rate Order* was arbitrary and capricious.[12]

II. ANALYSIS

In *Sorenson II*, the Court addressed whether Sorenson was precluded, by prior litigation, from challenging the *2013 Rate Order* before considering whether the *Order*'s rate-of-return methodology, overall impact on TRS providers' finances, speed-of-answer requirement, and tiered rate structure are arbitrary and capricious.

The Court precluded Sorenson from re-litigating the FCC's compensable expense list because the Tenth Circuit had already ruled on the issue and nothing had changed since that time.[13] It was not, however, precluded from challenging "features unique to the 2013 Rate Order [which] therefore could not have been resolved in the Tenth Circuit case," including the end result of the *2013 VRS Rate Order*, its newly-imposed requirements, its alterations to the rate structure, and whether it adequately considered changed circumstances.[14]

A. The Rate-of-Return Methodology Was Not Arbitrary or Capricious Because It Covered the Reasonable Costs of Providing VRS

The Court considered whether the FCC acted arbitrarily and capriciously by applying a rate-of-return scheme that was designed for traditional telephone companies to the substantially different VRS industry.[15] When the FCC crafts rate-setting methodology for TRS fund reimbursements, the Communications Act entitles VRS providers to compensation "only for the reasonable costs of providing

10. *See id.*
11. *Id.* at 40.
12. *See id.* (citing 5 U.S.C. § 706(2)(a)).
13. *See id.* at 44-45 (citing Sorenson Commc'ns Inc. v. FCC, 659 F.3d 1035 (10th Cir. 2011).
14. *See id.* at 46.
15. *See id.*

VRS."[16] First, the Court held that, when denying a return on labor costs, the FCC "act[ed] directly in accord with its statutory mandate by setting rates to compensate providers for their actual labor costs," not in excess of the reasonable costs of VRS provision.[17]

The Court further held that maintaining the 11.25% capital rate of return, which was borrowed twenty years ago from monopoly telephone regulations, was not itself arbitrary and capricious because, although perhaps a "misstep," petitioners bear the burden of demonstrating a decision's unreasonableness.[18] Still considering the capital rate-of-return's reasonableness, the Court held that the gross profit margin yielded by the rate, here less than 2%, is irrelevant because VRS providers are only entitled to reasonable reimbursement for costs, not profit.[19]

The Court explained, however, that the capital rate of return would be unreasonable and unlawful if it were too low to attract the capital necessary to operate a VRS business.[20] On this issue, the Court acknowledged that that the VRS industry has a "significantly different risk profile to the capital markets" than a traditional phone company, which "suggest[s] a Telephone Company's rate of return is not an obvious proxy for reimbursing a provider of VRS."[21] "[T]he [FCC's] admittedly flawed basis for selecting a rate," however, does not "lead[] to an arbitrary and capricious result because there is no evidence in the record to suggest Sorenson or any other provider actually has had trouble raising the necessary capital under the long-standing 11.25% rate regime."[22]

B. Allowing VRS Providers Incurring Unnecessary Expenses to Go Bankrupt Is Not Arbitrary and Capricious

Next, the Court considered Sorenson's "end result" challenge, which asks whether, even if all components of an agency's decision were individually reasonable, "they . . . *together* produce arbitrary or unreasonable *consequences*."[23] Here, the contested end result was Sorenson's contention that the rates were set so low as to drive VRS providers into bankruptcy.[24] First, the Court rejected Sorenson's

16. *Id.* at 46-47 (citing 47 U.S.C. § 225(d)(3)(B)).
17. *Id.*
18. *Id.* at 47.
19. *See id.*
20. *See id.*
21. *Id.* at 48.
22. *Id.* (footnote omitted).
23. *Id.*
24. *Id.*

contention that "every" provider would be driven to bankruptcy, because the FCC had already upwardly adjusted rates in response to several industry comments to that effect.[25]

Considering the prospect of *some* providers going bankrupt, the Court explained it is not unreasonable "to allow a provider to go bankrupt if that provider has incurred costs far in excess of what is necessary."[26] The Court also found that the FCC adequately addressed these contentions by explaining that "it would not cover all of a provider's actual costs even if the result were to bankrupt the company" because "it would be 'irresponsible and contrary to . . . the efficient provision of TRS to simply reimburse VRS providers for all capital costs they have chosen to incur—such as high levels of debt—where there is no reason to believe that those costs are necessary to the provision of reimbursable services.'"[27] Because VRS providers are not entitled to reimbursement in excess of costs and allowing some providers to go bankrupt based on voluntarily-incurred obligations was not unreasonable, the Court held it was not an arbitrary or capricious consequence.[28]

C. Enhancing Speed of Answer Requirements Its Effect on Costs Was Arbitrary and Capricious

The Court next considered whether the FCC acted arbitrarily and capriciously by failing to consider whether an enhanced speed-of-answer requirement would increase provider costs.[29] In the *VRS Rate Order*, the FCC required providers to answer more calls at a faster rate and changed the frequency of measurement from monthly to daily. [30] Despite Sorenson's comments to the contrary the FCC made the unsupported determination that this would not increase provider costs.[31] The Court held that the FCC acted arbitrarily and capriciously both by adopting the requirement without evidence of its impact on costs and by failing to exercise reasoned decision-making when disregarding the only record evidence of costs—Sorenson's comments.[32] The Court, however, declined to remedy the error by vacating the *Order*'s new VRS rates and instead vacated only the speed of answer requirement, remanding it to the agency for further

25. *See id.* at 48-49.
26. *Id.* at 48.
27. *Id.* at 49 (quoting *VRS Rate Order*, para. 195).
28. *See id.*
29. *See id.* at 49-50.
30. *See id.*
31. *See id.*
32. *See id.* at 50.

consideration.[33]

D. Retention of Inefficient Tiered Rate Structure During Transition to New Rate-Setting Scheme Was Not Arbitrary and Capricious

Finally, the Court considered whether the *Order*'s tiered rate structure is arbitrary and capricious because it is inefficient and ill-suited to its goal of supporting small providers.[34] The Court upheld the tiered rates over these challenges because some transitional inefficiency was acceptable as the FCC worked to implement its new competitive-bidding scheme and because the methodology "is explicitly aimed at achieving efficiency in the long run."[35]

III. CONCLUSION

In *Sorenson II*, the Court upheld the reduction of VRS rates because the FCC had considered costs necessary to the provision of VRS service when setting the rate and was not required to consider unnecessary voluntarily-incurred costs, even if ruinous for a provider.[36] The Court vacated the speed-of-answer requirement, remanding it to the FCC for further consideration, because the FCC acted arbitrary and capriciously when failing to consider compliance costs when setting the rate.[37] Finally it held that the FCC adequately justified the *Order*'s adjusted tiered-rate structure because, as a transitional measure, it was reasonable although inefficient.[38]

33. *See id.* at 51.
34. *See id.*
35. *Id.*
36. *See id.* at 40-41.
37. *See id.* at 41.
38. *See id.*

SORENSON COMMUNICATIONS, INC. V. FCC (SORENSON I)

755 F.3d 702 (D.C. Cir. 2014)

In *Sorenson Communications, Inc. v. FCC* (*Sorenson I*),[1] the District of Columbia Circuit struck down the FCC's *Misuse of Internet Protocol (IP) Captioned Telephone Service Interim Order*, and *Misuse of Internet Protocol (IP) Captioned Telephone Service Order*. First, the Court held that agency invocations of good cause to forgo notice-and-comment rulemaking procedures are reviewed de novo and that the FCC violated the APA by improperly invoking the good cause exception for impracticability. Next, the Court held that the agency acted

I. BACKGROUND

The Americans with Disabilities Act of 1990 require the FCC "to arrange for telecommunications relay services (TRS) that are 'functionally equivalent to the ability of a hearing individual who does not have a speech disability.'"[2] To cover the costs of these services the FCC created the TRS Fund, which is funded by communications industry contributions and pays TRS providers between $1.2855 and $6.2390 per minute, depending on the service provided.[3]

"One type of TRS service is the Internet Protocol Captioned Telephone Service (IP CTS), which uses the Internet to transmit phone conversations and captioned messages between hearing-impaired users, third-party callers, and relay operators."[4] IP CTS providers are reimbursed $1.7877 per minute for their services.[5]

One provider of IP CTS services, Sorenson Communications, began furnishing its caption-displaying phones to customers for free—unlike its competitors.[6] This lead to concern that Sorenson's method would strain the TRS Fund, far exceeding the projected disbursements.[7] Because of this concern the FCC promulgated several interim rules in an *Interim Order*, which "cited the potential for Fund depletion caused by IP CTS misuse as 'good cause' for bypassing the

1. Sorenson Comm'ns Inc. v. FCC (*Sorenson I*), 755 F.3d 702 (D.C. Cir. 2014).
2. *Id.* at 704 (quoting 47 U.S.C. § 225(a)).
3. *See id.*
4. *See id.*
5. *See id.* at 705.
6. *See id.*
7. *See id.*

notice-and-comment requirements of the Administrative Procedure Act (APA)."[8] The *Interim Order* instituted two new requirements: (1) a certification of hearing impairment for all new IP CTS users, those who purchase equipment for $75 or more could self-certify but below that threshold a professional certification was required; and (2) IP CTS phones must be distributed with captions defaulted to off.[9]

After notice and comment the FCC released a revised final rule, which revised the interim rules and, in their place, required: (1) most IP CTS phones were to cost $75 or more to be eligible for TRS reimbursement (the $75 Rule), and (2) captions must be off by default unless a medical professional certifies an individual is too disabled to turn on the captions manually (the Default-Off Rule).[10] Sorenson, dissatisfied with the Rule, petitioned for review.

II. ANALYSIS

Sorenson challenged the FCC's finding of good cause to waive the APA's notice and comment procedures.[11] Under the APA, an agency may "bypass the notice-and-comment requirement of the APA when it 'for good cause finds . . . that notice and public procedure thereon are impracticable, unnecessary, or contrary to the public interest.'"[12]

A. Courts Review an Agency's Invocation of Good Cause De Novo

The Court noted it had never "expressly articulated" the standard of its review of an agency's invocation of good cause, and the FCC urged that it should be afforded some measure of deference.[13] The Court rejected this argument, explaining that agencies lack interpretive authority over the APA and because affording deference "would conflict with this court's deliberate and careful treatment of the exception in the past."[14] Rather, the Court held that it reviews an agency's invocation of good cause *de novo*, while deferring "to an

8. *See id.* (citing Misuse of Internet Protocol (IP) Captioned Telephone Service, Interim Order, 28 FCC Rcd 703 (2013)).

9. *See id.*

10. *See id.* (citing Misuse of Internet Protocol (IP) Captioned Telephone Svc., Order, 28 FCC Rcd 13420 (2013)).

11. *See id.* at 706.

12. *See id.* (citing 5 U.S.C. § 553(b)(3)(B)).

13. *See id.*

14. *See id.*

agency's factual findings and expert judgments therefrom," unless arbitrary and capricious.[15]

B. Notice-and-Comment Procedures Were Not Impracticable for the Interim Order

The FCC justified its invocation of good cause on impracticability grounds, citing "the threat of impending fiscal peril" to the TRS Fund.[16] "Impracticability is an 'inevitably fact-or-context dependent' inquiry,"[17] which the Court has applied to "an agency's decision to bypass notice and comment where delay would imminently threaten life or physical property."[18] The Court noted that, although relying on the threat of fiscal peril as its good cause, the FCC offered no factual findings to support this speculative assertion.[19] Rejecting the FCC's argument, the Court held that "[t]hough we do not exclude the possibility that a fiscal calamity could conceivably justify bypassing the notice-and-comment requirement, this case does not provide evidence of such an exigency."[20] It explained that the FCC's record was "too scant" to show a fiscal emergency,[21] and "[t]hough no particular catechism is necessary to establish good cause, something more than an unsupported assertion is required."[22] Accordingly, the FCC's invocation of impracticability as good cause to waive notice-and-comment procedures was unlawful because it "[l]ack[ed] record support proving the emergency."

15. *See id.* at 706 & n.3.

16. *See id.* at 706.

17. *Id.* (quoting Mid–Tex Elec. Coop. v. FERC, 822 F.2d 1123, 1132 (D.C.Cir.1987)).

18. *Id.* (citing Jifry v. FAA, 370 F.3d 1174, 1179 (D.C. Cir. 2004) ("imminent hazard to air- craft, persons, and property"); Council of the S. Mountains, Inc. v. Donovan, 653 F.2d 573, 581 (D.C. Cir. 1981) (mine explosion)).

19. *See id.* In his partial dissent, however, Commissioner Pai provided some figures indicating that the TRS Fund's unsupportable payout rate would have saddled it with obligations between $108 and $159 million for the second half of the 2012-2013 fiscal year. *See id.* The Court noted that, while this might be cause for concern, it is "hardly a crisis." *Id.* at 707.

20. *Id.* at 707.

21. For example, the *Interim Order* "does not reveal when the Fund was expected to run out of money, whether the Fund would have run out of money before a notice-and-comment period could elapse, or whether there were reasonable alternatives available to the Commission, such as temporarily raising Fund contribution amounts or borrowing in anticipation of future collections." *See id.*

22. *Sorenson I*, at 707.

C. The Final $75 Rule and Default-Off Rule Were Arbitrary and Capricious

The Court then turned to Sorenson's assertions that the Final Order's $75 and Default-Off Rules are arbitrary and capricious, in violation of the APA.[23] The Supreme Court has explained that "[u]nder the arbitrary-and-capricious standard, an agency 'must examine the relevant data and articulate a satisfactory explanation for its action including a rational connection between the facts found and the choice made.'"[24] An agency contravenes this standard when it:

> [R]elie[s] on factors which Congress has not intended it to consider, entirely faile[s] to consider an important aspect of the problem, offer[s] an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise.[25]

Applying this standard, the Court first considered whether the FCC offered a satisfactory explanation for the $75 Rule, which it justifies as a way to "deter fraudulent acquisition and use of IP CTS equipment."[26] Characterizing the rule as "mystifying," the Court took issue with the dearth of record evidence indicating IP CTS fraud occurs, suggesting a causal relationship between hypothetical fraud and equipment pricing, or justifying why $75 is the appropriate price floor.[27] The FCC countered that its "predictive judgments" about the probable effect of the $75 are entitled to deference, but the Court explained that to warrant such deference "judgement[s] must be based on some logic and evidence not sheer speculation."[28] The Court, accordingly, determined that the FCC acted arbitrary and capriciously when promulgating the $75 Rule.

The Court then turned to the FCC's justifications for promulgating the Default-Off Rule to address fraudulent use of IP CTS technology.[29] But the Court concluded not only was fraudulent use of IP CTS a "boogeyman," but, moreover, the efficacy of the FCC's chosen means of addressing it was undercut by contrary

23. *See id.* Sorenson also argued that the FCC's action violated the ADA, but the Court did not reach that issue.

24. *Id.* (quoting Motor Vehicles Mfrs. Ass'n v. State Farm Mut. Auto. Ins., 463 U.S. 29, 43 (1983)).

25. *See id.* (quoting *State Farm*, 463 U.S. at 43).

26. *See id.*

27. *See id.* at 707-708.

28. *See id.* at 708.

29. *See id.* at 709.

evidence.[30] Because the contrary evidence cast doubt on the efficacy and necessity of the Default-Off Rule and the FCC "left these serious concerns unaddressed," its promulgation was arbitrary and capricious.

III. CONCLUSION

In sum, the Court reviewed the FCC's invocation of good cause to bypass APA rulemaking procedures *de novo*, vacating the Interim Rule because the commission failed to show that notice and comment would be impractical because the FCC's record was "too scant" to show a fiscal emergency, and "something more than an unsupported assertion is required" to establish good cause.[31].[32] The Court, moreover, vacated the FCC's final $75 and Default-Off Rules as arbitrary and capricious because the record supported neither its factual predicate nor reasoning and the agency failed to show its exercise of "predictive judgment" was based on anything more than "sheer speculation."[33]

30. *See id.* at 710.
31. *See id.* at 707, 710.
32. *See id.*
33. *See id.* at 708.

SPECTRUM FIVE LLC V. FCC

758 F.3d 254 (D.C. Cir. 2014)

In *Spectrum Five LLC v. FCC*,[1] the District of Columbia Circuit held that that a satellite operator, working in partnership with the Netherlands, lacked Article III standing to challenge the FCC's decision to grant a competitor's satellite-relocation request because vacating the *Order* was insufficiently likely to redress its injury.[2] The Court so concluded because redress would require an international orbital-location regulatory body, not subject the Court's jurisdiction, to reverse its prior determination that Bermuda had acquired the rights to the contested orbital location.[3]

I. BACKGROUND

Overlapping international and domestic authorities regulate broadcast satellites; internationally, the International Telecommunication Union (ITU) administers a treaty-based regulatory framework and, in America, the FCC regulates all satellites that transmit or receive signals within our territorial jurisdiction.[4]

A multi-national treaty, administered by the ITU, apportions orbital locations and spectrum among treaty-member nations (called "administrations" in ITU parlance).[5] The treaty's allocations, however, are not set in stone—an administration can seek to modify its apportionment by filing a request with the ITU.[6] To gain the rights to the requested location, the administration must then (1) "bring into use" the requested assignment, by operating a satellite at that location, within 8 years of filing the request and (2) reach an agreement with any affected administrations.[7]

1. Spectrum Five LLC v. FCC, 758 F.3d 254 (D.C. Cir. 2014).
2. *See id.*, at 261
3. See id.
4. *See id.*, at 256
5. *See id.*
6. *See id.*, at 257.
7. *See id.*

Bermuda[8] sought to gain the rights to a particular new orbital location[9] by modifying its apportionment under the treaty.[10] In 2005, it began the process by filing a request with the ITU, in accord with the international regulatory scheme.[11] Seeking to bring the orbital location into use, Bermuda then arranged to have a satellite, the FCC-licensed Echostar6, moved to the requested location.[12] Meanwhile, the Netherlands,[13] seeking the rights to essentially the same orbital location,[14] filed its own request with the ITU in 2011.[15] This filing, however, was subordinate to Bermuda's earlier-filed one and the location would be unavailable if Bermuda timely completed the steps to obtain the orbital rights.[16]

As an FCC-licensed satellite, FCC approval was required to move EchoStar6 and, accordingly, bring Bermuda's requested orbital location "into use."[17] To get FCC approval, a satellite operator must submit an application, which is then subject to a 30-day notice-and-comment period, after which the agency either grants or denies the application.[18]

But in early 2013, with only months remaining on the 8-year deadline for Bermuda to bring the orbital location into use, EchoStar, the satellite's owner, had yet to file an application to move it.[19] "Scrambling," the satellite owner filed an application with the FCC's International Bureau for special temporary authority (STA) to move EchoStar6.[20] Under FCC regulations, STA applications are granted "only upon a finding that there are extraordinary circumstances requiring temporary operations in the public interest and that delay in the institution of these temporary operations would seriously prejudice the public interest."[21] The Netherlands' partner, Spectrum Five, filed an objection to the STA application because of the nation's interest in obtaining the orbital location at issue.[22]

---

8. Bermuda partnered with EchoStar Satellite Operating Corporation, whose satellite was subject to the United States' jurisdiction.

9. Bermuda sought to secure the orbital location 96.2º W.L.

10. *See Spectrum Five*, 785 F.3d at 257.

11. *See id.*

12. *See id.*

13. The Netherlands partnered with Spectrum Five, the Petitioner in this suit.

14. The Netherlands sought 95.15º W.L.

15. *See Spectrum Five*, 785 F.3d at 258.

16. *See id.*, at 256

17. *See id.*, 257-58.

18. *See id.*

19. *See id.*

20. *See id.*, at 258.

21. *See id.* (citing 47 C.F.R. § 25.120(b)(1)).

22. *See id.*

The International Bureau granted the STA request and the Netherlands' partner sought Commission-level review of the Bureau's determination, but the FCC upheld the Bureau's determination in its *STA Order*.[23] A few months later, the ITU determined that Bermuda had secured the rights to the orbital location at issue and recorded the new assignment in its Frequency Register.[24]

Spectrum Five then petitioned the Court for review of the FCC's decision; arguing that it was arbitrary and capricious.[25] They sought to have the Court vacate the *STA Order* and compel the FCC to take steps that Petitioner believes would lead the ITU to reverse its determination that Bermuda had secured the rights to the contested orbital location.[26]

II. ANALYSIS

In *Spectrum Five*, the Court considered a "redressability" challenge to Petitioner's Article III standing to obtain judicial review of the FCC's *STA Order*.[27] The specific question was whether, under the circumstances, Spectrum Five could demonstrate that vacating the *STA Order* would likely cause the ITU to reverse course and determine that Bermuda had not obtained a particular orbital location's rights.[28]

As the Court explained, Article III standing is an "irreducible constitutional minimum" fulfillment of which requires a party to show (1) an injury in fact, (2) that the challenged conduct caused that injury, and (3) "that a favorable decision on the merits will likely redress the injury.''[29] When that redress depends on the choices and actions of a third party, the burden is on the proponent "'to adduce facts showing that those choices have been or will be made in such manner as to . . . permit redressability of injury.'''[30] The Court noted that "[h]ere, the asserted injury is even one step further removed from the typical case in which redress depends on the independent

23. *See id.*, at 259 (citing EchoStar Satellite Operating Co. Application for Special Temporary Authority Related to Moving the EchoStar6 Satellite from the 77º W.L. Orbital Location to the 96.2º W.L. Orbital Location, and to Operate at the 96.2º W.L. Orbital Location, Memorandum Opinion & Order, FCC 13-93, 28 FCC Rcd 10412, para. 1 (2013)).

24. *See id.*, at 256, 259.

25. *See id.*, at 260.

26. *See id.*

27. *See id.*, at 256.

28. *See id.*, at 260.

29. *See id.* (citing U.S. Ecology, Inc. v. Dep't of Interior, 231 F.3d 20, 24 (D.C. Cir. 2000); Klamath Water Users Ass'n v. FERC, 543 F.3d 735, 738 (D.C. Cir. 2008)).

30. *See id.*, at 260-61 (citing *U.S. Ecology*, 231 F.3d at 24-25).

action of a third party not before the court, because the ITU is an international organization that is not regulated by our government and therefore not bound by this Court or the FCC."[31]

In response to the standing challenge, Petitioner argued that vacating the *STA Order* would revoke both the United States' consent to bring EchoStar6 into use at the contested orbital location and the domestic authority under which it operates, thereby "significantly" increasing the likelihood that the ITU will find that Bermuda never brought the orbital location into use.[32]

Petitioner first pointed to ITU space-station frequency-assignment regulations,[33] which provide that such assignments are "brought into use," when they have the "capability" of transmitting or receiving the assignment, and argued that the requisite "capability," requires "lawful domestic authority to operate."[34] But, as the Court explained, this reading: (a) is contrary to the ordinary meaning of "capability," which means "power or ability" and not "legal authority";[35] (b) "makes little sense," in the context of the ITU's regulatory framework;[36] and (c) finds no support in the ITU's published guidance on how to demonstrate a satellite's "capability."[37] Thus, Petitioners failed to establish that for a satellite to be "brought into use," the ITU requires the satellite to have domestic legal authority to transmit and receive signals.[38] Accordingly, the Court found it uncertain "at best" whether vacating the order, thereby revoking the satellite's domestic authority, would mean that the orbital location had never been brought into use.[39]

The Court explains, moreover, that "even if this [domestic-authority] uncertainty . . . does not, standing alone, render [Petitioner's] claim insufficiently likely of redress, it clearly does when considered in combination with other aspects of the ITU's decision making process."[40] First, the ITU appears to give administrations only 90 days to object when another nation uses a satellite licensed under its laws to bring an assignment into use, which, in this case, lapsed in 2013.[41]

---

31. *See id.*, at 261.
32. *See id.*, at 260.
33. *See id.*, at 261 (citing ITU Radio Regs., Art. 11.44 B).
34. *See id.* (quoting Petitioner's Brief at 33-34, 2013 WL 6139922 (Nov. 21, 2013)).
35. *See id.*
36. *See id.*, at 261-62.
37. *See id.*, at 262
38. *See id.*
39. *See id.*
40. *Id.*
41. *See id.*, at 263.

Even assuming, *arguendo*, that the ITU would not apply the 90-day rule under the circumstances, redress would still hinge on discretionary acts of two regulatory bodies.[42] A letter from the ITU indicates it would only: (a) upon receiving an objection from the FCC (b) initiate an investigation into Bermuda's filing.[43] First, vacating the *STA Order* would not require the FCC to file a *post hoc* objection with the ITU.[44] Second, even if the FCC *did* object, that would only trigger an investigation, after which the ITU "may reaffirm its initial determination, or it 'could' reach a different conclusion."[45] This would merely "put Spectrum Five back to square one: the ITU would reconsider its determination," which is insufficient to meet the burden of showing a "significantly increased likelihood" of redress.[46]

The Court also distinguished cases finding redress dependent on a third-party agency's action sufficiently likely by pointing to ITU's statement that "its decision will depend on its independent assessment, 'irrespective' of [the Court's] views."[47] Unlike those cases, in which "the ultimate decision by the third party (*domestic* agency) not before the court depended significantly—if not solely—upon [its] ruling," in this case the "Court would not have any impact on the ITU's reconsideration."[48]

The Court concluded its analysis by briefly explaining that four further steps Petitioner urged it to take would not cure its redressability problem.[49] The first three, essentially, would entail the Court "directing the FCC to inform the ITU that the [contested] filing was not brought into use," which would only lead to reconsideration of the filing, not an ITU reversal.[50] The remaining request, that the Court order the FCC to revoke its ratification of a coordination agreement essential to the assignment also fails, because nothing indicates that an "an out-of-time, post-hoc 'objection' by the FCC is likely to cause the ITU to" suppress the filing.[51] Thus, none of the proposed measures would make redress sufficiently likely to satisfy the requirements of Article III standing.

---

42. *See id.*, at 263-64.
43. *See id.*, at 263.
44. *See id.*
45. *Id.*
46. *Id.*, at 263-64.
47. *See id.*, at 264.
48. *Id.* (citing Ams. for Safe Access v. DEA, 706 F.3d 438, 440 (D.C. Cir. 2013); Town of Barnstable v. FAA, 659 F.3d 28, 31-32 (D.C. Cir. 2011)).
49. *See id.*, at 264-65.
50. *Id.*, at 265.
51. *See id.*

III. CONCLUSION

In sum, the Court held that Petitioners failed to show vacating the FCC's *STA Order* would significantly increase the likelihood that the ITU, a third-party not subject to the Court's jurisdiction, would suppress the contested filing.[52] The Court, accordingly, dismissed the *Spectrum Five* petition for want of Article III standing.[53]

52. *See id.*
53. *See id.*

ILLINOIS PUBLIC TELECOMMUNICATIONS ASSOCIATION V. FCC

752 F.3d 1018 (D.C. Cir. 2014)

In *Illinois Public Telecommunications Association v. FCC*,[1] the District of Columbia Circuit held that the FCC has congressionally-granted discretion to determine the remedies available for violations of the prohibition on Bell Operating Companies charging discriminatory rates to competitor payphone operators, and that the Commission reasonably exercised that discretion when leaving individual remedial determinations up to the states.[2]

I. BACKGROUND

With the Telecommunications Act of 1996, Congress amended the Communications Act of 1934 to add new Section 276, which "prohibit[s] Bell Operating Companies from subsidizing their own payphones or charging discriminatory rates to competitor payphone providers."[3] Congress intended the provision "to ensure fair competition in the payphone market" by prohibiting "Bell Operating Companies from exploiting their control over the local phone lines to discriminate against other payphone providers in the upstream payphone market."[4] Congress then delegated the duty of implementing the statute to the FCC and provided that the FCC's regulations would preempt any inconsistent state laws.[5]

Five years after the statute took effect, the FCC issued further guidance on the pricing standard that state regulatory commissions, tasked with applying Section 276 and the FCC's regulations, should use to determine the appropriate rate.[6] Subsequently, a number of states determined that the Bell Companies had been charging excessive rates, which must be reduced.[7] The Bell Companies did so, effectively granting prospective relief to affected competitors, but a

1. Ill. Pub. Telecomms. Ass'n v. FCC, 752 F.3d 1018 (D.C. Cir. 2014).
2. *Id.* at 1020.
3. *See id.* (citing 47 U.S.C. § 276 (2012)).
4. *See id.*
5. *See id.*
6. *See id.* at 1021.
7. *See id.*

group of independent payphone operators also sought refunds for overpayments dating back to the requirement's 1997 effective date.[8]

In response, states took different tacks.[9] The Illinois commission and courts found that the field-rate doctrine, prohibiting retroactive revisions to regulator-approved rates, barred the refunds.[10] In New York, the commission and courts had resisted awarding refunds, but left the question open pending the outcome of the instant case.[11] In Ohio the outcome was split, with the state commission granting partial refunds and state courts citing the field-rate doctrine and procedural grounds to deny them.[12] Dissatisfied, the independent payphone operators in these three states took their case to the FCC, asking it to clarify that Section 276 created an absolute entitlement to the requested refunds.[13] In response, the FCC issued a 2013 declaratory ruling (the *Refund Order*),[14] interpreting Section 276 to permit but not require states to issue refunds for periods of overpayment dating back to 1997.[15]

Still dissatisfied with this outcome, the Illinois Public Telecommunications Association, a trade association representing independent payphone operators in New York, Ohio, and Illinois, filed a petition for review in the District of Columbia Circuit.[16] The Petitioners asked the Court to decide "whether independent payphone providers who were charged excessive rates by Bell Operating Companies are entitled to refunds or instead are entitled only to prospective relief in the form of lower rates."[17]

8. *See id.*
9. *See id.*
10. *See id.*
11. *See id.* at 1021-22.
12. *See id.* at 1022.
13. *See id.*
14. *See id.* (citing Implementation of the Pay Tel. Reclassification & Comp. Provisions of the Telecomm. Act of 1996, Declaratory Ruling and Order, 28 FCC Rcd 2615, 2621 (2013)).
15. *See id.*
16. *See id.*
17. *Id.* at 1020.

II. ANALYSIS

Mounting an Administrative Procedure Act (APA) challenge to the *Refund Order*, the independent payphone operators challenge the *Refund Order* as ''arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.''[18] They advanced three grounds for overturning it, the Court rejected each in turn.[19]

A. Consistency with Language of Section 276(a)

The independent payphone operators first contend that the *Refund Order* is contrary to the language of the Section 276(a), which they read as unambiguously creating an absolute entitlement to refunds for the overpayments.[20] The Court, however, explained that "Section 276(a) does not say that refunds are required, or that refunds are not required, or anything at all about refunds"; in fact, it is silent as to a mechanism for enforcing its prohibitions.[21] Congress's silence on the issue of remedy is more meaningful in light of its proscription of remedies in other roughly contemporaneous amendments to the Communications Act of 1934 and the usual discretion afforded agencies to fashion remedies.[22] The Court, accordingly, held that Section 276(a) does not unambiguously proscribe any remedy for its violation concluded that it must uphold any reasonable FCC interpretation.[23]

B. Consistency with Language of Section 276(c)

Next, the independent payphone operators argued that the Refund Order is contrary to the text of Section 276(c), which provides that, where conflict exists, the FCC's payphone pricing regulations preempt state law.[24] First, the Court explained that this argument rests on a misreading of the *Refund Order*, which provides that states *may* order refunds but does not require them to do so.[25] Thus, denying a refund is not inconsistent with the regulations and would not be preempted under Section 276(c).[26]

---

18. *Id.* at 1022 (quoting 5 U.S.C. § 706(2)(A)).
19. *See id.* at 1020.
20. *See id.* (citing 47 U.S.C. § 276(a)).
21. *See id.* 1022-23.
22. *See id.*
23. *See id.*
24. *See id.* at 1023-24 (citing 47 U.S.C. § 276(c)).
25. *See id.* at 1024.
26. *See id.*

As a corollary of this argument, the independent payphone operators contend that relying on state's refund determinations constitutes an unlawful subdelegation.[27] The Court began by noting that "states do not require any subdelegation of authority from the FCC to adjudicate federal statutory claims," because our federal system already assigns them this power.[28] Moreover, the petitioner's true complaint is not about the state's ability to adjudicate these disputes at all but rather the FCC's refusal to overrule the states in specific instances. Finally, the Court distinguished this case from *United States Telecom Association v. FCC*,[29] the leading unlawful subdelegation case, explaining that Section 276 lacks mandatory language expressly directing that the FCC be the arbiter of specific refund disputes.[30]

Thus, the Court concluded, leaving the question of remedy for overpayment under Section 276 up to the states neither violated Section 276(c)'s preemption provision nor constituted an unlawful subdelegation of federal power.[31]

C. Reasonableness of the FCC's Interpretation

Having already determined that, because Section 276(a) is silent on the question of remedy, any reasonable FCC interpretation must be upheld, the Court turned to "whether the [FCC's] was arbitrary or capricious."[32] When resolving such questions, ''[a]lthough [an] enforcement regime chosen by the [FCC] may not be the only one possible, we must uphold it as long as it is a reasonable means of implementing the statutory requirements.''[33]

The Court first considered "[t]he independent payphone provider[']s contention] that the FCC's approach is arbitrary and capricious because it leads to refund determinations that vary from state to state."[34] After considering general principles of federalism, the Court concluded that "there is nothing inherently arbitrary or capricious about state-to-state variation . . . [or] the FCC's decision not to further exercise its preemptive power to dictate a uniform

27. *See id.*
28. *See id.*
29. U.S. Telecom Ass'n v. FCC, 359 F.3d 554 (D.C.Cir.2004).
30. *See Ill. Pub. Telecom. Ass'n*, 752 F.3d at 1024.
31. *See id.* at 1024.
32. *Id.*
33. *Id.* at 1024 (quoting Global Crossing Telecom., Inc. v. FCC, 259 F.3d 259, 745 (D.C. Cir. 2001)).
34. *Id.* at 1025.

national answer to the refund question," especially given the "cooperative federalism" used in parts of the Communications Act.[35]

Next the Court considered the independent payphone operators' particular objection to states' use of the field-rate doctrine.[36] The Court was unmoved, explaining that it could hardly be unreasonable or arbitrary to allow the use of a doctrine that "has long been 'a central tenet of telecommunications law.'"[37] Further, the doctrine is not an "insuperable barrier to refunds or otherwise negate the FCC's position that refunds are permitted in individual cases," pointing out that two states have granted refunds notwithstanding the field-rate doctrine.[38]

The Court concluded that neither the state-to-state variation in refund decisions nor states' application of the field-rate doctrine rendered the Refund Order arbitrary and capricious and that there is "nothing unreasonable about how the FCC filled the statutory gap and exercised its discretion."[39]

III. CONCLUSION

In sum, the Court first held that Section 276(a) does not unambiguously proscribe any remedy for its violation and that it must uphold any reasonable FCC interpretation.[40] Next, the Court concluded that the FCC's decision to leave remedial determinations for overpayment under Section 276 up to the states neither violated Section 276(c)'s preemption provision nor constituted an unlawful subdelegation of federal power.[41] Finally, the Court held that neither the state-to-state variation in refund decisions nor states' application of the field-rate doctrine rendered the *Refund Order* arbitrary and capricious and that there is "nothing unreasonable about how the FCC filled the statutory gap and exercised its discretion."[42]

35. *Id.*
36. *See id.*
37. *Id.* (quoting TON Services, Inc. v. Qwest Corp., 493 F.3d 1225, 1236 (10th Cir. 2007)).
38. *Id.* at 1025-26.
39. *Id.* at 1026.
40. *See id.* at 1023.
41. *See id.* at 1024.
42. *Id.* at 1026.

Data Privacy in Our Federalist System: Toward an Evaluative Framework for State Privacy Laws

Tony Glosson*

TABLE OF CONTENTS

**J.D., The George Washington University Law School, 2015; Associate, Drinker Biddle & Reath LLP.* *I would like to thank Matthew Gerst for his helpful guidance and encouragement; Berin Szoka for the conversations that sparked my interest in this topic; Stephan Satterfield for providing valuable feedback on my arguments; and Natalie Roisman and Ryan Wallach for showing me how much fun communications law can be.*

I. INTRODUCTION

In 2013, Target drew fire for mailing pregnancy-themed advertisements to a teenage girl who had not yet revealed her pregnancy to her parents.[1] Drawing from myriad data points including age, income, address, ethnicity, spending patterns, and more, Target's analytics algorithm identified the girl as likely to be pregnant.[2] In other words, Target knew before her parents did—ultimately forcing her hand in the timing of her announcement to her family.[3]

Even as privacy advocates increasingly express concern, the demand for consumer data is exploding. One industry study projects that consumer data collection—or colloquially, "big data"—will be a $16.9 billion industry in 2015, up from $3.2 billion in 2010.[4] Simultaneously, it is becoming cheaper to gather information. Consulting firm McKinsey & Co. has estimated a growth rate of roughly 40% in consumer data collected year over year, with a mere 5% corresponding increase in IT spending.[5] In fact, the growth in data collection may force major changes in technological infrastructure: according to some reports, over half of the surveyed C-level executives acknowledge that their infrastructure lacks the capacity to handle the demands of modern data collection.[6]

But the story does not end with the collection of traditional demographic data by previously disinterested players. Instead, wholly new data points emerge daily, each with its own set of privacy implications. The so-called Internet of Things—geek-speak for network connectivity built into traditionally "dumb" apparatus like refrigerators or thermostats—allows collection of personal data in the unlikeliest of places.[7]

---

1. Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 02, 2012), http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

2. *See id.*

3. Since this revelation, California lawmakers have introduced a ballot measure that would potentially provide tort damages for instances like this one where companies use consumer data in an unpredictable way without first obtaining the data subject's affirmative permission. *See* Cynthia Larose, *Will California Voters Move US to Opt-In?*, PRIVACY & SECURITY MATTERS (Aug. 6th, 2013), http://www.privacyandsecuritymatters.com/2013/08/3949/.

4. *Big Data Will Be a $16.9 Billion Market by 2015: IDC*, IDC (Mar. 09, 2012), http://www.cioinsight.com/c/a/Latest-News/Big-Data-Market-to-Grow-to-169-Billion-by-2015-IDC-118144/.

5. James Manyika et al., *Big Data: The Next Frontier For Innovation, Competition, And Productivity*, MCKINSEY GLOBAL INSTITUTE (May 2011), http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

6. *Is Big Data Producing Big Returns?*, AVANADE (June 2012), http://www.avanade.com/en-us/approach/research/pages/big-data.aspx.

7. Michael Chui et al., *The Internet of Things*, MCKINSEY GLOBAL INSTITUTE (Mar. 2010), http://www.mckinsey.com/insights/high_tech_telecoms_Internet/the_Internet_of_things; *see*

But what role should the law play in guarding privacy during the data revolution? More fundamentally, *whose* law should play *which* roles in our federalist system? The allocation of regulatory authority over data collection may be as consequential as the substantive regulations imposed.[8] On the one hand, technology firms view the prospect of a medley of fifty assorted state privacy regimes as economically unworkable, and have already begun to object that recent state laws are "impossible to implement" and "extremely burdensome for start-up [companies]." [9] These firms assert that, if data collection is to be regulated, it is the role of the federal government to implement a single, coherent set of laws that apply nationwide.[10] Some state attorneys general, meanwhile, argue that the federal government might not act as quickly or as sweepingly as they would like.[11]

This Note offers a constitutional framework for analyzing the distribution of regulatory authority over data privacy, and ultimately concludes that the Dormant Commerce Clause precludes most state data privacy legislation.[12]

A. Overview of Note

When assessing state data privacy law, the challenge is to apply traditional principles of federalism to a revolutionary industry. The academic literature in this emerging field is somewhat sparse. Nonetheless, established constitutional doctrines guide this inquiry and this Note proffers a methodical application of those principles to the growing body of state data privacy laws.

This Note begins by reviewing a seminal district court decision on state Internet regulation, *American Library Association v. Pataki*.[13] *Pataki*

---

also FTC Seeks Input on Privacy and Security Implications of the Internet of Things, FTC (Apr. 17, 2013), http://www.ftc.gov/news-events/press-releases/2013/04/ftc-seeks-input-privacy-and-security-implications-Internet-things.

8. In this regard, it is worth considering the implications for the national economy should individual states continue down the path of the European Union, which has enacted stringent data privacy regimes forbidding data transfers to nations with less demanding privacy laws. If certain states enact similar laws aimed at preventing data transfers to other states that do not have congruent privacy protections, it is not difficult to imagine, for example, a startup webmail company becoming trapped in California, unable to transfer its data to new servers in Texas if the latter state had fewer privacy protections.

9. Steven Harmon, *Silicon Valley tech firms win privacy bill battle*, MERCURY NEWS (May 3, 2013), http://www.mercurynews.com/ci_23160780/silicon-valley-tech-firms-win-privacy-bill-battle.

10. Jessica Meyer, *States Defend Turf from Feds on Data Breach Rules*, POLITICO (Feb. 19, 2014), http://www.politico.com/story/2014/02/states-defend-turf-from-feds-on-data-breach-rules-103647.html.

11. *See id.*

12. Importantly, this note does *not* argue that any particular privacy protection, or set of protections, are good or bad policy objectives. Rather, this note suggests that as a matter of constitutional law, those policy debates must transpire at the federal level.

13. American Library Ass'n v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997).

demonstrates how courts have traditionally applied the Dormant Commerce Clause doctrine in the Internet context. Next, the Note addresses the ways in which modern technology has altered the applicability of the *Pataki* analysis. Finally, this Note concludes that geolocation changes the Dormant Commerce Clause analysis, but leaves several problems with state data privacy laws unresolved.

It bears mention that there are a number of constitutional grounds on which an entity might challenge state Internet regulations. Although this Note focuses on one, the Dormant Commerce Clause, state Internet regulations may implicate constitutional doctrines like preemption and personal jurisdiction as well.

II. BACKGROUND

The federal government has enacted a number of laws regulating elements of Internet activity and commerce.[14] However, many of those laws deal with criminal concerns such as hacking or gambling, or particular sets of data such as health records or information about children. Unlike most European countries,[15] and the European Union as a whole,[16] the United States has not enacted an overarching set of data privacy standards.[17] Instead, the United States tends toward spot-regulation, targeting specific data privacy issues or high-risk industries.[18] The closest the United States has come to enacting a uniform standard is the Federal Trade Commission's ("FTC") authority to prosecute "unfair or deceptive" business acts or practices,[19] which the FTC has interpreted to include regulation of data protection practices.[20] Some states, perceiving a gap in privacy protections,

14. *See, e.g.*, Unlawful Internet Gambling Enforcement Act, 31 U.S.C. §§ 5361–5367 (2012); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012); Internet Tax Freedom Act, Public Law No. 105-277, Title XI (1998) (extended until Dec. 11, 2015).

15. *See, e.g.*, Germany's Federal Data Protection Act (Bundesdatenschutzgesetz), http://translate.google.com/translate?hl=en&prev=search&sl=de&u=http://www.bfdi.bund.de/SharedDocs/Publikationen/GesetzeVerordnungen/BDSG.pdf%3F__blob%3DpublicationFile&sandbox=0&usg=ALkJrhi0OuKjCszTXrsZgauQoKtf97Uziw; European Commission, *National data protection authorities*, EU JUSTICE (last visited May 05, 2015), http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm.

16. *See* Elizabeth Dwoskin, *EU Seeks to Tighten Data Privacy Laws*, WALL ST. J. (Mar. 10, 2015), http://blogs.wsj.com/digits/2015/03/10/eu-seeks-to-tighten-data-privacy-laws/.

17. Paul M. Schwartz, *The Eu-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966 (2013) [hereinafter Schwartz, *Eu-U.S. Privacy Collision*].

18. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, Aug. 21, 1996, 110 Stat. 1936.

19. *See* Federal Trade Commission Act, 15 U.S.C. § 45.

20. *See* Pl.'s Opp. Mot. Dismiss, *FTC v. Wyndham Worldwide Corp.*, 2012 WL 4766957 (D. Ariz.).

have passed their own privacy regulations.[21] For example, several states have enacted data breach disclosure obligations, which mandate that businesses inform their customers when private information may have been compromised in a data breach.[22] More aggressive examples include California's "Online Eraser" law, which requires websites to implement a mechanism for registered users who are minors to take down any embarrassing past posts,[23] and California's "Do Not Track" law, which requires website operators to explain how they respond to data collection opt-out signals sent by users' browsers.[24] This patchwork of state laws can be particularly onerous for Internet-based companies because, in addition to tracking the developments in fifty-one jurisdictions, they must also tailor their products to comply with sometimes-conflicting demands under state laws. These state laws also raise questions regarding the constitutional allocation of regulatory authority over the Internet.

Under the U.S. Constitution, state authority is limited by several provisions, including the so-called "Dormant Commerce Clause." The Commerce Clause grants to Congress the power "[t]o regulate commerce . . . among the several states . . . ."[25] Over time, the courts have recognized that this grant of federal power precludes the states from enacting regulations that unjustifiably burden interstate commerce.[26] Nevertheless, states retain a residuum of power by which they may regulate matters affecting their citizens' health and safety, even if those regulations have an incidental effect on interstate commerce.[27] Accordingly, the constitutional analysis of a state data privacy law examines whether the law's effects on interstate commerce adequately respect the sovereignty of the coequal states over their own economies.

21. *State Laws Related to Internet Privacy*, NAT'L CONF. OF STATE LEGISLATURES (Jan. 02, 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-Internet-privacy.aspx.

22. National Conference of State Legislatures, *Security Breach Notification Laws*, NCSL RESEARCH (last visited May 06, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

23. *See* S.B. 568, 2013-14 Sess. (Cal. 2013), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568.

24. *See* A.B. 370, 2013-14 Sess. (Cal. 2013), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB370.

25. *Id.* art. I, § 8, cl. 3.

26. City of Philadelphia v. New Jersey, 437 U.S. 617, 623 (1978)

27. Southern Pacific Co. v. Arizona. *ex rel.* Sullivan, 325 U.S. 761, 766 (1945).

III. THE DORMANT COMMERCE CLAUSE AND THE EARLY APPROACH TO THE INTERNET: *AMERICAN LIBRARY ASSOCIATION V. PATAKI*

American Library Association v. Pataki, decided in 1997, was one of the first cases to apply the Dormant Commerce Clause to a state Internet regulation.[28] Since that decision, three circuit courts have adopted the *Pataki* court's reasoning to invalidate other state legislation regulating the Internet.[29] In *Pataki*, the law at issue was a New York statute that prohibited transmitting obscene content to minors.[30] Because libraries often provide content through their websites that could be considered obscene, the American Library Association ("ALA") sued to enjoin New York from enforcing the law. The ALA explained that its members generally did not know the ages or locations of their website visitors, and were therefore concerned that they would need to censor content that was perfectly legal in other states to guard against prosecution under New York law.[31]

The court agreed, and issued an injunction.[32] Judge Preska began her analysis by noting that laws governing the Internet inherently regulate interstate commerce.[33] She observed that "Internet protocols were designed to ignore rather than document geographic location;"[34] that the Internet itself is an instrument of interstate commerce because it "serves as a conduit for transporting digitized goods;"[35] and that "the novelty of the technology should not obscure the fact that regulation of the Internet impels traditional Commerce Clause considerations."[36] Having established that Dormant Commerce Clause principles apply to Internet regulations, Judge Preska worked through three independent modes of Dormant Commerce Clause doctrine: (a) extraterritoriality; (b) *Pike* balancing; and (c) susceptibility to inconsistent regulations.[37]

28. *Pataki*, 969 F. Supp. 160 (1997).

29. *See, e.g.*, American Booksellers Foundation v. Dean, 342 F.3d 96 (2d Cir. 2003); American Civil Liberties Union v. Johnson, 194 F.3d 1149 (10th Cir. 1999); PSINet, Inc. v. Chapman, 362 F.3d 227 (4th Cir. 2004).

30. *See* N.Y. Penal Law § 235.20(6).

31. *Pataki*, 969 F. Supp. at 162.

32. *See id*.

33. *Id*.

34. *Id*. at 170.

35. *Id*. at 173.

36. *Id*.

37. *Id*.

A. *Extraterritoriality: New York's Law Was Invalid Because It Necessarily Governed Wholly Out-of-State Transactions.*

Extraterritoriality doctrine holds that a state law is invalid if it regulates transactions outside the borders of the regulating state.[38] Judge Preska invoked several Supreme Court extraterritoriality decisions to hold the New York law invalid, including *Healy v. The Beer Institute*[39] and *Southern Pacific Co. v. Arizona*.[40]

First, in *Healy v. Beer Institute*, the Court invalidated a Connecticut statute that required beer distributers to affirm that the prices they charged in Connecticut did not exceed those charged in neighboring states.[41] Though the distributors were free to charge whatever prices they wished in other states, the affirmation requirement for beer shipped to Connecticut effectively compelled the distributors to account for the Connecticut market when making price determinations for other states.[42] The Supreme Court invalidated the provision, noting that a law may violate the commerce clause "regardless of whether the statute's extraterritorial reach was intended by the legislature."[43] The inquiry, according to the *Healy* court, is simply "whether the practical effect of the regulation is to control conduct beyond the boundaries of the State."[44] Moreover, the Supreme Court reasoned, the analysis turns on "what effect would arise if not one, but many or every, State adopted similar legislation."[45] Under this analysis, the Connecticut statute was unconstitutional because distributors had to take Connecticut price law into account while engaging in wholly out-of-state liquor sales, thereby precluding them from setting promotional prices or taking full advantage of unique market conditions in neighboring states.[46]

Second, in *Southern Pacific Co. v. Arizona*, the Court held unconstitutional an Arizona train length limitation because, as a practical matter, it forced railroad companies to limit the length of their trains in every state on the rail line.[47] Although the statute purported to regulate only trains within Arizona's borders, the Court in that case reasoned that a law that made it economically infeasible to tailor compliance to the regulating state had the same practical effect as one that explicitly regulated conduct within other

38. Healy v. The Beer Institute, 491 U.S. 324 (1989).
39. *Id.*
40. Southern Pacific Co. v. Arizona, 325 U.S. 761 (1945).
41. *Healy*, 491 U.S. 324.
42. *Id.*
43. *Id.* at 336.
44. *Id.*
45. *Id.*
46. *Id.* at 338-40.
47. *Southern Pacific Co.*, 325 U.S. at 775.

states.[48] Accordingly, the Arizona statute was unconstitutional under the extraterritoriality mode of Dormant Commerce Clause analysis.[49]

Applying those concepts to the New York law, Judge Preska determined that the law contained the same constitutional defects as the Connecticut statute in *Healy* and the Arizona statute in *Southern Pacific*.[50] Because website administrators could not determine whether a user resided in New York or elsewhere, much less the user's age, it was impossible to spot-comply with New York's statute.[51] Citing testimony that the plaintiffs had restricted the content available on their website nationwide to comply with New York's statute, Judge Preska concluded that New York's law was an "encroachment upon the authority which the Constitution specifically confers upon the federal government and upon the sovereignty of New York's sister states."[52] Thus, the extraterritoriality analysis counseled in favor of granting the injunction.

B. Pike Balancing: New York's Law Was Unconstitutional Because It Substantially Chilled Interstate Commerce with Few Countervailing Local Benefits.

Judge Preska next moved to a second mode of Dormant Commerce Clause analysis, the *Pike* balancing test.[53] *Pike* balancing, derived from the Supreme Court's analysis in *Pike v. Bruce Church*, applies to state laws that indirectly regulate interstate commerce.[54] The difference between a direct regulation of interstate commerce and an indirect one is not always a bright line, but the inquiry centers on whether a regulation facially applies to out-of-state transactions.[55] The *Pike* analysis consists of two steps: first, the court must determine the legitimacy of the state interest in enforcing the law; and second, the court must weigh the burden that the law places on interstate commerce against its legitimate local benefit.[56]

---

48. *Id.* at 774-75.
49. *Id.* at 775.
50. *Pataki*, 969 F. Supp. at 176-77.
51. *Id.*
52. *Id.*
53. *Id.*
54. 397 U.S. 137, 142 (1970).
55. Brown-Forman Distillers Corp. v. New York State Liquor Auth., 476 U.S. 573, 578-79 (1986):

> This Court has adopted what amounts to a two-tiered approach to analyzing state economic regulation under the Commerce Clause. When a state statute directly regulates or discriminates against interstate commerce, or when its effect is to favor in-state economic interests over out-of-state interests, we have generally struck down the statute without further inquiry.

56. *Id.* at 579.

In evaluating the legitimacy of an asserted state interest, courts give the legislature wide latitude to determine the problems their constituents face, and the relative benefit of solving them.[57] Stating that "[i]t is evident beyond the need for elaboration that a State's interest in safeguarding the physical and psychological well-being of a minor is compelling," Judge Preska quickly determined that New York's prohibition on obscene-for-minors internet communications fell within the legitimate scope of state interest.[58]

New York's law, however, did not fare as well under *Pike*'s second prong: because the law could not possibly affect content originating from outside the United States, the local benefits were "not overwhelming."[59] Foreign obscene-for-minors content is just as readily accessible to New York children as United States content, the court noted.[60]

On the other hand, the burden on interstate commerce was "extreme."[61] Beyond the burden of removing content actually deemed illegal under the New York law, website administrators would likely be forced to "steer clear of the Act by a significant margin."[62] Unsure of whether a given set of content—say, a library's collection of artwork—would offend New York's community standards of obscenity for minors, a website administrator may decide not to host that content on its site, regardless of whether the artwork was, in fact, obscene for New York minors.[63] Judge Preska then reasoned that the modest local benefits could not outweigh the law's burden on interstate commerce.[64] Accordingly, New York's law failed under the *Pike* test as well as under the extraterritoriality analysis.[65]

C. Inconsistent Regulations: New York's Law Was Unconstitutional Because Permitting States to Govern the Internet Would Result in Interlocking Regulatory Schemes that Would Stifle Interstate Commerce.

Finally, Judge Preska turned to the probability that, were other states to enact similar laws, website administrators could be subjected to inconsistent regulatory schemes.[66] In *Southern Pacific Co. v. Arizona*, the

57. *Pike*, 397 U.S. at 148.
58. *Pataki*, 969 F. Supp. at 169 (*citing* New York v. Ferber, 458 U.S. 747, 756–57 (1982)).
59. *Id.* at 170.
60. *Id.*
61. *Id.* at 171.
62. *Id.* at 179.
63. *Id.* at 179.
64. *Id.*
65. *Id.* at 183.
66. *Id.*

Court was particularly concerned that differing state regimes would create confusion for train operators given the inherently interstate nature of their businesses, observing that, "[w]ith such laws in force in states which are interspersed with those having no limit on train lengths, the confusion and difficulty with which interstate operations would be burdened under the varied system of state regulation and the unsatisfied need for uniformity in such regulation, if any, are evident."[67] There was, of course, one way a railroad could comply with all such limits: by configuring all of its trains to meet the most stringent limit. The railroad in *Southern Pacific* was forced to resort to that strategy, causing the Supreme Court to note disapprovingly that the effect of Arizona's length limit was to regulate trains "all the way from Los Angeles to El Paso."[68] Similarly, in *Bibb v. Navajo Freight Lines*, the Court invalidated an Illinois statute that required trucks on its highways to use contoured mud guards.[69] In that case, different states had contradictory mud guard requirements, so truckers would have to carry multiple sets of mud guards to change out during trips through states with different standards.[70]

Importantly, in neither case was compliance with the differing state regulatory schemes *technically impossible*. Indeed, Judge Preska noted that "the truck driver or train engineer . . . can steer around Illinois or Arizona, or change the mudguard or train configuration at the state line."[71] Rather, in both decisions, the Supreme Court struck the regulations down because compliance would be *economically infeasible*. Specifically, both laws would have forced businesses operating primarily through the instruments of interstate commerce to track and comply with numerous sets of regulatory schemes—a tall order even for the relatively well-established freight businesses in those cases.[72]

Applying the rationale behind both these cases to the facts in *Pataki*, Judge Preska concluded that the New York law was also likely to be unconstitutional under the third mode of analysis because other states would enact different regulatory standards, forcing website administrators either to track developments in each state and comply with each individually, or else to comply with the most stringent across the board.[73] This predicament was substantially the same as the choice put to railroads in *Southern Pacific* and truckers in *Bibb*, and resulted in the same constitutional defects for the New York law.[74] Having determined that New York's obscenity-for-minors statute impermissibly burdened online interstate commerce under each of the

67. *Id.* at 181 (quoting *Southern Pacific Co.*, 325 U.S. at 773-74).
68. *Southern Pacific Co*., 325 U.S. at 774.
69. 359 U.S. 520 (1959).
70. *Id.* at 525.
71. *Pataki*, 969 F. Supp. at 183.
72. *Id.*
73. *Id.* at 181-82.
74. *Id.*

three proffered Dormant Commerce Clause analyses, Judge Preska preliminarily enjoined enforcement of the law.[75]

IV. GEOLOCATION TECHNOLOGY CHANGES THE DORMANT COMMERCE CLAUSE ANALYSIS, BUT NOT NECESSARILY THE RESULT

Pataki has since become a landmark case in Internet law.[76] It is not, however, without its weak points. For one, *Pataki*'s language, at times, seems to foreclose *any* state laws affecting the Internet,[77] although in the context of the Court's balancing analysis, that interpretation seems strained. One commentator suggests that the Court wrongly imported elements of First Amendment scrutiny into its Dormant Commerce Clause analysis by framing the law's burden in terms of its "chilling effect" on commerce.[78] But today, the most common critique is that dramatic improvements in geolocation capabilities—technologies that enable service providers to identify a user's location—have undermined the *Pataki* analysis.[79] This Section briefly overviews the state of modern geolocation technology, then walks through their implications for the *Pataki* analysis, and concludes that geolocation does not solve the Dormant Commerce Clause problems with many state data privacy laws.

Businesses use a variety of geolocation technologies today. Four of the most common are Internet protocol (IP) geolocation, WiFi network mapping, cell site geolocation, and GPS.[80] IP geolocation relies on Internet protocol addresses, the structural feature of the Internet that permits computers to identify and communicate with one another. Internet service providers (ISPs) obtain blocks of IP addresses that they then distribute to customers.[81] Thus, if one knows that a user's IP address is associated with an ISP located in

75. *Id.* at 183.

76. *See, e.g.*, ORIN S. KERR, COMPUTER CRIME LAW 697 (2013) (excerpting Pataki as the first case for state-based Internet regulations).

77. *Pataki*, 969 F. Supp. at 177 ("New York has deliberately imposed its legislation on the Internet and, by doing so, projected its law into other states whose citizens use the Net."). This criticism, however, seems to undervalue the *Pike* balancing analysis, which would permit some state internet regulations

78. James E. Gaylord, *State Regulatory Jurisdiction and the Internet: Letting the Dormant Commerce Clause Lie*, 52 VAND. L. REV. 1095, 1116 (1999) [hereinafter *State Regulatory Jurisdiction*].

79. *See, e.g.*, Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785 (2001) [hereinafter *The Internet*].

80. Marketa Trimble, *The Future of Cybertravel: Legal Implications of the Evasion of Geolocation*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 567, 594 (2012) [hereinafter *The Future of Cybertravel*]; Timothy J. Van Hal, *Taming the Golden Goose: Private Companies, Consumer Geolocation Data, and the Need for A Class Action Regime for Privacy Protection*, 15 VAND. J. ENT. & TECH. L. 713, 716 (2013) [hereinafter *Taming the Golden Goose*].

81. Trimble, *supra* note 110, at 594.

Illinois, that information supports a preliminary inference that the user is accessing the service from Illinois.

The second method, WiFi network mapping, is a relatively newer technology.[82] Companies that offer WiFi network mapping services collect data on the names of WiFi networks and their corresponding locational coordinates.[83] Once a company has compiled a sufficiently large database of WiFi networks, it can query a user's device for names of nearby WiFi networks, and compare the response to the database, establishing the device's location.[84] Cell site geolocation and GPS technologies can help determine the location of users accessing a website or application from a mobile device configured to permit disclosure of location data.[85]

The accuracy of these technologies is somewhat disputed.[86] However, most accept that, using some combination of the available technologies, geolocation accuracy is at least in the eighty percent range at the state level. Estimates run up to 99.9 percent accuracy on the high end.[87] Even if geolocation is insufficiently accurate for legal purposes at the present, the progress of technology may moot the accuracy debate in the relatively near future.[88] Still, location-masking tools will likely continue to advance as well, so no geolocation regime will be perfect in all situations.

A. Extraterritoriality: Geolocation Mandates Are On Constitutionally Questionably Ground Because They Directly Regulate Wholly Out-of-State Transactions

The advancement in technology has several implications for the analysis employed in *Pataki*. First, geolocation muddies the once

82. Van Hal, *supra* note 110, at 717.

83. *Id.* at 118

84. *Id.*

85. *Id.* at 716.

86. Trimble, *supra* note 110, at 598; *see also* Mahesh Balakrishnan, et al., *Where's That Phone?: Geolocating IP Addresses on 3G Networks*, 9 ACM SIGCOMM 294 (2009).

87. Kevin F. King, *Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies*, 21 ALB. L.J. SCI. & TECH. 61, 70 (2011) (citing PriceWaterhouseCoopers, Report of Independent Accountants: Quova. Inc., 3 (Oct. 23, 2008), http://www.quova.com/documents/PricewaterhouseCoopers_Audit.pdf) ("Today, leading geolocation technologies are up to 99.9% accurate at the country level and more than 97% accurate at the state level within the United States.") [hereinafter *Personal Jurisdiction*]; Kevin F. King, G*eolocation and Federalism on the Internet: Cutting Internet Gambling's Gordian Knot*, 11 COLUM. SCI. & TECH. L. REV. 41, 59 (2010) ("Experts have estimated accuracy rates of between 85 and 98 percent at the state level and over 99 percent at the national level.") [hereinafter *Geolocation and Federalism*]; *see also* Pioneer Military Lending, Inc. v. Dufauchard, CIV S061445 LKKPAN, 2006 WL 2053486 (E.D. Cal. 2006) (reciting a forensic expert's assessment that "the accuracy level of a 'state level' geolocation investigation is approximately 80% to 99% accurate"). Note that the latter assessment reflects the state of the technology over eight years ago.

88. *Cf.* Trimble, *supra* note 110.

straightforward extraterritoriality analysis. Unlike *Pike* balancing, which applies to laws governing commercial activity with *both* in-state and out-of-state elements, extraterritoriality doctrine is concerned with the possibility of *wholly out-of-state* application of state laws.[89] The *Pataki* court, in addressing extraterritoriality, relied heavily on the idea that "[a]n Internet user who posts a Web page cannot prevent New Yorkers or Oklahomans or Iowans from accessing that page and will not even know from what state visitors to that site hail."[90] As a result, *all* website administrators would need to comply with New York law during *all* transactions or risk liability in the case of the indistinguishable New York visitor. On this understanding, the *Pataki* court concluded that New York's regulation necessarily imposed its policy preferences on out-of-state transactions. In the Court's parlance, New York was *directly* regulating out-of-state commerce, as there was no way to isolate in-state commerce.[91] Under the extraterritoriality analysis, then, the law was *per se* invalid.

With the advent of geolocation technology, however, the question becomes more complex. Now it *is* often possible, at least in theory, to distinguish communications sent to devices in New York from those sent to devices in any other state. At this point, the extraterritoriality conversation undergoes an important shift: no longer is the analysis centered on the problems associated with identifying the jurisdiction in which a user resides; instead, firms have the option of implementing geolocation technologies, then blocking or tailoring their services on a state-by-state basis.

In many cases, firms would likely choose to comply with the most stringent state laws across the board, rather than incurring the expense of adopting geolocation technologies and tailoring their products accordingly. Consequently, the result from an end-user standpoint is indistinguishable from a *Pataki*-like regime in which the provider universally complies with one state's law because it cannot possibly know whether it governs a transaction. Either way, providers are choosing to apply the regulating state's law universally, even as they reach that decision for different reasons. From a *legal* standpoint, however, a court might decide that the technical possibility of tailoring content's availability based on geolocation is all that matters, even if that option is economically infeasible.

The analysis is further complicated by the fact that extraterritoriality doctrine is unsettled. As one commentator aptly noted: "[c]yberspace imbues state regulation with tremendous potential for extraterritorial effect, potential which invites the federal judiciary to cut down a broad swath of state law. This invitation is made all the more appealing by the rather amorphous nature

89. *See Brown-Forman Distillers Corp. v. New York State Liquor Auth*., 476 U.S. 573, 582 (1986).

90. *Pataki*, 969 F. Supp. at 171.

91. *Id.* at 177.

of the Supreme Court's extraterritoriality jurisprudence."[92] *Healy* provides perhaps the most complete judicial expression of extraterritoriality doctrine:

> Taken together, our cases concerning the extraterritorial effects of state economic regulation stand at a minimum for the following propositions: First, the Commerce Clause precludes the application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the State, and, specifically, a State may not adopt legislation that has the practical effect of establishing a scale of prices for use in other states. Second, a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature. The critical inquiry is whether the practical effect of the regulation is to control conduct beyond the boundaries of the State.[93]

The Court then continued:

> Third, the practical effect of the statute must be evaluated not only by considering the consequences of the statute itself, but also by considering how the challenged statute may interact with the legitimate regulatory regimes of other States and what effect would arise if not one, but many or every, State adopted similar legislation. Generally speaking, the Commerce Clause protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State.[94]

Initially, cases in which the cost of tailoring exceeds the cost of compliance appear to implicate that "practical effects" element of extraterritoriality doctrine. Clearly, should providers of online services overwhelmingly choose to comply with a state law across the board, one might conclude the "practical effects" of that state law have altered transactions outside the state's borders.

Nonetheless, a question exists as to whether the ability to block one's service from a particular state's market, rather than complying with that state's laws, takes state Internet-governance regimes out of the realm of *direct* commercial regulations to which extraterritoriality analysis pertains.

92. Gaylord, *supra* note 78, at 1097.
93. Healy v. Beer Institute, 491 U.S. 324, 336-37 (1989) (internal citations omitted).
94. *Id.*

After all, economies of scale provide a strong incentive to standardize products in *all* industries—not just online ones—and a great many state laws result in similar across-the-board compliance. [95] Are all such laws unconstitutional under the "practical effects" doctrine?

A closer look at the Supreme Court's "practical effects" cases suggests they are not. Specifically, the facts of those cases indicate that the Commerce Clause is concerned with laws that have the practical effect of subjecting wholly out-of-state transactions to *potential enforcement*—not merely those with which private parties choose to comply on an across-the-board basis for economic reasons. For example, in what some have called the "fount" of extraterritoriality jurisprudence,[96] *Edgar v. MITE Corp*., the Supreme Court struck down an Illinois corporate takeover law that governed any offers for firms in which "any two of the following three conditions are met: the corporation has its principal executive office in Illinois, is organized under the laws of Illinois, or has at least 10% of its stated capital and paid-in surplus represented within the State."[97] As *Pataki* noted, "[i]n striking the law as violative of the Commerce Clause, the [*Edgar*] Court found particularly egregious the fact that the Illinois law on its face would apply to a transaction that would not affect a single Illinois shareholder if a corporation fit within the definition of a 'target company.'"[98] Thus, the important "practical effect" was the law's enforceability against out-of-state transactions.

Similarly, in *Healy*, Connecticut could not possibly apply its price affirmation statute to liquor sellers without projecting its law into neighboring states.[99] By enforcing it at all, Connecticut threatened to penalize liquor sellers specifically on the basis of the terms of transactions occurring wholly outside of Connecticut borders.[100] Again, in *Brown-Forman Distillers v. New York*, the Court struck down a liquor price scheduling law that would have penalized sellers that provided lower-than-scheduled prices in other states without simultaneously lowering the New

95. For a discussion on a similar effect resulting from a California tobacco labeling law, *see* Lorillard Tobacco Co. v. Reilly, 84 F. Supp. 2d 180, 199-200 (D. Mass. 2000) *aff'd in part, rev'd in part sub nom.* Consol. Cigar Corp. v. Reilly, 218 F.3d 30 (1st Cir. 2000) *aff'd in part, rev'd in part sub nom.* Lorillard Tobacco Co. v. Reilly, 533 U.S. 525 (2001) ("In support of their argument that the cigar market requires uniform national regulation, the Cigar Companies point out that a regulation by California requiring a warning on all cigars has resulted in those California warnings appearing on 90% of all cigar packages in the United States and that the addition of other warnings from other states will result in multiple warnings on the same packaging . . . Those business decisions do not take a market of recreational consumer goods typically sold in local stores and automatically turn that market into one requiring national uniformity in regulation. The Cigar Warnings are not invalid on the basis of Southern Pacific or its progeny.")

96. *See* Goldsmith, *supra* note 109, at 805.

97. Edgar v. MITE Corp., 457 U.S. 624, 627 (1982).

98. *Pataki*, 969 F. Supp. at 174.

99. Healy v. The Beer Institute, 491 U.S. 324 (1989).

100. *Id.*

York price.[101] Because that law had the "practical effect" of regulating prices outside New York, it was invalid under the Commerce Clause.[102]

Before geolocation technology, state Internet regulations suffered from the same constitutional defect. A state could not enforce such laws without projecting them onto transactions in all other states; as one circuit court explained, "because there was no effective way to limit access to online materials by geographic location, a Web site owner operating legally in California would have to comply with New York's law to avoid being subject to liability there."[103] In each of these cases, the troublesome practical effects were the necessary extraterritorial results of the statute's application, *not* mere economic choices by private actors that could have complied within the regulating state wholly independent of their transactions in other states.

Geolocation technologies, therefore, appear to remove from state Internet regulations many of the unconstitutional practical effects on out-of-state commerce. However, those state laws still require that *all* providers implement geolocation technologies in the first place—a mandate that itself looks a lot like direct regulation of extraterritorial conduct, because out-of-state providers of Internet services must utilize the geolocation during transactions with out-of-state consumers in order to distinguish them from in-state ones. Whether this initial geolocation requirement is within a state's constitutional authority will likely depend on the way courts conceptualize extraterritoriality doctrine.

On the one hand, no matter how relatively easy or difficult implementing geolocation may be, *any* direct regulation of conduct occurring outside a state's borders seems to violate extraterritoriality principles. As the *Edgar* Court put it, extraterritoriality doctrine "precludes the application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the State."[104] From this unqualified language, a state law that enacts a nationwide geolocation mandate appears to be unconstitutional irrespective of the relative difficulty of implementing geolocation because such a law necessarily applies to wholly out-of-state transactions.

On the other hand, some commentators doubt that extraterritoriality doctrine is a complete bar to laws with wholly extraterritorial potential applications. For example, in their Yale Law Journal piece, *The Internet and the Dormant Commerce Clause*, Jack L. Goldsmith and Alan O. Sykes argue that the Supreme Court's extraterritoriality jurisprudence should be viewed as a balancing analysis.[105] On this view, state regulations that result in extraterritorial application of laws are valid unless they impose "a significant

101. 476 U.S. 573 (1986).

102. *Id.*

103. PSINet, Inc. v. Chapman, 362 F.3d 227, 239 (4th Cir. 2004) (citing *Pataki*, 969 F. Supp. at 64).

104. Edgar v. MITE Corp., 457 U.S. 624, 642-43 (1982).

105. Goldsmith, *supra* note 109, at 805.

out-of-state burden on communications between noncitizens [that is] not justified by the meager benefits achieved."[106]

Others are persuaded of extraterritoriality doctrine's demise, viewing a string of recent Supreme Court decisions that avoided extraterritoriality principles as the proverbial writing on the wall for extraterritoriality analysis.[107] In particular, Professor Brannon P. Denning has gone so far as to compose a "post-mortem" for extraterritoriality that purports to chronicle "the lifecycle of constitutional doctrine, from birth to death."[108] Citing to Goldsmith and Sykes' work, Denning argues that extraterritoriality is a poorly-defined and ultimately unworkable doctrine—particularly as it relates to state Internet laws.[109] Similarly, another commentator has predicted that "extraterritoriality analysis of Internet matters will have a brief lifetime under the Dormant Commerce Clause," suggesting that "[j]ust as *ALA v. Pataki* coupled a simple analogy to transportation with broad pronouncements of state incompetence to regulate the Internet, so too did the early [Dormant Commerce Clause] telegraph cases. But the Supreme Court eventually retrenched its analogy in the telegraph context to accommodate state regulatory interests."[110]

Nonetheless, even as some courts reject extraterritoriality analysis in the Internet context, others continue to accept the *Pataki* approach. All things considered, extraterritoriality concerns are worth exploring in challenges to state Internet laws, but judicial receptiveness to that argument has been haphazard at best. To maximize chances of success, an extraterritoriality challenge might include two specific arguments.

First, the challenge might explore the ambiguity in the "practical effects" cases by suggesting that regulations are invalid if the cost of tailoring greatly exceeds the cost of compliance. Consider that in *Southern Pacific*, the Supreme Court characterized the *economic infeasibility* of tailoring one's compliance on state-by-state basis as an invalid practical effect of Arizona's law:

> Frequently it is not feasible to operate a newly assembled train from the New Mexico yard nearest to Arizona, with the result that the Arizona limitation governs the flow of traffic as far east as El Paso, Texas. For similar reasons the Arizona law often controls the length of passenger trains all the way from Los

106. *Id.*

107. Brannon P. Denning, *Extraterritoriality and the Dormant Commerce Clause: A Doctrinal Post-Mortem*, 73 LA. L. REV. 979 (2013). For support, Denning offers State Farm Mutual Automobile Insurance Company v. Campbell, 538 U.S. 408 (2003), along with Phillip Morris, U.S.A. v. Williams 549 U.S. 346 (2007). Both cases employed Due Process, rather than extraterritoriality, as the appropriate analysis in cases seemingly ripe for extraterritoriality analysis.

108. *Id.* at 184.

109. *Id.*

110. Gaylord, *supra* note 108, at 1117.

> Angeles to El Paso. If one state may regulate train lengths, so may all the others, and they need not prescribe the same maximum limitation. The practical effect of such regulation is to control train operations beyond the boundaries of the state exacting it because of the necessity of breaking up and reassembling long trains at the nearest terminal points before entering and after leaving the regulating state.[111]

Likewise, it may be economically infeasible for providers to implement differential treatment of web traffic based on geolocation data, and a challenge to a law enacting such a mandate might argue that its practical effect is therefore to control the provider's behavior in all states, rendering the law unconstitutional. At least one federal court has recently adopted this approach in the privacy context. In evaluating a state requirement that businesses disclose when they record customer support calls, the court reasoned that the dispositive issue was "whether [the defendant] could feasibly comply with California law without altering its conduct with regard to non-California clients."[112]

Secondly, an extraterritoriality challenge to a state Internet law might attack the mandate that providers in all states implement geolocation technology for all interactions to identify the users subject to the state's law. Unlike laws that have extraterritorial effects only because of a business' economic decision to comply across the board, a geolocation mandate *does* directly regulate wholly extraterritorial conduct by threatening potential liability for out-of-state providers—even if most interactions in which those providers engage involve out-of-state users. If the court takes a stringent view of extraterritoriality doctrine that regards as invalid *any* direct regulation of transactions wholly outside state borders, geolocation mandates may well be unconstitutional.

Ultimately, given the wide divergence between courts, predictions as to the application of extraterritoriality analysis to a given Internet regulation are largely speculative. It is, therefore, likely that the Dormant Commerce Clause's other facets will supply the more consistently promising grounds for constitutional challenges to state Internet regulations—particularly in the data privacy context.

B. Pike Balancing: Common State Data Privacy Laws Are Unconstitutional Because Their Underwhelming Local Benefits Cannot Justify the Burden of Location-Based User Filtering.

Pike balancing represents a more fertile ground for Dormant Commerce Clause challenges because the doctrine is more settled than extraterritoriality, so potential plaintiffs can get a better idea of a court's likely reaction to such challenges. In evaluating the implications of

111. *Southern Pacific Co.*, 325 U.S. at 775-76.

112. Ades v. Omni Hotels Mgmt. Corp., 46 F. Supp. 3d 999, 1015-16 (C.D. Cal. 2014).

geolocation for *Pike* balancing, the particular state interest asserted becomes especially important; indeed, *Pike* balancing explicitly evaluates that state interest in the first step of the analysis.[113] Accordingly, a generic category of "state Internet regulations" is insufficient to inform the *Pike* inquiry because the state interests at issue may vary dramatically.

This Section will focus on the state interest in protecting general data privacy, particularly with regard to data commonly considered "personally identifiable information," or PII.[114] As yet, there is little jurisprudence regarding the state interest in data privacy under the Dormant Commerce Clause analysis.[115] This Section attempts to provide a framework for evaluating that interest in a *Pike* balancing context.

To begin, consider how other asserted state interests have fared under *Pike*. The first, and easiest, hurdle that a challenged regulation must clear is that the asserted state interest must be a legitimate matter of local concern.[116] In the realm of Internet commerce, federal courts have weighed the states' interests in protecting children from obscenity;[117] in regulating online pharmacies;[118] in controlling the terms of online sales and online loans to resident consumers; [119] and in dictating website audible accessibility standards.[120] Additionally, state courts have addressed the state's interest in restricting online gambling.[121] Each time, the court accepted the asserted interest as a legitimate one without prolonged analysis.

Perhaps the closest courts have come to evaluating the legitimacy of a state's interest in data privacy is a string of cases addressing state regulation

113. *Pike*, 397 U.S. at 145.

114. There is no universally accepted definition of PII, but generally, any information that might reasonably be associated with a specific person or small group of people qualifies as PII.

115. *See, e.g.*, King, *supra* note 117, at 63 ("[T]he law has reacted inadequately to [geolocation] technologies, or in some cases, failed to react at all. While these failings are widespread, they are most glaring in three particular areas: personal jurisdiction, Internet commerce regulation, and privacy law."). Moreover, states may have stronger interest in preserving their citizens' data privacy in some areas, such as health information, than in others, like shopping habits.

116. *Pike*, 397 U.S. at 142 ("Where the statute regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits.").

117. *See, e.g.*, *Pataki*, 969 F. Supp. at 163; Am. Booksellers Found. v. Dean, 342 F.3d 96, 103 (2d Cir. 2003); PSINet, Inc. v. Chapman, 362 F.3d 227, 240 (4th Cir. 2004); Am. Civil Liberties Union v. Johnson, 194 F.3d 1149, 1161 (10th Cir. 1999); Cyberspace Commc'ns, Inc. v. Engler, 55 F. Supp. 2d 737, 751 (E.D. Mich. 1999), *aff'd & remanded*, 238 F.3d 420 (6th Cir. 2000).

118. Knoll Pharm. Co. v. Sherman, 57 F. Supp. 2d 615, 623 (N.D. Ill. 1999).

119. *See, e.g.*, Ford Motor Co. v. Texas Dep't of Transp., 264 F.3d 493, 500 (5th Cir. 2001); Quik Payday, Inc. v. Stork, 549 F.3d 1302, 1305 (10th Cir. 2008).

120. Nat'l Fed'n of the Blind v. Target Corp., 452 F. Supp. 2d 946, 958 (N.D. Cal. 2006).

121. Rousso v. State, 170 Wash. 2d 70, 82, 239 P.3d 1084, 1090 (2010).

of unsolicited commercial emails ("spam").[122] There too, a federal court accepted that "the Act served the 'legitimate local purpose' of banning the cost-shifting inherent in the sending of deceptive spam."[123] Although the concerns addressed by anti-spam laws—like fraud and annoyance—are different from those inherent in data privacy, there also exist conceptual similarities: the desire for anonymity in consumption, the "right to be let alone,"[124] and the ability to exclude unwanted kinds of correspondence.[125]

Taken together, these cases suggest that courts give state legislatures wide latitude in evaluating the legitimacy of asserted interests. In any event, it seems improbable that a state interest in the data privacy is substantially less legitimate than curtailing unsolicited emails or ensuring audible accessibility for websites. Accordingly, for *Pike* balancing purposes, a state's interest in data privacy will likely be a legitimate one.

However, that does not end the judicial evaluation of a state interest under *Pike*. After ascertaining that a state interest is legitimate, courts must then weigh the gravity of that legitimate interest against the burden thereby imposed on interstate commerce.[126] The common theme at this stage in Internet cases, which could factor prominently in a challenge to a state data privacy law, is that the real weight of a state interest appears to depend less on its importance as a societal goal than on its likelihood of being achieved through the challenged regulation.

Thus, in *PSINet, Inc. v. Chapman*[127] and *American Civil Liberties Union v. Johnson*[128] the Fourth and Tenth Circuits struck down statutes criminalizing transmission of obscene-for-minors material to minors. Even if courts permitted states to apply such statutes against out-of-state actors within the United States, the Tenth Circuit reasoned, "[p]ornography from, say, Amsterdam will be no less appealing to a child on the Internet than pornography from [Albuquerque], and residents of Amsterdam have little incentive to comply with [the statute]."[129] Those courts concluded that the regulation would fail significantly to affect the availability of such materials

---

122. *See* Beyond Sys., Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523, 535 (D. Md. 2006); State v. Heckel, 143 Wash. 2d 824, 840 (2001); MaryCLE, LLC v. First Choice Internet, Inc., 166 Md. App. 481, 519 (2006). *See also* Free Speech Coal., Inc. v. Shurtleff, 2:05CV949DAK, 2007 WL 922247 (D. Utah 2007). *Shurtleff*, however, is of limited use for data privacy purposes because the statute at issue permitted the court to evaluate the state interest as protecting minors from obscenity, not merely protecting some form of inbox privacy.

123. *Keynetics*, 422 F. Supp. 2d at 534 (quoting *Heckel*, 143 Wash. 2d at 836).

124. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

125. One might consider the protections embodied in the "Do-not-call" registry, at 47 C.F.R. § 64.1200, as expressions of this ability.

126. *Pike*, 397 U.S. at 143-44.

127. *PSINet*, 362 F.3d 227 (4th Cir. 2004).

128. *Johnson*, 194 F.3d 1149 (10th Cir. 1999).

129. *Id.* at 1162 (quoting ACLU v. Reno, 929 F.Supp. 824, 882 (E.D.Pa.1996), *aff'd*, 521 U.S. 844 (1997) (second and third alterations in the original)).

to minors within the regulating state. The state interest in its enforcement was, therefore, *de minimis*.

By contrast, in *Ford Motor Co. v. Texas*,[130] the Fifth Circuit upheld the application of Texas' ban on manufacturer-owned auto dealerships to Ford's online used vehicle market. In that case, the state's interest was "to prevent vertically integrated companies from taking advantage of their incongruous market position."[131] Noting that Ford had previously unloaded its used vehicles through closed auctions to dealers before discontinuing the practice in order to sell them through its own online dealership, the court concluded that "there is certainly evidence from which a reasonable legislator could believe [the statute] would further the State's legitimate interest in preventing manufacturers from utilizing their superior market position to compete against dealers."[132] That is, unlike harmful-to-minors content originating from overseas sources beyond any state's control, Texas is quite capable of enforcing its economic favoritism for cars bought and sold within its own boundaries. Accordingly, despite the initially strange result that statutes enacted for the protection of minors were invalidated, while others supported only by economic protectionism were upheld, the probable efficacy of a state's law in addressing its asserted interest would explain these outcomes.[133]

The implications for data privacy laws are significant. Consider a hypothetical law that would create a presumption of harm if a defendant shares personal information without obtaining the data subject's prior opt-in.[134] The law would allow consumers to bring actions against businesses that transfer such data without consumer consent.[135] While a state may be able to enforce such a law against domestic firms, under current Dormant Commerce Clause jurisprudence, the ubiquitous collection and sale of such information among foreign providers of websites and applications may preclude the state from actually achieving its interest in protecting its citizens' privacy.

---

130. Ford Motor Co. v. Texas Dep't of Transp., 264 F.3d 493 (5th Cir. 2001).

131. *Id.* at 503.

132. *Id.* at 504.

133. *See also* Greater Los Angeles Agency on Deafness, Inc. v. CNN, Inc., 742 F.3d 414 (9th Cir. 2014) (upholding against summary judgment a California statute mandating video closed captioning). Although the analysis is exceedingly brief, the result is informative as an illustration: presumably, California's interest in "providing hearing-impaired citizens equal access to online news videos," *Id.* at 433, is likely to be substantially realized through domestic enforcement alone, given consumers' relatively greater demand for United States news compared to foreign news.

134. *See* Julian D. Perlman, *Opening The Flood Gates? California Voters May Create Presumption Of Harm In Privacy Breach Cases*, MONDAQ (Oct. 2013), http://www.mondaq.com/unitedstates/x/266604/Data+Protection+Privacy/Opening+The+Flood+Gates+California+Voters+May+Create+Presumption+Of+Harm+In+Privacy+Breach+Cases.

135. *Id.*

Against that underwhelming state interest, courts must weigh the burden a challenged law places on interstate commerce.[136] Several commentators suggest that modern geolocation capabilities lower the burden that state laws place on interstate commerce by enabling them to block citizens of states in which they do not wish to do business,[137] although precedent supportive of this proposition remains sparse.[138] Even so, commentators have observed that "server-side geolocation tools cost thousands of dollars per year and client-side tools still involve non-trivial implementation costs as well."[139] Those expenses may dissuade companies from launching new online services.[140]

Alternatively, a court might conceptualize the burden as the actual cost of bringing a website into compliance—even if geolocation makes it technically possible to block a given jurisdiction. Consider that the statutes in *Bibb* and *Southern Pacific Co.* were both invalid even though "the truck driver or train engineer . . . can steer around Illinois or Arizona, or change the mudguard or train configuration at the state line . . . ."[141] On this view, the burden will likely vary depending on the challenged statute. For example, in the case of data breach notification laws, the burden is (among other things) the cost of contacting all affected parties. Similarly, in the case of California's Online Eraser law, the burden consists of devising a mechanism by which minors may completely remove previous posts from public view.

Along with the technological burden of any given state law—however a court conceptualizes it—comes the additional burden of potentially inconsistent regulations from other states.[142] *Pataki* analyzed the law's

136. *Pike*, 397 U.S. at 143.

137. *See, e.g.*, Goldsmith, *supra* note 109, at 808; Michael W. Loudenslager, *Allowing Another Policeman on the Information Superhighway: State Interests and Federalism on the Internet in the Face of the dormant commerce clause*, 17 BYU J. PUB. L. 191, 243 (2003).

138. To date, the only federal court opinions to have directly addressed the burden associated with implementing geolocation technology as it relates to *Pike* balancing are *Target*, 452 F. Supp. 2d at 962; and *CNN*, 742 F.3d at 433. Both courts reasoned that, because major companies sometimes integrate national-level geolocation technology into their websites, geolocation at the state level must not be a burden. It is unclear whether courts would be as dismissive of the burden if presented by a smaller company, nonprofit, or sole proprietor. Additionally, both cases were decided at pre-trial stages obligating the courts to draw inferences in the plaintiffs' favor. For further analysis, see King, *Personal Jurisdiction*, 21 ALB. L.J. SCI. & TECH. at 91. King acknowledges the possibility that, for *Pike* balancing purposes, some geolocation mandates may be unconstitutionally "disruptive or onerous." *Id.* at 115.

139. *Id.* at 110.

140. *Id.* at 96 ("In theory geolocation tools are available to every Internet site. In practice, however, only some sites can realistically afford to employ them.").

141. *Pataki*, 969 F. Supp. at 183 (citing Bibb, 359 U.S. 520; and Southern Pac. Co., 325 U.S. 761).

142. Goldsmith, *supra* note 109, at 806 ("The inconsistent-regulations cases do not concern inconsistencies in the sense that acts required in one state are prohibited in another. Rather, they concern different regulations across states that heighten compliance costs for multijurisdictional firms.").

susceptibility to inconsistent regulatory schemes as a separate mode of Dormant Commerce Clause analysis, but it is probably best viewed as part of the burden on interstate commerce for Pike balancing purposes. [143] Recall that "the statute must be evaluated not only by considering the consequences of the statute itself, but also by considering how the challenged statute may interact with the legitimate regulatory regimes of other States."[144] In the data privacy sphere, this is a very real concern; for example, some states may require that businesses destroy data that is no longer in use, while others could require them to save the same records for law enforcement purposes.

Thus, there are several key arguments that a challenge to a state privacy law might include with respect to *Pike* balancing. First, the challenge might evaluate the law's prospects for successfully implementing the state's asserted interest, especially considering any unreachable foreign contributions to the putative problem. Second, the challenge might argue that implementing geolocation is itself a substantial burden—many times a prohibitively costly one. Third, the challenge might detail the possibilities for inconsistent regulations, highlighting the frequency with which data changes physical location in the modern economy. Important principles that might inform these analyses include the presence or absence of sales of physical goods within the state[145] and the relative burden to collect information, including whether a provider presently collects location information.[146] The more burdensome a state data privacy regulation, the more vulnerable it will be to the *Pike* test.

V. CONCLUSION

State data privacy laws currently face significant constitutional hurdles. Geolocation technology may alter the Dormant Commerce Clause analysis, but it is unlikely to mitigate the constitutional difficulties in all, or even most, cases. Challenges to modern data privacy laws, therefore, have

143. Gaylord, *supra* note 108, at 1116 ("The court's third mode of analysis, the potential for inconsistent regulation, is not an independent constitutional test. Rather, it represents "double-dipping" in the Commerce Clause pot."); William Lee Biddle, *State Regulation of the Internet: Where Does the Balance of Federalist Power Lie?*, 37 CAL. W. L. REV. 161, 167 (2000) ("As has been noted by other commentators, these first two reasons given by the court actually represent "double dipping" from the same line of Commerce Clause cases.").

144. *Healy*, 491 U.S. at 336-37.

145. *Compare Target*, 452 F. Supp. 2d 946 and *Ford*, 264 F.3d 493 (upholding challenged laws involving sales of physical goods), *with*, *PSINet*, 362 F.3d 227 and *Johnson*, 194 F.3d 1149 (striking challenged laws involving commerce in digital goods).

146. *Target*, 452 F. Supp. 2d at 961 ("Websites can determine the location of a user from information they provide, such as a credit card number . . . ."). *See also* Michael W. Loudenslager, *Allowing Another Policeman on the Information Superhighway: State Interests and Federalism on the Internet in the Face of the Dormant Commerce Clause*, 17 BYU J. PUB. L. 191, 245 (2003) ("Web sites on which users may download software or receive information or services, such as legal advice or other professional services, do not have the same opportunity to verify the location of the site user . . . .").

several lines of attack at their disposal. Among those arguments are extraterritoriality analyses, focusing on the practical economic effects of the law in question as well as its implicit geolocation mandate. Also available are *Pike* balancing arguments, including the likelihood that a law will achieve the asserted state interest, the costs of implementing unwanted geolocation technology, and the potential for inconsistent state regulations. At bottom, data privacy laws affect far more commerce than any obscenity statute or car dealership regulation ever has because privacy laws impact businesses of all shapes and sizes. Thus, the Dormant Commerce Clause likely has a significant role to play in protecting state comity in this important sector.

Cross-Border Commerce without Constraint: Shifting from Territorial-Based Regulation to an Industry-Based Code of Conduct for the Online Payment Processing Industry*

Anna Myers**

TABLE OF CONTENTS

*****This note was submitted for publication on April 8, 2014. The Asian-Pacific Economic Commission (APEC) finalized a certification scheme for information processors during August 2015. The scheme, APEC Privacy Recognition for Processors (PRP) is corollary to APEC's Cross-Border Privacy Rules (CPBR), for more information visit the CPBR website, http://www.cbprs.org/. *See* APEC Privacy Recognition for Processors Ready for Implementation, Hunton Privacy Blog (Sept. 8, 2015), https://www.huntonprivacyblog.com/2015/09/08/apec-privacy-recognition-processors-ready-implementation/.

******J.D., The George Washington University Law School, 2015; B.A. in Rhetoric and Media Studies, Willamette University. The author would like to thank her life-long mentor, Dr. Mary Jo Myers, M.D.

I. OVERVIEW

News of a data breach[1] during the last shopping days of the year can be devastating for a company. Target announced a massive data breach on December 19, 2013 that compromised up to 40 million customers' payment information from purchases made between November 27 and December 15, 2013.[2] Reports of similar data breaches at other U.S. retailers, such as at Neiman Marcus and Michaels Stores, continued to make headlines into the New Year.[3] Breaches like these are not easy to recover from, financially and otherwise, costing banks the credit and debit card replacements, costing consumers their personal information, and costing the breached businesses the resulting damages, including their customers' trust. It is no wonder Target offered 20% off at their brick-and-mortar stores to salvage what holiday sales they could in the wake of their breach.

When only one company suffers a breach it may be because that company somehow failed to follow industry best practices for data security.[4] However when large U.S. retailers are falling victim to breaches one after

1. A data breach occurs when sensitive, protected, or confidential information is accessed by a hacker or disclosed through an error by the company or agency storing the information. Definition: Data Breach, TECHTARGET.COM, http://searchsecurity.techtarget.com/definition/data-breach (last updated May 2010).

2. Melanie Eversley & Kim Hjelmgaard, *Target Confirms Massive Credit-Card Data Breach*, USA TODAY, Dec. 19, 2013, http://www.usatoday.com/story/news/nation/2013/12/18/secret-service-target-data-breach/4119337/.

3. *See* Elizabeth A. Harris et al. , *Neiman Marcus Data Breach Worse Than First Said*, NEW YORK TIMES, Jan. 23, 2014, http://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html; Nicole Perlroth, *Michaels Stores Is Investigating Data Breach*, NEW YORK TIMES, Jan. 25, 2014, http://www.nytimes.com/2014/01/26/technology/michaels-stores-is-investigating-data-breach.html.

4 . Additionally companies may be subject to compulsion by the United States Government to share the information they store. The USA PATRIOT Act and Foreign Intelligence Surveillance Act (FISA), under the premise of preventing espionage or terrorism, allows the United States Government to engage in warrantless, domestic surveillance programs and to order telecom and Internet companies to provide data in relation to national security investigations. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001); *see also* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511 92 Stat. 1783 (1978) [hereinafter *FISA*]. Without the protection of an Anti-hacking bill, companies are required to share the information they hold on their users with the government while also being accountable to their users for sharing that information; an Anti-Hacking Bill designed to provide protection from liability for companies that share information with the government was delayed because of the Snowden Leaks. Chris Strohm, *Anti-Hacking Bill Aiding Verizon Delayed by Snowden Leaks*, BLOOMBERG POLITICS (June 28, 2013, 12:01 AM ET), http://www.bloomberg.com/news/2013-06-28/anti-hacking-bill-aiding-verizon-delayed-by-snowden-leaks.html.

the other it signals a greater problem within the industry: that the current standards employed by businesses to prevent breaches are not working.[5]

While abstinence from data collection is the only absolute protection currently[6] – if there is no data there is nothing to breach – eliminating all data collection is not a realistic option for retailers in today's information age.[7] The data businesses collect feed essential operations, such as processing payments and providing customer service.[8] Liability can be minimized in some industries, such as the advertising industry, by limiting the data collected to less sensitive types of information.[9] Retailers, however, often use third-party payment processors to serve as middlemen in a transaction to collect and process financial information so the retailers do not have to face the liability associated with collecting that information.[10] The payment processors bear the liability[11] for the sensitive data they need to collect to operate effectively.[12]

During the sales process the collected information is used to verify the identity of the purchaser, verify that the payment method is authentic, and

---

5. Nicole Perlroth, *Experts Find a Door Ajar in an Internet Security Method Thought Safe*, N.Y. TIMES, Apr. 8 2014, http://bits.blogs.nytimes.com/2014/04/08/flaw-found-in-key-method-for-protecting-data-on-the-internet.

6. There is always a risk of a breach no matter how well data is secured or how much is invested in data security. "You can never completely stop attackers from accessing data because there's a lot of clever tricks they can play…(Encryption is) like locking your front door (to deter burglars), but there are other ways in." Jessica Morris, *Yahoo Announces Latest Move in Privacy Battle*, CNBC, (Apr. 3, 2014, 10:31AM), http://www.cnbc.com/id/101551972.

7. BUSINESS WITHOUT BORDERS: THE IMPORTANCE OF CROSS-BORDER DATA TRANSFERS TO GLOBAL PROSPERITY, U.S. CHAMBER OF COMMERCE AND HUNTON & WILLIAMS LLP 6 (2014), https://www.huntonprivacyblog.com/files/2014/05/021384_BusinessWOBorders_final.pdf.

8. Data Security, FTC, http://www.business.ftc.gov/privacy-and-security/data-security (last visited Apr. 8, 2014)

9. *See generally* UPDATE TO THE 2015 NAI CODE OF CONDUCT, NETWORK ADVERTISING INITIATIVE (2015), http://www.networkadvertising.org/sites/default/files/NAI_Code15encr.pdf. Types of information listed from least to most sensitive: anonymous, pseudonymous, personally identifiable information (PII), and sensitive PII.

10. For example, PayPal allows users to send and receive payments without sharing financial information with the other transacting party, whether the purchaser or the seller. PAYPAL, ABOUT PAYPAL, https://www.paypal-media.com/about (last visited Mar. 4, 2014).

11. Stewart Room, *The Privacy Regulatory Bear Market and Playing Political Football with Business*, PRIVACY & INFO. L. BLOG (Jan. 23, 2014), http://privacylawblog.ffw.com/2014/the-privacy-regulatory-bear-market-and-playing-political-football-with-business.

12. "The ready availability of personal information helps businesses 'deliver the right products and services to the right customers, at the right time, more effectively and at lower cost.'" Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877, 882 (2000) (quoting Fred Smith, founder and President of the Competitive Enterprise Institute at the time).

verify the necessary funds are available for the purchase.[13] Collecting that information, however, makes payment processors a target for hackers. Akin to the Target breach, Heartland Payment Services, Inc., a payment processor, suffered a breach in 2009 that compromised as many as 100 million payment card records.[14] Similarly, online payment processors (OPPs), such as PayPal, collect financial information, such as a credit card number, expiration date, and verification code, to process purchases and authorize sales online.[15] E-commerce is valued at an estimated $8 trillion per year[16] – which equates to more than ten-percent of the Gross World Product.[17] While commerce is increasingly conducted online via cross-border data flows,[18] "merchants, financial institutions, and consumers all still have substantial concerns about the security of online payments . . . and the privacy of personal information."[19]

Data protection standards should aim to limit possible data breaches, the resulting damages from any breaches, and simultaneously to limit the liability of companies when they are the non-offending party. Under current data-breach regulations, financial institutions – including banks, payment processors, and OPPs – bear the liability for a breach of any information they collect, even when they are not the offending party.[20] Data breach notification laws vary by state, but they all assign liability through an indirect liability regime.[21] This indirect liability regime punishes the OPP or payment intermediary, which are already victims of the data breach, instead of punishing the actions of the actual bad actor: the hacker.[22]

Hackers can be difficult to punish because technology can obscure the hacker's identity and true location.[23] An IP address is regarded as a weak identifier to serve as evidence in a criminal case that a particular individual carried out an activity, such as illegal downloading, because an IP address

---

13. *See id* at 882-884.

14. Mark McCarthy, *Information Security Policy in the U.S. Retail Payments Industry*, 2011 STAN. TECH. L. REV. 3, ¶ 60.

15. About PayPal, *supra* note 10.

16. *Business Without Borders*, *supra* note 7, at 5.

17. World GDP (Official Exchange Rate) estimates the Gross World Product (GWP) at $74.31 trillion (2013), http://www.indexmundi.com/world/gdp_%28official_exchange_rate%29.html.

18. Joshua Meltzer, *The Internet, Cross-Border Data Flows and International Trade*, BROOKINGS.EDU (Feb. 25, 2013), http://www.brookings.edu/research/papers/2013/02/25-internet-data-flows-international-trade-meltzer.

19. ESTHER C. RODITTI, 3-11A COMPUTER CONTRACTS § 11A.01 , at 1 (Matthew Bender & Co. 2013), LEXIS.

20. McCarthy, *supra* note 14, at ¶ 34.

21. *Id.* at ¶ 20.

22. *See id*.

23.*See* VPR Int'l v. Does 1-1017, No. 11-2068, 2011 U.S. Dist. LEXIS 64656 at *4 (C.D. Ill. Apr. 29, 2011) (finding that IP address provided by ISP did not accurately identify illegal downloader).

merely identifies the location where a certain activity occurred.[24] A hacker's true location though can sometimes be found through online geo-location tools that can collect more information than just a hacker's location.[25] That collected data can be aggregated at times to sufficiently identify an individual.[26] OPPs, however, should not be liable just because the true criminal may be difficult to find; instead OPPs should be held to high standards that if met limit their liability in the case of a data breach.

The current data protection regime is not effective at limiting possible data breaches or OPP industry liability when a hacker gains unauthorized access to data.[27] In contrast, other legal regimes such as copyright law give OPPs a safe-harbor when third parties use OPPs to commit illegal acts.[28] For example, when distributors use an OPP to sell copyright infringing work, OPPs are not liable for those sales because OPPs do not make a material contribution to infringement by processing those sales.[29] Similarly, if OPPs meet sufficiently high data protection standards they should not be liable for unauthorized access by a hacker.

Data management compliance for OPPs is complex, costly, and ineffective because the laws are constantly evolving and still do not alleviate the concerns of merchants, financial institutions, or consumers.[30] OPPs are currently regulated under a traditional territorial-based approach, with regulations applying at the state, national, and international levels.[31] At the state level, each state has its own data breach notification law, at the national level there is no national standard for data breach notification,[32] and at the international level, multiple countries have laws specific to data security practices within their borders.[33] Outside of formal regulations, countries and

---

24. *See In re* BitTorrent Adult Film Copyright Infringement Cases, 296 F.R.D. 80, 84-5 (E.D.N.Y. 2012). A computer in a household is usually shared, which means a child, a boyfriend, or any other visitor, is just as likely to be using the computer. *See id.* Many households now have a wireless network and if the network is not secured others may use an IP address without the original account holder's knowledge. *See id.*

25. *See* Jerusha Burnett, Note, *Geographically Restricted Streaming Content & Evasion of Geolocation: The Applicability of the Copyright Anti-Circumvention Rules*, 19 MICH. TELECOMM. & TECH. L. REV. 461, 484 (2013).

26. *See id.* at 483.

27. *See* McCarthy, *supra* note 14, at ¶ 34.

28. *See* Perfect 10, Inc. v. Visa Int'l Serv. Assoc., 494 F.3d 788, 795-96 n.4 (9th Cir. 2007).

29. *Id.*

30. Roditti, *supra* note 19, at 1.

31. McCarthy, *supra* note 14, at ¶ 12; *Business Without Borders: supra* note 7, at 14.

32 . Security Breach Notification Chart, PERKINS COIE, revised Oct. 2013, http://www.perkinscoie.com/statebreachchart/.

33. "Such inconsistency. . . saddles businesses with the cost of identifying which data protection regime applies to a given act of data processing, understanding the requirements of that regime, and then applying them appropriately, and the risk of liability if they fail to reconcile inconsistent data protection requirements appropriately. The problem is especially true online. The Internet crosses state and national boundaries and has facilitated truly global markets. . .The price of inconsistent data protection laws is borne by entities that must comply

international organizations promulgate general guidelines.[34] These guidelines consist mainly of lists of basic information practice principles that are too broad to apply to specific industries, are unenforceable, and lack consensus. This traditional approach has proven to be an ineffective approach to cyber regulation because it fails to adapt to online, globally connected networks.[35]

Data security regulation, especially for the OPP industry, needs to shift away from territorial-based regulation and towards industry-based regulation. This shift is best achieved for OPPs through an industry-specific code of conduct, because it encourages active participation by industry members to develop industry standards and best practices; it can be implemented more quickly than regulation; it is flexible enough to be applied internationally and nationally; it is flexible enough to adapt to changing technologies; and it takes into account the business and technological capabilities of OPPs.

First, this note provides more in-depth information on OPPs, the current territorial-based regulatory landscape for OPPs, and models of industry-based regulatory systems from other industries that should be used to create an industry code of conduct for OPPs. Second, this note analyzes the reasons behind the need for a shift away from territorial-based regulation and towards industry-based systems. Lastly, this note constructs the basics of an OPP industry code of conduct from a combination of self-regulation industry models.

II. OPPS AND THE DATA SECURITY REGULATION LANDSCAPE

The OPP regulatory landscape is challenging for several reasons. First, OPPs are unique because of the sensitive information they need to collect to run their business. Without information identifying the individual initiating a transaction and the relevant financial information, an OPP would be unable to process a payment. Second, the current regulation surrounding OPPs is territorial-based which does not reflect the global nature of online commerce. Third, self-regulation industry-based models used by other industries could be used by OPPs to address the data security challenges of their industry and to construct a code of conduct for the OPP industry.

---

with those laws and by individuals whose privacy is supposed to be protected by them." Fred H. Cate, *The Failure of the Fair Information Practice Principles in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 368-69 (Jane K. Winn ed., Ashgate Pub. Ltd. 2006), http://ssrn.com/abstract=1156972.

34. *Id.* at ¶ 13.

35. "Looking at the bigger picture of privacy law enforcement, penalties and sanctions, the climate has been getting worse for businesses year-on-year … [t]he regulatory rhetoric getting stronger and darker over the cycle…[with the] imposition of large financial penalties and negative rhetoric in press statements, television appearances and promulgation of guidance and policy documents." Room, *supra* note 11.

A. Online Payment Processors and Cross-Border Data Transfers

OPPs process online payments using information provided by the purchaser(s) to validate financial information. For example, OPPs based in the United States collect credit card information to authorize a transaction such as the credit card number, cardholder name, expiration date, billing address, and the Card Verification Value (CVV) number from the back of a credit card.[36] The collected information is then transmitted, using the account number for routing, to the appropriate bank that either authorizes or denies the transaction based on the authenticity of the information provided.[37] The CVV is a primary means of authorization and is used as an access code that if entered correctly indicates to the bank that the cardholder is initiating the transaction and access to the related account is authorized.[38] Internationally, other countries use chip and PIN technology; the authentication process is similar, but instead of using a CVV, a new authentication code is used for each transaction to reduce the risk of fraud.[39] Similarly, PayPal provides a security option for consumers to have a security code sent to their mobile device each time they log onto their account or use PayPal in a transaction.[40] OPPs, through those authentication processes, facilitate cross-border transactions that grow the global economy.[41]

B. Territorial-Based Regulation Models

Existing regulations surrounding OPPs are primarily based on political territories, meaning that the laws applying to OPPs vary from country to country, ignoring the modern reality that online transactions occur across borders and across the globe. On a global scale there is a lack of clarity of which jurisdiction a company is subject to (or should be subject to), or what list(s) of international guidelines a company should follow. The interconnected world calls for a release from this territorial-based regulation

36. McCarthy, *supra* note 14, at ¶ 27.

37. *Id.* at ¶ 24.

38. *Id.*

39. *Id.* at ¶ 26.

40 . PAYPAL, PAYPAL SECURITY KEY, https://www.paypal.com/us/webapps/mpp/security/security-key (last visited Mar. 3, 2014).

41. *Sotto Speaks on the Importance of Cross-Border Data Transfers to Global Prosperity*, PRIVACY & INFO. SEC. L. BLOG (May 20, 2014), https://www.huntonprivacyblog.com/2014/05/articles/sotto-speaks-importance-cross-border-data-transfers-global-prosperity/.

because it is limited in its reach, applicability, and ability to protect information.[42]

1. United States Regulation of OPPs

In the United States, data breach notification law is regulated at the state level (there is currently no national data-breach notification standard), and OPPs are primarily regulated indirectly through standards developed to apply to financial institutions, such as banks and the payment card industry.[43] Attempts to create data protection standards at the national level by the United States Congress have failed. In 2005 Senator Patrick Leahy (D-VT) introduced the Personal Data Privacy and Security Act.[44] The bill sought to *inter alia* require notice of security breaches, increase protections against security breaches, and enhance criminal penalties for security breaches.[45] Senator Leahy has reintroduced the bill in each Congress since 2005 and it has failed to pass each time.[46] On January 8, 2014, Senator Leahy reintroduced the bill again.[47] That version of the bill again proposes a national standard for data breach notification, criminal penalties for intentionally concealing breaches that cause economic damage to consumers, and requirements that businesses protect sensitive customer information from cyber threats by implementing internal data protection policies.[48] The bill additionally contains provisions that explicitly grant authority to the Federal Trade Commission (FTC) to create and enforce rules requiring companies to protect personally identifiable information and to

42. "Because location has less meaning in an electronic world, protecting privacy requires attaching protection to the … record itself, rather than to the institution that generates it." Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 513 (1995).

43. Eunice Chung et al., *Consumer Data Protection In Online Retail: On Protecting Privacy in the EU, US, and China*, DLA PIPER RE:MARKS ON COPYRIGHT & TRADEMARK (Nov. 17, 2014), http://www.remarksblog.com/internet/consumer-data-protection-in-online-retail-on-protecting-privacy-in-the-eu-us-and-china/.

44. Personal Data Privacy and Security Act of 2005, S.1789, 109th Cong. (2005) (related bill S. 1332 introduced on June 29, 2005), https://www.govtrack.us/congress/bills/109/s1789.

45.*See id.*

46. *See e.g.*, *Senators Renew Efforts to Pass Data Privacy Legislation*, PRIVACY & INFO. SEC. L. BLOG (Jan. 13, 2014), https://www.huntonprivacyblog.com/2014/01/articles/senators-renew-efforts-pass-data-privacy-legislation/; Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007) (reintroduced as S. 1490 on July 22, 2009); Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (2009) (reintroduced as S. 1151 on June 7, 2011); Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011) (reintroduced as S. 1897 on Jan. 8, 2014).

47. Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014), https://www.govtrack.us/congress/bills/113/s1897.

48. The bill also includes a provision requiring the Computer Fraud and Abuse Act to be updated to make attempted computer hacking and conspiracy to commit computer hacking punishable under the same criminal penalties as the underlying offense. *See id.*

notify customers of a breach.[49] However, given the bill's legislative record it is unlikely it will pass without more significant amendments from prior versions of the bill proposed in previous Congressional sessions and suffers from the inability to apply on an international level.

The United States House of Representatives' version of a data-breach notification bill, the Data Accountability and Trust Act (DATA), also has a poor legislative record. First introduced in 2007, the House bill failed all three times it was introduced (and reintroduced) by Congressman Bobby Rush (D -Ill.).[50] In 2009, DATA, which aims to eliminate the confusion and cost in meeting multiple states regulations for breach notification procedures, passed the House but not the Senate.[51] If DATA had passed, it would have superseded existing state laws for data breach notification[52] – essentially creating a federal data breach notice process.[53] Once again, such a law would be limited in its reach to United States territory.

Specifically, the Gramm-Leach-Bliley Act requires financial institutions, which indirectly includes service providers such as OPPs[54] to adopt information security programs to protect consumer information.[55] The

---

49. Currently the FTC exercises authority over data security through section 5 of the FTC Act's prohibition on unfair or deceptive acts or practices. *See* FTC v. Wyndham Worldwide Corp., 2013 U.S. Dist. LEXIS 41494 (D. Ariz. Mar. 25, 2013); LabMD, Inc., FTC Docket No. 9357, *dismissal denied* Jan. 16, 2014; *see also* FTC, 2014 PRIVACY & DATA SECURITY UPDATE (2014), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

50. Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007) (reintroduced as H.R. 2221 on Apr. 30, 2009), https://www.govtrack.us/congress/bills/110/hr958. Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009), (reintroduced as H.R. 1707 on May 4, 2011), https://www.govtrack.us/congress/bills/111/hr2221. Data Accountability and Trust Act, H.R. 1707, 112th Cong. (2011), (reintroduced as H.R. 1707 on May 4, 2011), https://www.govtrack.us/congress/bills/111/hr2221.

51. H.R. 2221, *supra* note 50.

52. States are largely opposed to federal regulation that would supersede their local laws. States want to maintain their own rules because of fears that the national standard will be weaker than their own rules and to preserve their authority to enforce data breach regulations. Jessica Meyers, *States Defend Turf from Feds on Data Breach Rules*, POLITICO (Feb. 19, 2014), http://www.politico.com/story/2014/02/states-defend-turf-from-feds-on-data-breach-rules-103647.

53. Richard E. Mackey, Jr., *Understanding the Data Accountability and Trust Act*, INFO. SEC. (Dec. 2010), http://searchsecurity.techtarget.com/magazineContent/Understanding-the-Data-Accountability-and-Trust-Act.

54. MacCarthy, *supra* note 14, at ¶ 45. Counter intuitively, service providers are requested to "store transaction data much longer than needed for billing purposes in order to facilitate criminal investigations." *See* Sarah Spiekermann & Lorrie Faith Cranor, *Engineering Privacy*, 35 IEEE Transactions on Software Engineering, no. 1, January/February 2009, at 72, http://ssrn.com/abstract=1085333.

55. 15 U.S.C. § 6801(a). More specifically, 16 C.F.R. § 314.4 explains the necessary elements of an information security program. *See* FTC, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FINANCIAL INFORMATION RULE OF THE GRAMM-LEACH-BLILEY ACT: A GUIDE FOR SMALL BUSINESS FROM THE FEDERAL TRADE COMMISSION (July 2002),

Act requires multiple agencies, including the FTC, Comptroller of the Currency, and the SEC to establish "appropriate standards for the financial institutions subject to their jurisdiction," "to insure security and confidentiality of customer records and information" and to "protect against unauthorized access" to the information.[56] The Act and other United States laws all have the same flaw – they do not account for the global nature of online commerce and are limited in their reach and enforceability by territorial jurisdiction.

Challenges to data protection for trans-border data flows cannot be solved with isolated regulations promulgated by individual countries focused on the location of the data sender, receiver or processor.[57] In addition to the territorial limits on the reach of government regulations, "[i]t is difficult to see how broad or comprehensive new privacy laws or regulations at the present time could keep pace with the revolutionary and extraordinarily rapid transformation of the Internet and other new media technologies."[58] Location, geographic-based legislation is limited in its effectiveness, inconsistent, costly, fails to incorporate industry expertise, and impedes cross-border data flows necessary for modern business.[59]

2. International Regulation

Currently there is no international standard for data protection and "[t]he situation only grows worse as more states and nations develop inconsistent data protection laws with which they attempt to regulate increasingly global information flows."[60] Existing regulation varies by country, with each country using different scales[61] to balance privacy rights[62] and the free flow of information.[63] Guidelines that do apply at the international level consist mainly of lists of basic information practice

---

http://www.business.ftc.gov/documents/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.

56. 15 U.S.C. § 6801(b).

57. Joel R. Reidenberg, *Symposium: Electronic Communications and Legal Chance: Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms*, 6 HARV. J. LAW & TECH. 287, 290 (1993).

58. Wendy Davis, *Ad Groups Tout Self-Regulation to White House*, THE DAILY ONLINE EXAMINER (Apr. 1, 2014), http://www.mediapost.com/publications/article/222759/ad-groups-tout-self-regulation-to-white-house.html#reply (quoting the Association of National Advertisers).

59. Ira Rubenstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 ISJLP 356, 361 (2010).

60. Cate, *supra* note 33, at 344.

61. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 155-56 (2004).

62. Nader v. General Motors Corp., 255 N.E.2d 765, 772 (N.Y. Ct. App. 1970) (Brietel, J. concurring).

63. Cate, *supra* note 12, at 884.

principles that are too broad to apply to specific industries, are unenforceable, and lack consensus. Even within the European Union (EU), conflicting provisions impede "the ability of computer users in the European Union to transfer computerized information across national borders."[64]

The EU, Malaysia, Brazil, Mexico, the Netherlands, and France[65] all are working on creating or revising their existing data protection regulations, joining the close to 100 countries already with individual data protection statutes.[66] Proposed and current regulations aim to simultaneously meet the needs of multiple industries and balance the competing goals of privacy protection and the free flow of information.[67] Even under the slim possibility that the laws from these 100 countries integrate harmoniously to create a global web of data protection regulation,[68] the ability to create a cohesive understanding of all the regulations (much less comply with them) is a daunting and costly task for any business. While OPPs face the challenge of meeting this myriad of international data protection regulations, countries in turn struggle to design regulations that meet the needs of their citizens, are broad enough to cover multiple industries, and simultaneously are narrow enough to be enforceable.[69]

For example, Brazil recently proposed a requirement that domestic and international companies who collect data related to Brazilian citizens store

64. Amy Fleischmann, Note, *Personal Data Security: Divergent Standards in the European Union and the United States*, 19 FORDHAM INT'L L.J. 143, 150 (1995) (noting as an example when the French Government prohibited the transfer of Fiat's employee information from Italy because it considered Italian data security requirements inadequate).

65. In fact, the Netherlands and France are subject to their own data protection regimes as well as the overlapping EU regulations. For example, the French Data Protection Authority (CNIL) adopted new guidelines on processing bank card details related to the sale of goods and services at a distance in response to the increase in online transactions. Olivier Proust, *CNIL Issues New Guidelines on the Processing of Bank Card Details*, PRIVACY & INFO. L. BLOG (Feb. 27, 2014), http://privacylawblog.ffw.com/2014/cnil-issues-new-guidelines-on-the-processing-of-bank-card-details.

66. Phil Lee, *2013 a Big Year for Privacy? You Ain't Seen Nothing Yet!*, PRIVACY & INFO. L. BLOG (Dec. 31, 2013), http://privacylawblog.ffw.com/2013/2013-a-big-year-for-privacy-you-aint-seen-nothing-yet.

67. "Data privacy rules are often cast as a balance between two basic liberties: fundamental human rights on one side and the free flow of information on the other side. Yet, because societies differ on how and when personal information should be available for private and public sector needs, the treatment and interaction of these liberties will express a specific delineation between the state, civil society, and the citizen." Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1341-42 (2000).

68. DLA Piper provides a comprehensive and interactive tool on the varying state of data protection laws around the globe. *See Data Protection Laws of the World*, DLA PIPER, (Paul McCormack & Kate Lucente, eds.), http://www.dlapiperdataprotection.com (last visited Mar. 5, 2014).

69.Reidenberg,, *supra* note 57, at 290.

that data physically on servers in Brazil.[70] This localization effort received criticism from organizations across the globe[71] because it would have the consequence of forcefully subjecting companies to Brazil's data protection law if they do business with Brazilian citizens.[72] Additionally, companies attempting to avoid the law would face the choice of complying with its requirements, or limiting their business to customers outside of Brazil.[73] It is unclear how the nationality or physical location will affect how the law impacts the collection of personal information by a corporation. Does the law apply to anyone physically located within Brazil, regardless of their nationality? If a company collects information on a Brazilian citizen while they are traveling abroad, is the law valid, or is its application limited solely to Brazilian citizens while they are located on Brazilian soil?

Brazil has since dropped the local data storage rule from the proposed bill, but it still states that global Internet companies, including financial services such as OPPs,[74] "are subject to Brazilian laws in cases involving information on Brazilians even if the data is stored abroad."[75] This could have a chilling effect on global business especially as other countries follow in Brazil's footsteps[76] and extend the reach of their laws to businesses that collect information on their citizens.[77] Even without the local storage rules, such legislation hinders the growth of the global economy because it forces

---

70. Loretta Chao & Paulo Trevisani, *Brazil Legislators Bear Down on Internet Bill*, WALL ST. J. (NOV. 13, 2013, 6:45 PM ET), http://online.wsj.com/news/articles/SB10001424052702304868404579194290325348688.

71. Letter from the Global Business Community to Members of the Brazilian Congress in re Data Center Localization (Oct. 22, 2013), http://www.wilsoncenter.org/sites/default/files/Data%20Center%20Localization%20-%20English%20version.pdf.

72. *See* Chao, *supra*.

72. *See* Chao, *supra*.

73. *See* Chao, *supra* (stating that companies that don't comply could be "barred from doing business in one of the world's most significant markets or be obligated to pay millions of dollars in fines).

74. "In-country data requirements threaten to harm Brazil's competitive and global automotive, its manufacturing and service industries, like aerospace, oil and gas, financial services, retail, and healthcare industries and also R&D operations." *Id.*

75. *Brazil Removes Local Data Storage Requirement from Internet Bill*, PRIVACY & INFO. SEC. L. BLOG (Mar. 19, 2014), https://www.huntonprivacyblog.com/2014/03/articles/brazil-removes-local-data-storage-requirement-internet-bill/.

76. *Russian Parliament Adopts Internet Privacy Bill Requiring Data Localization*, PRIVACY & INFO. SEC. L. BLOG (July 7, 2014), https://www.huntonprivacyblog.com/2014/07/articles/russian-parliament-adopts-internet-privacy-bill-requiring-data-localization/; HUNTON & WILLIAMS LLP, *Deadline for Compliance with Russian Localization Law Set for September 1, 2015*, PRIVACY & INFO. SEC. L. BLOG (Jan. 2, 2015), https://www.huntonprivacyblog.com/2015/01/articles/deadline-for-compliance-with-russian-localization-law-set-for-september-1-2015/.

77. Phil Lee, *Challenges in Global Data Residency Laws – and How to Solve Them*, PRIVACY L. BLOG (Sept. 13, 2014), http://privacylawblog.fieldfisher.com/2014/challenges-in-global-data-residency-laws-and-how-to-solve-them.

companies to choose to comply with Brazilian (or the propagating country's) law or to limit the geographic reach of their business.[78]

International data protection standards, embodied in multiple lists of guidelines, are beneficial in providing education and resources on improving data protection; however, these guidelines have failed to bring unity to European data security requirements.[79] The high level at which the guidelines were developed provides a theoretical framework, not a practicable one. First, the guidelines do not supersede existing data security requirements.[80] Second, the guidelines cannot be enforced on an international level without universal adoption by all countries and a body to enforce the guidelines.[81] Finally, global standards are too broad to meet the needs of multiple groups with differing needs and capabilities and are challenging to apply to any specific issues, industries, or types of information.[82]

For example, in 2013 the Organization for Economic Cooperation and Development (OECD) updated the privacy guidelines it originally promulgated in 1980.[83] The guidelines outline the need for a practical, risk management-based approach to implementing privacy protection, enhanced privacy protection on a global level through interoperability, national privacy strategies, privacy management programs, and for global standards for notification following a data security breach.[84] The revised guidelines make suggestions for the protection of privacy and trans-border flows of personal information, highlighting the challenge to create international standards. International standards created through guidelines however lack the enforceability of regulations or legislation.[85] Additionally the guidelines are

78. "Thus, in-country data storage requirements would detrimentally impact all economic activity that depends on data flows." Letter from the Global Business Community, *supra* note 71.

79. Herald D.J. Jongen & Gerrit A. Vriezen, *The Council of Europe and the European Community*, *in* DATA TRANSMISSION AND PRIVACY 140-55, 150 (Dennis Campbell & Joy Fisher eds., 1994).

80. Alexander D. Roth, *Introduction to Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 19 I.L.M. 282, 282 (1980).

81. For example, The German Data Protection Authority (DPA) published its own recommendations for mobile payment services. HUNTON & WILLIAMS LLP, *German DPA Publishes Recommendations for Mobile Payment Systems*, PRIVACY & INFO. SEC. L. BLOG (Nov. 13, 2013), https://www.huntonprivacyblog.com/2013/11/articles/german-dpa-publishes-recommendations-mobile-payment-systems/.

82. Reidenberg Symposium, *supra* note 57, at 290.

83. OECD, GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (July 11, 2013), http://www.huntonprivacyblog.com/wp-content/uploads/2013/09/2013-oecd-privacy-guidelines.pdf.

84. *See generally id.*

85. *OECD Issues Updated Privacy Guidelines*, PRIVACY & INFO. SEC. L. BLOG (Sept. 16, 2013), http://www.huntonprivacyblog.com/2013/09/articles/oecd-issues-updated-privacy-guidelines/.

meant to apply on a large scale, "at the highest level of government," and so are too broad to provide effective protection for online consumers.[86]

Industry-focused data management standards for OPPs therefore could help synthesize the myriad regulations, guidelines, and recommendations into understandable and applicable principles that are specific to the needs of the industry and would be easier for the OPP industry to implement.[87]

C. Industry-Based Self-Regulation Models

Government agencies such as the Department of Commerce and the FTC favor self-regulation in the privacy arena because it is more flexible, cost-effective, and can keep pace with technological advancement.[88] The United States additionally recognizes the validity of self-regulation through safe-harbor programs in copyright law, under the COPPA rule, and in the Online-Based Advertising industry.[89] An effective safe-harbor program combines the advantages of a flexible self-regulatory code with the enforcement power of a governmental body. However, safe-harbor programs suffer from the same scalability challenge that territorial-based regulation does because it is unclear how consistent application of the standards can occur on the international scale without an international 'governmental' body to vest with enforcement power. While safe-harbor framework exists for some cross-border data transfers,[90] "sectors not regulated by the FTC, such as financial services, telecommunication common carriers, and insurance, are not covered by the Safe Harbor Frameworks."[91] Therefore an

86. *Id.*

87. "Information about individuals' needs and preferences is the cornerstone of any system that allocates goods and services within an economy." *Federal Privacy Issues: Hearing Before the Subcomm. on Fin. Insts. & Consumer Credit of the Comm. on Banking and Fin. Servs*,.106th Cong. (1999) (testimony of Fed. Reserve Bd. Governor Edward Gramlich), http://www.federalreserve.gov/boarddocs/testimony/1999/19990721.htm.

88. Rubenstein, *supra* note 59, at 356.

89. Perfect 10, Inc. v. Visa Int'l Serv. Ass'n., 494 F.3d 788, 795 n.4 (9th Cir. 2007); *FTC Acts on Several Industry COPPA Proposals*, PRIVACY & INFO. SEC. L. BLOG (Mar. 14, 2014), https://www.huntonprivacyblog.com/2014/03/articles/ftc-acts-several-industry-coppa-proposals/; ADVERTISING SELF-REGULATORY COUNCIL, SUNTRUST BANK REFERRED TO THE CFPB FOR REFUSAL TO PARTICIPATE IN SELF-REGULATION (May 8, 2014), http://www.asrcreviews.org/2014/05/suntrust-bank-referred-to-the-cfpb-for-refusal-to-participate-in-self-regulation/.

90. *Business without Borders*, *supra* note 7, at 21. "The Safe Harbor framework is composed of a set of Privacy Principles and Frequently Asked Questions. To certify to the Safe Harbor, organizations generally are required to (1) conform their privacy practices to the Safe Harbor Privacy Principles; (2) file a self- certification form with the Department of Commerce; and (3) publish a Safe Harbor privacy policy that states how the company complies with the Privacy Principles."

91. Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, *at 33, The White House, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (last visited July 3, 2012).

independent self-regulation model is necessary for financial services such as OPPs.

Three primary industry-based models created by other organizations and industries are useful for creating a code of conduct for the OPP industry. First, the Fair Information Practice Principles (FIPPs) are an appropriate starting point for any data collection system, because they are principles agreed upon by the United States and a number of European Countries through privacy agreements and national laws.[92] Second, the Network Advertising Initiative's code of conduct models a successfully implemented voluntary code of conduct in the third-party online advertising industry. Third, the Payment Card Industry's (PCI) Data Security Standard is relatable to, and can be adapted for, the OPP industry.

1. The Fair Information Practice Principles (FIPPs)

The eight FIPPs "are the benchmark against which the FTC and privacy advocates evaluate any self-regulatory privacy scheme," and are used by the private and public sector as a basis for their privacy and data collection policies.[93]

> **1. Transparency**: information collectors should be transparent in their collection, use, dissemination, and maintenance practices.
> **2. Individual Participation**: consent of the individual for the collection of the data should be obtained.
> **3. Purpose Specification**: the specific purpose(s) the information is being collected for should be articulated.
> **4. Data Minimization**: only the information necessary to accomplish the specified purpose should be collected.
> **5. Use Limitation**: the information should only be used for the specific purpose(s) for which it is being collected.
> **6. Data Quality and Integrity**: To the extent practicable collected information should be accurate, relevant, timely, and complete.
> **7. Security**: Collected information should be protected from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

---

92. The FIPPs are the core of the Privacy Act of 1974, are adopted by the Department of Homeland Security as its policy framework, and are the root of the OECD privacy guidelines. *See* HUGO TEUFEL III, U.S. DEP'T OF HOMELAND SEC., MEMO. NO. 2008-01, PRIVACY POLICY GUIDANCE MEMORANDUM 2-4 (Dec. 29, 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

93. Rubenstein, *supra* note 59, at 382; *see also,* Appendix B to the White House's 2012 Privacy Report includes a table demonstrating the continuity of the FIPPs through the Consumer Privacy Bill of Rights, the OECD Privacy Guidelines, the DHS Privacy Policy, and the APEC Principles. Consumer Data Privacy, *supra* note 91, at 49.

> **8. Accountability and Auditing**: Collecting organizations should be accountable for compliance with the FIPPs and the use of information should be audited to demonstrate compliance with the FIPPs and all applicable data protection requirements.[94]

A data collection practice assessed under the FIPPs is analyzed for the methods used to achieve each FIPP, the barriers to achieving each FIPP, the risks and impacts in the system to achieving each FIPP, and any compensating controls or measures that can mitigate those risks and impacts. In some cases, not all of the FIPPs are applicable to a given system.[95]

2. Network Advertising Initiative

The Network Advertising Initiative (NAI) developed a code and mobile code of conduct based on the FIPPs as well as additional principles for the online third-party advertising industry.[96] NAI is essentially a trade association of third-party online advertisers that voluntarily adhere to its code.[97] NAI's code is based on the FIPPs outlined above and serves as an example of how those principles can be adapted to a particular industry.[98] While membership in the NAI is voluntary, prospective members must achieve compliance with the NAI code before being granted membership and all existing members must maintain compliance with the code.[99] The NAI received criticism at its start for four primary reasons: (1) the NAI opt-out cookie did not work consistently; (2) the NAI had a static approach to self-regulation which was not flexible enough to emerging technologies or the varying business models of ad networks; (3) the NAI self-regulation model did not include a majority of groups within the behavioral advertising industry; and (4) the enforcement program lacked transparency and independence.[100]

Despite initial setbacks, the NAI is now recognized for its robust compliance and enforcement program and NAI's 2013 compliance report demonstrates how its strict self-regulatory code can be effectively used to protect data privacy and honor consumer choices.[101] In 2013, 3.9 million

---

94. Descriptions of FIPPs adapted from Privacy Policy Guidance Memorandum, *supra* note 92, at 3-4.

95. *Id.*

96. About the NAI, http://www.networkadvertising.org/about-nai/about-nai (last visited Mar. 5, 2014).

97. NAI Code of Conduct, at 1, http://www.networkadvertising.org/2013_Principles.pdf (last visited Mar. 5, 2013).

98. *Id.* at 3.

99. *Id.* at 1-2, 8.

100. *Id.*

101. *NAI Achieves Highest Level of Member Compliance in Consumer Privacy*, THE MAKEGOOD (Apr. 8, 2014), http://www.the-makegood.com/2014/04/08/nai-achieves-highest-

consumers used NAI's opt-out mechanism to opt-out of tracking by NAI member ad networks.[102] NAI's membership represents "a significant portion of the marketplace" with 88 member ad networks in 2013.[103] NAI membership additionally includes the largest ad networks such as Google, Yahoo, AOL, and Microsoft and all members must comply with the strict standards of NAI's code of conduct.[104] NAI's code of conduct is more easily updated than regulation, because the code can be revised as frequently as necessary to reflect technological changes. For example, NAI's updated 2014 code of conduct requires ad-networks to use opt-in consent for sexual orientation[105] and its mobile code of conduct recognizes "that maintaining an effective Mobile Application Code may require, at least initially, regular iterations, with full notice and participation by stakeholders."[106]

3. The PCI Data Security Standard and Security Standards Council

More closely related to OPPs, the Payment Card Industry (PCI) developed a Data Security Standard in 2004 and an independent Security Standards Council (PCI SSC)[107] in 2006 to manage the standard.[108] The PCI wanted a "truly industry-wide standard, administered by an entity independent of the particular card companies that originally developed the standard."[109] Similar to the FIPPs, the PCI standard is conceptualized by

---

level-of-member-compliance-in-consumer-privacy/; *see also* Katy Bachman, *Report: Ad Networks Adhering to Strict Privacy Guidelines* (Mar. 13, 2014) (quoting NAI CEO, Marc Groman) http://www.adweek.com/news/technology/report-ad-networks-adhering-strict-privacy-guidelines-156277.

102. *Id.; contra* Wendy Davis, *Ad Groups Tout Self-Regulation to White House*, (Apr. 1, 2014) ("[I]t's not practical for consumers to try to 'turn off' the data machine . . . [t]here have to be regulatory rules that limit the collection of data and empower individuals to make their own privacy decisions.") (quoting the Center for Digital Democracy), http://www.mediapost.com/publications/article/222759/ad-groups-tout-self-regulation-to-white-house.html#reply.

103. Katy Bachman, *Report: Ad Networks Adhering to Strict Privacy Guidelines* (Mar. 13, 2014) (quoting NAI CEO, Marc Groman), http://www.adweek.com/news/technology/report-ad-networks-adhering-strict-privacy-guidelines-156277.

104. *Id.*

105. *Id.*

106 . 2013 NAI Mobile Application Code (2013), http://www.fcclaw.com/wp-content/uploads/2013/08/LNGS-Mobile-Payments-Network-Advertising-Initiative-2013-Mobile-Application-Code-2013-08-02.pdf.

107. PCI SSC was created by American Express, Discover Financial Services, JCB, MasterCard, and Visa. McCarthy, *supra* note 14, at ¶ 40.

108. *Id.*

109. *Id.*

basic requirements with more detailed sub-requirements. The PCI standard has twelve basic requirements:

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.[110]

The PCI requirements, however, were designed to meet the business needs of payment card companies such as Visa and therefore do not meet the needs of OPPs.[111] PCI members store financial information for different purposes than OPPs.[112] PCI members store financial information to maintain financial accounts for their customers.[113] The types of information PCI members need to maintain financial accounts include the account holder's name, billing address, email address, and phone number, a record of every transaction made using the account, the account balance or credit limit.[114] Essentially PCI members collect and store information related to a customer's account to create a comprehensive financial record for the customer's account. Maintenance of a customer's account requires storing this data for the duration of the life of the account.[115]

While the PCI standard applies directly to members of the PCI, such as MasterCard and Visa, they apply indirectly to OPPs who are considered "service providers" to the Payment Card Industry.[116] The PCI standard applies indirectly to service providers by requiring that members only do

110. *Id* at ¶ 41.
111. *Id* at ¶ 40.
112. *See id.*
113. *See id.*
114. *See id.* at ¶¶ 40-41.
115. *See id.* ¶ 41.
116. *Id.* at ¶¶ 40, 45.

business with PCI-compliant service providers.[117] OPPs, however, only need financial information for the duration of processing a transaction. The data storage requirements under the PCI standard should not be applied to OPPs in the same way they are applied to PCI members, because it requires OPPs to store and maintain payment information beyond the time required to process a payment. Once the transaction is processed, the information is no longer needed by the OPP and OPPs should not be compelled to unnecessarily store and maintain sensitive payment information in order to do business with the PCI. For example, OPPs should instead destroy the payment information once the transaction is completed so that it is not vulnerable to hackers. Requiring PCI members and their service providers to store and maintain payment information duplicates the locations in which payment information can be found. The less locations payment information can be found, the less chance that information will be compromised. Therefore the standards applicable to PCI members should not unilaterally apply to their service providers because it creates greater risk of a data breach. Instead OPPs should be regulated by standards tailored to the business processes and needs of the OPP industry.[118]

III. DATA SECURITY REGULATION, OF OPPS NEEDS TO SHIFT AWAY FROM TERRITORIAL-BASED REGULATION AND TOWARDS INDUSTRY-BASED REGULATION

OPPs should adopt international standards through an industry specific code of conduct because it is a proven solution that meets the modern needs of global-based businesses and economies in ways that territorial-based regulation fails. The code should concern itself not with *where* data is processed but *why* it is processed and *how* it is protected.[119] First, international standards for data security should be based on the business needs of specific industries rather than the physical location of a piece of data to accurately reflect the global nature of modern commerce. Second an

117. *Id.* at ¶ 45.

118. "If sound rules for the use of personal data are not established and enforced, society as a whole will suffer because people will decline to engage in a range of different social interaction due to concerns about use of personal information." Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2089 (2004).

119. "So long as data is kept secure and processed in accordance with the controller's legal obligations and in keeping with its data subjects' reasonable expectations, it should be free to process that data wherever in the world it likes. Maintaining unrealistic restrictions on international data exports at best achieves little—organizations will do it any way using check-box solutions like model clauses—and, at worst, will adversely impact critical technology developments like the cloud." Phil Lee, *What a 21st Century Privacy Law Could – and Should - Achieve*, IAPP PRIVACY PERSPECTIVES, (Jan 20, 2014), https://www.privacyassociation.org/privacy_perspectives/post/what_a_21st_century_privacy_law_couldand_shouldachieve.

industry standard should be adopted through an industry code of conduct based on other successful self-regulation industry models.

A. Government Regulation is Ineffective Because it is Limited by its Territorial Jurisdiction, Which is Contrary to the Structure and Boundaries of the Internet Commerce Facilitated by OPPs. An Industry-Based Code of Conduct is the Solution to Today's Interconnected World

In the past territorial-based laws made sense because "norms of privacy in fact vary considerably from place to place, culture to culture, period to period."[120] The laws protecting individuals reasonably reflected the cultural values and norms of an individual's nationality. Political borders were a natural legal boundary because of the location-based nature of criminal activity before the Internet globalized society as well as crime. The rapid interconnection facilitated by the Internet globalized communities and globalized the way services are provided and business is conducted. "When self-regulation works effectively, it's a win for consumers and industry and regulators that have limited enforcement resources." [121] A regulation structure that accounts for the international nature of modern commerce is needed because "the boundaries of networks are defined by technological protocols and network infrastructure, not by physical geography."[122] Rather than being built on the basis of the culture and values of each country, the code should be built to meet the needs of the industry and be specific to the type of data being collected.[123]

B. OPPs Should Merge and Adapt Self-Regulation Models Employed by Other Industries to Construct an Industry Code of Conduct

In combination the three industry-based models, the FIPPs, the NAI Code of Conduct, and the PCI Data Security Standard can be used to create

120. Nissenbaum, *supra* note 611, at 155-56.

121. Katy Bachman, *Report: Ad Networks Adhering to Strict Privacy Guidelines* (Mar. 13, 2014) (quoting NAI CEO, Marc Groman), http://www.adweek.com/news/technology/report-ad-networks-adhering-strict-privacy-guidelines-156277.

122. RODITTI, *supra* note 199, at 2.

123. "[N]ational laws are often incompatible, they often impose explicit barriers to the international flow of personal data, and they are increasingly supplemented by state, provincial, and even local data protection laws. As a result, data protection has grown inconsistent and unpredictable, and increasingly burdensome to multinational commerce, trade, and information flows." Cate, *The Failure of the Fair Information Practice Principles*, *supra* note 33, at 367.

FIPP	Possible Interpretation[124]
Transparency	This principle is broadly applicable to all information collectors because it requires collectors to be transparent in their collection, use, dissemination, and maintenance practices. This transparency is often achieved through a company's privacy policy. OPPs should have a privacy policy that explains their privacy practices to the consumer and should be easily accessed for example through a link or displayed when requesting consumer information.
Individual Participation	This requirement is focused on the consent of the individual for the collection of the data. However, this is generally inapplicable to OPPs because consent of an individual is usually clear in a payment transaction. Consent of the individual providing the information is usually clear because the individual is providing the financial information specifically for the purpose of a transaction. In comparison, an individual browsing the web may be unaware that by conducting a Google search, the individual may be served advertisements based on the keywords they use in the search. OPPs should obtain consent for use of any information outside of the purpose of processing a transaction. See the Purpose Specification interpretation for more information.
Purpose Specification	The objective of this principle that the specific purpose(s) the information is being collected for should be articulated is also often achieved through a privacy policy. Additionally consent check boxes can be used for users to opt-in to allowing their data to be used for purposes beyond completing the transaction, for example being added to a mailing list to receive coupons from the seller.
Data Minimization	Data minimization is a significant principle that is not implemented as often as it should be. Ideally only the information necessary to accomplish the specified purpose should be collected and it should only be stored for the duration necessary to accomplish that specified purpose. OPPs would benefit from removing data from their systems after the necessary time to process a transaction.
Use Limitation	This principle is related to Purpose Specification. The difference is Purpose Specification is focused on providing notice to individuals about the purpose for which the information is being collected while Use Limitation addresses the actual use of the information. Information collected should only be used for the specific purpose(s) for which it is being collected and for which individuals have notice of its use. This is essential to a code of conduct for OPPs because they are required by United States law to only use the information collected to process the payment unless the individual manually consents to other uses for the information.
Data Quality & Integrity	This principle is core to the function of OPPs. The purpose of OPP data collection is to ensure the identity of the purchaser and the authenticity of the payment information. It is of high importance that the information OPPs collect is accurate, relevant, timely, and complete to the extent practicable.
Security	OPPs should protect collected information from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. In addition to a comprehensive security program, once again OPPs should

	only retain the information as long as necessary to complete the transaction.
Accountability & Auditing	This is the most important principle of the FIPPs because it provides the enforcement mechanism for the FIPPs. An OPP industry code of conduct should hold OPPs accountable for compliance with the code and OPPs should be audited to demonstrate compliance with the code's data protection requirements.

a comprehensive OPP industry code of conduct. There are three main goals for an OPP code of conduct. First, the code should be constructed with clearly defined principles specific to the OPP industry with additional commentary to explain the provisions of the code. Second, the code should be flexible enough to take advantage of advancements in technology. Finally, the code should be enforceable.[125]

1. An OPP code of conduct should have clearly defined principles specific to the OPP industry

The FIPPs are useful as a starting place to construct a code of conduct, but are broad and require interpretation based on a comprehensive understanding of OPP business processes. Using the FIPPs to help design the code can illuminate business processes that can also be helpful in protecting information, such as limiting the amount of data necessary for those processes and removing any unnecessary information once the transaction is complete. For example once the financial information has been verified the CVV may no longer be needed and once the transaction has been fully processed the remaining financial information is no longer needed. The following possible interpretation of the FIPPs serves as an example of how the FIPPs may be adapted to the OPP industry and the general applicability of each FIPP. The code created by the OPP industry should expand on and amend the suggested interpretations as necessary to reflect OPP business processes. The code should contain additional commentary to explain the

124. Interpretations of FIPPs for the OPP industry adapted from Privacy Policy Guidance Memorandum, *supra* note 923, at 3-4.

125. These three main goals for an OPP code of conduct track with the six critical elements for the success of a self-regulatory code identified by Ira S. Rubenstein: (1) efficiency - achieving regulatory objectives at the lowest attainable cost; (2) openness - whether the system allows public stakeholders to play a role in the development of the code – and transparency - regulatory system's ability to promulgate industry normative standards and provide information about the performance of member companies in meeting those standards; (3) completeness -code addresses all relevant aspects of standards governing industry practices; (4) Free rider problems – prevents members from enjoying the benefits of the program without having to meet its obligations; (5) oversight and enforcement – consumer complaint mechanism, routine audits, and consequences for failure to comply; and (6) Use of second-generation design features – reward members for superior performance. Rubenstein, *supra* note 599, at 381-83:

intent and provisions of the code, and to provide examples of ways members can meet the code.[126]

OPPs additionally should use the institutional knowledge about financial services offered by the PCI Data Security Standard to develop an OPP industry-specific code of conduct. However, the requirements of the PCI Data Security Standard should not apply directly to OPPs because it was designed with the business processes of bank card companies such as Visa and MasterCard in mind.[127] Instead the standards should be adapted to reflect the business processes of OPPs. Banks for example need to store information for longer periods of time – as long as a customer holds an account – and OPPs only need the information for as long as necessary to complete a given transaction. Some of that information such as the CVV value can be purged in the initial stages of that transaction once it has served its purpose.

2. An OPP code of conduct should be flexible enough to take advantage of advancements in technology

The code should include technical recommendations on equipment and practices that will help companies meet the code and should be flexible enough to take advantage of advancements in technology. Technological solutions can also help ensure industry compliance. For example, NAI has a tool that crawls the web to make sure companies are complying with their code.[128] Technical mechanisms similar to NAI's web tool can be used to perform daily auditing tasks and boost compliance with a code of conduct.[129]

In addition, the code should have technical standards to ensure the security and protection of information. Technology is rapidly advancing and data security standards that were previously thought to be secure are sometimes discovered to have flaws.[130] A code needs to be adaptable to these changes. For example, encryption technology could be used to simplify the payment authentication process and provide additional protections to

126. 2013 NAI Code of Conduct, at 9 (2013), http://www.networkadvertising.org/2013_Principles.pdf (last visited Mar. 5, 2014).

127. McCarthy, *supra* note 14, at ¶ 42.

128. About the NAI, http://www.networkadvertising.org/about-nai/about-nai (last visited Mar. 5, 2014).

129. Spiekermann & Cranor, *supra* note 544, at 73.

130. For example the SSL encryption key used to encrypt websites was recently discovered to have a flaw. Nicole Perlroth, *Experts Find a Door Ajar in an Internet Security Method Thought Safe*, NEW YORK TIMES, Apr. 8 2014, http://bits.blogs.nytimes.com/2014/04/08/flaw-found-in-key-method-for-protecting-data-on-the-internet.

consumer information. Further technological developments could allow for payment authentication with limited identifying information.[131] The industry code of conduct should be designed so it can be consistently revised to keep pace with such technological advancements.[132]

3. An OPP code of conduct should be enforceable

For the code to be effective, it needs to be enforceable and provide accountability for compliance with its provisions. A code is enforceable when it is enforced by a single enforcement body to ensure uniform interpretation of the code and when it has multiple methods of enforcement that analyze, track, and enforce compliance with the code.

First, the enforcement structure should include multiple methods of enforcement, because not all methods of enforcement are effective nor is any one method effective on its own. For example, codes that are enforced only when a company receives a complaint, investigates the complaint and finds the complaint valid require knowledge by consumers of the code and assertive action by those consumers.[133] This model lacks an auditing process for compliance. Audits for compliance should be conducted at regular intervals. The NAI code of conduct in particular demonstrates the impact a self-imposed code with real teeth can have as compared to a code created as a public relations move or window-dressing. A significant part of the success of the NAI code of conduct is its yearly compliance audits for its members.[134] Each year the NAI conducts a compliance audit of all of its members' activities and publicly publishes a compliance report.[135]

While useable as a model, NAI's code, like the PCI Data Security Standard, is not directly applicable to the OPP industry. NAI members are online advertisers that usually collect non-sensitive, anonymous data, while OPPs collect sensitive financial information. Therefore because NAI members and OPPs collect different types of information codes of conduct for each industry should reflect those differences.

Moreover, the goals of data collection for advertisers differ from the goals of OPPs. Advertisers are less concerned about actual identification of the consumer (by name, etc.) and more that the consumer is receiving

131. "By using anonymous or pseudonymous credentials that attest to the relevant fact rather than to a person's identity, secure transactions can take place outside the user sphere without the transfer of personal information." Spiekermann & Cranor, *supra* note 544, at 74.

132. "System designers should consider the extent to which users can remain unidentified during electronic transactions." Spiekermann & Cranor, *supra* note 544, at 74.

133. *NAI's Marc Groman on Setting and Keeping High Standards in Online Advertising*, THE MAKEGOOD (Jan. 6, 2014), http://www.the-makegood.com/2014/01/06/nais-marc-groman-on-setting-and-keeping-high-standards-in-online-advertising/.

134 . NETWORK ADVERTISING INITIATIVE, 2013 ANNUAL COMPLIANCE REPORT http://www.networkadvertising.org/2013_NAI_Compliance_Report.pdf.

135. *Id.*

advertising that reflects his or her interests. For OPPs the goal is exactly the opposite, it is already clear what the consumer wants – the item in his or her digital shopping cart – the question is whether the consumer is who he or she says they are and is therefore authorized to use the method of payment they offer. Consequently the focus in data collection for OPPs is informational accuracy, identification, and verification.

An additional difference is that consent is a large issue with advertisers, whereas consent in payment processing is usually apparent because a user provides consent for the information to be used to process the payment at the time of purchase.[136] A code created specifically for OPPs would need to reflect these differences with heightened data security standards to match the heightened sensitivity of the financial information collected.[137] Privacy solutions are not one-size fits all[138] and solutions should reflect the context and content of the information involved.[139]

IV. CONCLUSION

Online payment processors are specifically vulnerable to cyber-attacks because they collect personally identifiable information and sensitive financial information to facilitate online transactions. The regulation needs to shift from a territorial based model to an industry-based model that accounts for individual businesses' needs and the types of information they collect and maintain.

This objective is best achieved through a self-regulated industry code of conduct. The code of conduct should be based in sound principles, such as the FIPPS, adapted to the OPP industry, should be flexible to adapt to emerging technologies and varying business practices, and should be enforceable through a comprehensive enforcement program.

---

136. However making sure the information collected to process a payment is limited to that purpose is often confusing for consumers. For example, when after a purchase a consumer starts receiving advertising emails from the same company it made the purchase from.

137. "Different categories of data present different levels of risk." 2013 NAI Code of Conduct, *supra* note 1266, at 9; *see also* Bruce Morris, *Responsible Data Management and Maintaining Consumer Trust*, NAI (Apr. 17, 2014), http://www.networkadvertising.org/blog/responsible-data-management-and-maintaining-consumer-trust ("NAI Code also has higher standards for sensitive information such as financial data that can result in identity theft…").

138. 2013 NAI Code of Conduct, *supra* note 1266, at 3; FTC REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, 19-20 (2012); WHITE HOUSE REPORT, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 9 (2012).

139. *Id.* at 18.