EDITOR'S NOTE

Welcome to the second issue of Volume 70 of the *Federal Communications Law Journal* ("*Journal*"), the official journal of the Federal Communications Bar Association. In March 2018, the *Journal* successfully held its 2nd Annual Symposium at The George Washington University Law School. Lawyers from the government, private and public sectors had lively discussions on the issue of how regulation over communications technology should change as new types of technology add jurisdictional complications. Along those lines, this Annual Symposium issue explores the theme of regulation and reform.

The first article of this issue is penned by John W. Mayo, a Professor of Economics, Business and Public Policy, in the McDonough School of Business at Georgetown University. Professor Mayo examines various avenues for regulatory reform, as he sees the importance of regulation in accelerating the deployment of next-generation broadband networks.

The first Student Note is written by Donald Crowell, who suggests that law enforcement's access to content-based information should be made more difficult, that provisions in the Stored Communications Act should be revised, and that the NTIA should be given the authority to define and regulate electronic communications providers and remote communication service providers. The second Student Note is written by Michael Farr, who seeks to correct what he sees as the FCC's abuse of transaction review authority by subjecting such transactions ending in voluntary commitments to judicial review instead. In the last Student Note, Alison Cheperdak juxtaposes the privacy rules set out by the FCC and the FTC, and argues that giving the FTC complete jurisdiction over Internet data security and preempting state laws that conflict with FTC's policies would effectively serve the interests of both the industry and the consumer.

Last but not least, the *Journal* thanks the Annual Symposium panelists who submitted short articles for this issue. From a proposal to construct a national first responder communications infrastructure, to an examination of the authoritative tensions among the federal government, state legislatures, and the industry, five authors have generously contributed their perspectives on the topic of telecommunications sovereignty.

I believe this issue captures the essence of a student-run journal with a professional edge, as it is not only packed with fresh and diverse ideas on a wide array of relevant topics, but the articles are also varied in length, style, and written by authors at different stages in their professional careers. As always, we welcome your feedback or questions to fclj@law.gwu.edu. Please direct article submissions to fcljarticles@law.gwu.edu. This issue and our archive will be available at www.fclj.org.

Jane Lee
Editor-in-Chief

FEDERAL COMMUNICATIONS LAW JOURNAL

GW | LAW

FCBA
FEDERAL COMMUNICATIONS BAR ASSOCIATION

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 United States, 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 Street NW, Suite LL-020, Washington, DC 20052. The *Journal* can be reached at fclj@law.gwu.edu, and any submissions for publication consideration may be directed to fcljarticles@law.gwu.edu. Address all correspondence with the FCBA to the Federal Communications Bar Association, 1020 19th Street NW, Suite 325, Washington, DC 20036-6101.

Subscriptions: Subscriptions are $30 per year (domestic), $40 per year (Canada and Mexico), and $50 per year (international). Subscriptions are to be paid in US dollars, and are only accepted on a per-volume basis, starting with the first issue. All subscriptions will be automatically renewed unless the subscriber provides timely notice of cancellation. Address changes must be made at least one month before publication date, and please provide the old address or an old mailing label. Please direct all requests for address changes or other subscription-related questions to the journal via email at 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* (20th ed., 2015), 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 70 FED. COMM. L.J. ___ (2018).

FEDERAL COMMUNICATIONS LAW JOURNAL

GW LAW

VOLUME 70 ISSUE 2

MAY 2018

FCBA FEDERAL COMMUNICATIONS BAR ASSOCIATION

ARTICLES

Although the United States is deeply divided ideologically, and this divide nominally may seem to halt opportunity for policy advances, this need not necessarily be the case. Notwithstanding our ideological differences, a number of practical opportunities for policymakers to improve economic welfare have emerged, about which there is considerable agreement if not complete political consensus, that allow policy progress. These opportunities create a potential path for practicality to forge agreement even in the face of widespread ideological discord across American society.

This basic thesis is no more evident than in the set of infrastructure industries that policymakers across the political spectrum have identified as crucial for U.S. competitiveness in the 21st century. As such, this paper focuses on broadband technologies (both wired and wireless), which policymakers of all political stripes have identified as crucial for economic growth. To make its point, this paper identifies: (1) the practical, as opposed to ideological, case for regulatory reform in the broadband sector; and (2) a number of available measures that create opportunities for meaningful and beneficial regulatory reform.

NOTES

Modern technology is rapidly changing the way society interacts and collaborates. Cloud technology is an integral part of this evolution and is being integrated into all kinds of computer-based platforms to provide users with functionality and convenience. To date, Fourth Amendment jurisprudence has failed to keep up with the use of modern technology, and statutes, such as the Electronic Communications Privacy Act ("ECPA") and the Stored Communications Act ("SCA") continue to infringe on the rights that citizens hold in their digital property.

The U.S. Circuit Courts of Appeal are split on the application of the Fourth Amendment to digital communications. While the Sixth Circuit in *United States v. Warshak* found that individuals did have an expectation of privacy in their electronic communications, other circuits, including the Eleventh Circuit in *Rehberg v. Paulk*, have applied the Voluntary Disclosure Doctrine to determine that no expectation exists. Due to the courts' failure to reach a consensus in this area, the ECPA and SCA continue to fail to protect the rights of individuals who choose to store their personal files, photos, and other information in the Cloud. Further, the Supreme Court's holding in *California v. Riley*, that police officials did not have a right to search an individual's cell phone incident to an arrest, provided both clarity and ambiguity as the Court limited its holding to the factual context at-hand in the case.

Reform is needed at both legislative and judicial levels. The most crucial of these reforms is raising the threshold for law enforcement's access to content-based information to require a warrant based on probable cause. Other provisions of the SCA also need to be replaced and amended, including the 180-day distinction and the 90-day renewable delay notice. Additionally, a federal agency, such as the National Telecommunications & Information Administration ("NTIA"), should be given the authority to regulate and define which entities are considered electronic communications providers and remote communication service providers under the SCA. Granting this authority will allow flexibility in keeping up with the changing landscape of communications technologies, which, as seen with the outdated applicability of the SCA to modern technology, is something that is indisputably needed.

Industry can also assist with making warrant and non-warrant requests worthless by developing stronger encryption technologies and standards, as well as encrypting customer Cloud data such that companies cannot access it themselves. This solution would be less viable than others simply due to economic costs associated with not having access to customer data, as well as the likely possibility that the government would find a way to gain access to encrypted data anyway.

Brace Yourself, Voluntary Commitments Are Coming: An Analysis of the FCC's Transaction Review

The role of the Federal Communications Commission ("FCC") in transaction review is ever expanding. Under its "public interest standard," the FCC has authority to deny applications or approve transactions involving licenses, subject to conditions. These conditions are made in the form of "voluntary commitments." Parties to the transaction are left without a choice but to accept these voluntary commitments in order to avoid denial of a deal. Often, these commitments are unrelated or ancillary at best to the transaction at hand. This Note asserts that the FCC uses its transaction review authority to engage in de facto rulemaking, creating policy outside the confines of the Administrative Procedure Act and its organic statute. Such a practice wholly offends the checks and balances enshrined in our Constitution and represents apparent violations of the non-delegation doctrine. This Note thus argues that in order to curb these abuses, transactions ending in voluntary commitments are final agency actions that must be subject to judicial review.

Will Ideology Block Opportunity? Regulatory Reform in the Infrastructure Industries

John W. Mayo *

TABLE OF CONTENTS

* Professor of Economics, Business and Public Policy, McDonough School of Business, Georgetown University, and Executive Director of the Georgetown Center for Business and Public Policy.

I. INTRODUCTION

It is no secret that the United States is politically fractured. Citizens have increasingly retreated or have been drawn to information streams that identify different profound problems facing the country and which offer vastly different solutions.[1] This tendency creates and reinforces knee-jerk resistance to policy proposals from the opposition political camp. Democrats often reflexively reject Republican proposals, and Republicans similarly and with equal speed reject out-of-hand policy proposals offered by Democrats.

In some cases, this political polarization is based on fundamental and substantive grounds that stem from profound ideological differences. In such cases, proposals for policy change fail to gain traction or end in stalemates.[2] Even in the rare instances where the roughshod politics of the stronger party prevail to advance a policy, the results remain vulnerable to the likelihood of reversal in the event that the influence of the politically stronger group falters.[3]

While this ideological standoff is disheartening, it need not bring policy progress to a halt. Indeed, in the realm of regulatory reform, a number of practical opportunities exist to improve economic welfare, and careful consideration of those opportunities points toward considerable agreement, if not consensus among policymakers of all political stripes. These opportunities create a potential path for practicality to forge agreement, even in the face of widespread ideological discord across American society.

This basic thesis is no more evident than in the set of infrastructure industries that policymakers across the political spectrum have identified as crucial for U.S. competitiveness in the 21st century. As a case in point, this paper will focus on broadband technologies (both wired and wireless), which policymakers of all political stripes have identified as crucial for

1. *See generally* Jessica Taylor, *Republicans And Democrats Don't Agree, Or Like Each Other — And It's Worse Than Ever*, NAT'L PUB. RADIO, INC. (Oct. 5, 2017), https://www.npr.org/2017/10/05/555685136/republicans-and-democrats-dont-agree-dont-like-each-other-and-its-worst-than-eve.

2. Among many examples, consider the lack of legislative progress on gun control and immigration in recent years.

3. Consider, for instance the political back-and forth over so-called net neutrality at the Federal Communications Commission in recent years that has been prompted by changes in the majority position of either Republicans or Democrats.

economic growth.[4] In the specific case of broadband, there is little to no disagreement that numerous regulatory policies touch upon, and may be constraining, the deployment and adoption of broadband in the United States.[5]

II. THE PRACTICAL NEED FOR REGULATORY REFORM IN THE BROADBAND COMMUNICATIONS SECTOR

Any discussion of forward-looking regulatory policies governing broadband infrastructure should begin with three widely agreed to premises. First, broadband deployment enhances Americans' personal lives and stimulates productivity and economic growth.[6] Second, next-generation broadband networks will require massive capital investments.[7] Third, the

4. In political discussions of the policy imperatives for the broadband sector, some have emphasized the need to remove artificial impediments to greater deployment while others have tended to emphasize the need for affordable broadband. *See* John Eggerton, *House Digs Into Broadband Infrastructure*, MULTICHANNEL NEWS (Mar. 21, 2017), http://www.multichannel.com/news/telco-tv/house-digs-broadband-infrastructure/411648 [https://perma.cc/B3CP-LXAT]. While creating a nominal difference, these different points of emphasis are, from an economic perspective, not distinct. Specifically, policy measures designed to enhance the supply of broadband will inevitably put downward pressure on price, which in turn, promotes the affordability of broadband services. To the extent that even with generally affordable broadband, some households may find broadband too expensive to purchase. An efficient policy of targeted subsidies to enhance demand (such as through the Connect America Program) can supplement policies designed to enhance supply.

5. Numerous policy dockets are in progress at the Federal Communications Commission that address the potential impacts of regulatory policies on the deployment and adoption of broadband. *See generally*, *ECFS Most Active Proceedings*, FCC, https://www.fcc.gov/rulemaking/most-active-proceedings (last visited Apr. 18, 2018).

6. *See, e.g.*, ACCENTURESTRATEGY, SMART CITIES: HOW 5G CAN HELP MUNICIPALITIES BECOME MORE VIBRANT 1 (2017), https://www.ctia.org/docs/default-source/default-document-library/how-5g-can-help-municipalities-become-vibrant-smart-cities-accenture.pdf; *see also* David Sunding, Martha Rogers & Coleman Bazelon, The Farmer and the Data: How Wireless Technology is Transforming Water Use in Agriculture, at 2 (April 2016), http://files.brattle.com/files/7336_the_farmer_and_the_data_-_how_wireless_technology_is_transforming_water_use_in_agriculture.pdf (showing how farmers can leverage advanced wireless technology to preserve resources in droughts and optimize watering levels); JEFFREY T. MACHER, JOHN W. MAYO & OLGA UKHANEVA, DOES THE INTERNET IMPROVE HEALTH BEHAVIORS AND OUTCOMES? EVIDENCE FROM THE NATIONAL HEALTH INTERVIEW SURVEY (2016), https://ssrn.com/abstract=2756388 (showing the effect of the internet on health behavior and outcomes).

7. According to USTelecom, total broadband industry capital investments for wireline, wireless, and cable totaled $1.6 trillion between 1996 and 2016. *See* PATRICK BROGAN, BROADBAND INVESTMENT CONTINUES TRENDING DOWN IN 2016, at 1 (2017), https://www.ustelecom.org/sites/default/files/documents/Broadband%20Investment%20Trending%20Down%20in%202016.pdf. In 2016, broadband investments totaled $76 billion with 43% of spending by the wireless industry, 35% by the wireline industry, and 22% by cable. Looking forward, Accenture Strategy estimates that telecommunications firms may invest $275 billion over the next seven years to deploy next generation wireless broadband facilities. *See* ACCENTURESTRATEGY, *supra* note 6, at 1.

investments necessary to produce widely-deployed next-generation broadband infrastructure in the United States will be provided almost exclusively by the private sector.[8]

Given these basic premises, regulatory policies governing the broadband sector take on additional importance. Specifically, in addition to the traditional role of consumer protections afforded by regulation, it is essential that modern regulation be fashioned to complement and accelerate the deployment of next-generation broadband networks. Indeed, with the rapid growth in demand for mobile and fixed broadband services, the economic fact is that failure to enable infrastructure buildout will produce an array of maladies ranging from elevated prices to reduced quality. These realities, in turn, require a careful review of the regulatory structure governing broadband communications, especially regulations pertaining to broadband infrastructure. It is important to note, however, that such a review and consequent reforms should be driven not by the ideological distaste for regulation so often championed in political discourse, but rather by the practical possibilities that regulatory reforms could accelerate America's efforts to deploy and adopt 21st century broadband. Both individuals' personal lives and the United States' competitiveness would benefit from such reforms.

The potential for practical regulatory reform is especially promising in the modern broadband sector. This is for several reasons. First, the regulations governing the communications sector were largely established within an environment of monopolistic provision of communications services, which starkly differ from the 2018 marketplace.[9] Through the passage of the Telecommunications Act of 1996 ("Telecommunications Act"), the telecommunications industry has evolved rapidly into an

8. Despite the widespread embrace of a public infrastructure initiative to contribute to the deployment of next-generation broadband infrastructure, it is apparent that the Trump Administration will not allot substantial federal funds toward this goal: "Providing more Federal funding, on its own, is not the solution to our infrastructure challenges. Rather, we will work to fix underlying incentives, procedures, and policies to spur better infrastructure decisions and outcomes, across a range of sectors" *See* OFFICE OF MGMT. & BUDGET, FACT SHEET 2018 BUDGET: INFRASTRUCTURE INITIATIVE 1 (2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/fact_sheets/2018%20Budget%20Fact%20Sheet_Infrastructure%20Initiative.pdf. For a more general discussion of the fiscal challenges facing public funding of infrastructure projects, *see Improving Infrastructure Outcomes through Better Capital Allocation*, MCKINSEY & CO. (Nov. 2017), https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/improving-infrastructure-outcomes-through-better-capital-allocation?cid=other-eml-alt-mip-mck-oth-1711.

9. *See The History of the Federal Communications Commission (FCC)*, MITEL, https://www.shoretel.com/history-federal-communications-commission-fcc (last visited Apr. 18, 2018).

ecosystem in which effective competition is the norm.[10] Competition among broadband providers has increasingly taken on characteristics in which firms race to deploy next-generation facilities that have more bandwidth, and provide higher quality at greater speeds and at lower prices.[11] In such a Schumpeterian environment, it is especially important to be aware of the potential for existing regulations to slow innovation and the time-to-market deployments of next-gen broadband facilities.[12] More fundamentally, where consumers are protected by competition (and the general protections afforded by the United States' agencies enforcing competition policy, such as the Federal Trade Commission[13]), some regulations that would otherwise be necessary for consumer protection are no longer required.

Second, in some cases, regulations that govern the communications sector were designed to be congruent with particular point-in-time technologies.[14] But the technologies that provide modern communications are stunningly different than those employed only a few years ago.[15, 16] Consequently, it would seem incontrovertible that technology-specific regulations that were established to govern the wireline provision of plain-old-telephone service ("POTS") are unlikely to advance economic welfare in a world in which consumers increasingly turn to wireless smartphones to handle an array of voice, data, and video communications services. Similarly, arduous regulations governing large macro-cell antennas to support cellular service become deterrents to the rapid deployment of much more densely-packed, but substantially smaller, micro-cell antennas that are

10. For a detailed discussion of the evolution of "effective competition" in general and in the industries governed by the Federal Communications Commission, *see* Amanda B. Delp & John W. Mayo, *The Evolution of 'Competition': Lessons for 21st Century Telecommunications Policy*, 50 REV. OF INDUST. ORG. 393-416 (2017).

11. *See Hearing on "Investing in America's Broadband Infrastructure: Exploring Ways to Reduce Barriers to Deployment" Before the S. Comm. on Commerce, Science & Transportation*, 115th Cong. (2017) (Testimony of Larry Downes), https://www.commerce.senate.gov/public/index.cfm/2017/5/investing-in-america-s-broadband-infrastructure-exploring-ways-to-reduce-barriers-to-deployment.

12. For a background discussion of Schumpeterian competition, *see* HERBERT HOVENKAMP, SCHUMPETERIAN COMPETITION AND ANTITRUST 273 (2008), https://www.competitionpolicyinternational.com/assets/0d358061e11f2708ad9d62634c6c40ad/Hovenkamp_webwcover.pdf.

13. *See generally Guide to Antitrust Laws*, FTC https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws (last visited Apr. 18, 2018).

14. *See Communications Act of 1934*, FCC, https://transition.fcc.gov/Reports/1934new.pdf (last visited Apr. 18, 2018).

15. See *Tech Transitions: Network Upgrades That May Affect Your Service*, FCC https://www.dailydot.com/layer8/what-is-title-ii-net-neutrality-fcc/ (last visited Apr. 18, 2018).

16. *See generally Fact Sheet*, PEW RES. CTR., http://www.pewinternet.org/fact-sheet/mobile/ (last visited Apr. 18, 2018) (notes in 2018 "95% of Americans now own a cellphone of some kind, and 77% of Americans own a smartphone […] up from just 35% in […] 2011").

required to provide next-generation 5G wireless services.[17] Such regulations are ripe for reform.

Third, given the overwhelming need for capital investments to expand and enhance the broadband platform in the United States, regulations that retard investment also become candidates for reform. In some cases, the investment-retarding effects of regulation may be offset by countervailing and significant consumer protections afforded by the existing regulation. In other cases, however, regulatory reforms may be identified that can ensure consumer protections while removing the investment-deterring effects of the regulation. It is important to note that these considerations provide a compelling practical basis to review extant regulations with an eye toward preserving consumer protections, while simultaneously promoting private sector investment in this crucial sector of the economy. Importantly, by circumventing ideologically-driven policy actions, this more practical approach creates the real possibility of policy progress and agreement among political parties who may find themselves ideologically in stark disagreement.

Evidence of such bipartisan potential abounds at the city, state, and federal levels of government, as well as among federal regulators. A number of cities have embraced the need to adopt rules and regulations that accelerate and complement the private sector's push to accelerate broadband deployment. For example, the city of Chicago has adopted a "Tech Plan" that encourages the development of "world-class broadband infrastructure and increased digital access across the city" and has adopted initiatives to "foster a regulatory and policy-based environment in which businesses can flourish and grow by reviewing current business-related requirements and processes, such as permits and procurement, updating where appropriate."[18]

At the state level, numerous states in bipartisan efforts have facilitated the adoption of legislation designed to remove archaic regulatory barriers to streamlining the deployment of fixed and mobile broadband. For example, in August 2017, Delaware adopted the Advanced Wireless Infrastructure Investment Act to accelerate investment in mobile broadband infrastructure.[19] The bill had 11 Democrat sponsors and 10 Republican sponsors, passed both the Delaware legislative chambers with overwhelming

17. *See generally* Accelerating Wireless Broadband Deployment by Removing Barriers to Infrastructure Investment, 82 Fed. Reg. 21761, https://www.federalregister.gov/documents/2017/05/10/2017-09431/accelerating-wireless-broadband-deployment-by-removing-barriers-to-infrastructure-investment.

18. See THE CITY OF CHICAGO TECHNOLOGY PLAN 5, 16 (2013), http://techplan.cityofchicago.org/wp-content/uploads/2013/09/cityofchicago-techplan.pdf. While cities like Chicago have been proactive in reforming local regulations that are acting to impede the deployment of next-generation broadband facilities, other localities have to this point failed to act. Section III below addresses some of practical steps that can be taken to remove these impediments.

19. H.R. 189, 149th Gen. Ass., (De. 2017) codified as DEL. CODE ANN tit. 17, §§1601-1614 (2017).

bipartisan majorities, and was signed into law by its Democrat governor, John Carney.[20] As detailed in the next section, bipartisan bills in both the United States House of Representatives and the Senate are making their way through the legislative process. These bills do not promote removal of existing regulations on ideological grounds, but instead are designed to remove practical impediments that currently act to retard the deployment of highly sought after broadband services.

Similarly, agreement exists among federal regulators that streamlining deployment and removing bottlenecks is central to efforts to promote affordability for consumers. For example, Democrat Federal Communications Commissioner Mignon Clyburn has observed that a "[l]ack of affordability remains one of the largest barriers to connected communities. . . . Streamlining deployment is central to this effort. We must ensure that all providers are able to deploy and upgrade their infrastructure at the lowest costs and quickest pace."[21] Similarly, Chairman Ajit Pai, the Republican head of the Federal Communications Commission ("FCC") has noted that:

> [W]e have to focus on bringing high-speed broadband to economically deprived areas. And to do that, we must recognize that deploying broadband isn't easy. The Internet isn't an abstraction. It's a physical network of networks that requires massive investment to deploy and constant adjustment to manage. Internet service providers (ISPs) must trench conduit, lay cable, install electronics, attach antennas, and stitch together a seamless communications network from aging copper and brand-new fiber, legacy switches and modern routers.[22]

Finally, beyond these compelling economic motivations for regulatory reform to stimulate the expansion of broadband infrastructure in the United States, the federal legislature similarly compels this review and reform, specifically when states' actions threaten the mission of the Commission. For example, the Telecommunications Act provides that "no state or local regulation … may prohibit or have the effect of prohibiting the ability of any entity to provide any interstate or intrastate telecommunications service."[23] The statute goes on to state that if the FCC determines that "a State or local

---

20. *See generally* Delaware House Bill 189, https://legiscan.com/DE/bill/HB189/2017 [https://perma.cc/N8GQ-T35S].

21. *See* Remarks of FCC Commissioner at the #Solutions2020 Policy Forum, Georgetown University Law Center, at 4 (Oct. 19, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DOC-341824A1.pdf.

22. *See* Remarks of FCC Commissioner Ajit Pai at the Brandery "A Digital Empowerment Agenda" Cincinnati, Ohio (Sept. 13, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DOC-341210A1.pdf.

23. *See* 47 U.S.C. § 253 (a).

government has permitted or imposed any statute, regulation, or legal requirement that [acts to prohibit or has the effect of prohibiting the ability of firms to provide interstate or intrastate services], the Commission shall preempt the enforcement of such statute, regulation, or legal requirement to the extent necessary to correct such violation or inconsistency."[24]

Together both practical economic necessity and statutory authority compel federal regulators to assess federal, state, and local regulations. These regulations may act to retard the ability of broadband service providers to expand services and capabilities. When such regulations can be identified they become practical opportunities for otherwise politically disparate parties to work collectively to advance economic welfare.

III. LOW HANGING FRUIT

The practical case for review and reform of existing regulations to remove barriers to efficient infrastructure investment is not new. Indeed, as early as the scrutiny offered in the National Broadband Plan of 2010, it was observed that gaining regulatory approval to access rights-of-way "is often a difficult and time-consuming process that discourages private investment."[25] To mitigate this barrier, the FCC suggested that "government should take steps to improve utilization of existing infrastructure to ensure that network providers have easier access to poles, conduits, ducts and rights-of-way" as "[t]he cost of deploying a broadband network depends significantly on the costs that service providers incur to access [them] on public and private lands."[26]

Yet while the need for this review and reform is not new, the overwhelming growth in demand for broadband services creates situations in which local and state regulations retard the ability of broadband firms to efficiently respond to that demand through broadband investment and infrastructure growth. This creates the opportunity for practical policy solutions to reduce or remove economic impediments to expansion.

Consider, for example, the Broadband Conduit Deployment Act of 2018.[27] This bill advances the cause of accelerating broadband deployment and adoption by requiring states to evaluate the need for broadband conduits as they expand their highway systems.[28] In particular, the bill requires state governments, in concert with broadband firms, to evaluate any anticipated need within 15 years for broadband conduit deployment beneath the state's

24. *See* 47 U.S.C. § 253 (d).

25. See FCC, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 109 (2010), https://www.fcc.gov/general/national-broadband-plan [https://perma.cc/D35C-QJUZ].

26. *Id.* at 109.

27. Broadband Conduit Deployment Act of 2018, H.R. 4800, 115th Cong. (2nd Sess. 2018).

28. *Id.* at § 331(a)(1).

new and expansion highway projects.[29] If the evaluation reveals an anticipated need for additional broadband deployment, the bill requires that the conduit necessary to support that broadband deployment be installed at the time of construction.[30] By establishing this "dig-once" policy, the cost of broadband deployment will fall precipitously. While the precise cost savings associated with dig-once deployment depends on a variety of factors, including population density and the topography of the relevant terrain, it has been estimated that the cost savings from a coordination of conduit and fiber installation with highway projects ranges from 25-33%, with higher cost savings in more densely parts of urban areas.[31] Cost savings in rural areas, while lower, have been estimated to be in excess of 15%.[32]

Additionally, this dig-once legislation not only seeks to promote the speedy deployment of broadband infrastructure, but also has the by-product benefit of minimizing traffic disruptions that would necessarily occur in the event of multiple trenching efforts. The practical, cost-saving reform also blunts ideologically-driven fears that policymakers seeking to facilitate deployment are turning a blind eye to the important goal of promoting competition by locking in monopolies.[33] Specifically, by explicitly compelling that conduit be provided "on a competitively neutral and non-discriminatory basis" the legislation would protect competition.[34] Finally, consistent with sound economic principles, the bill requires that access to conduit be at a charge not to exceed a cost-based rate."[35] This legislation provides exactly the sort of practical reform that is necessary to accelerate the deployment of broadband. And importantly, this practical reform is supported by members of both political parties.[36]

Just as the Broadband Conduit Deployment Act of 2018 addresses the deployment of wireline broadband facilities, the "Making Opportunities for Broadband Investment and Limiting Excessive and Needless Obstacles to Wireless Act" ("MOBILE NOW Act") seeks to facilitate deployment of mobile broadband facilities.[37] This bipartisan bill[38] contains a variety of

29. *Id*. at § 331(a)(1-3).
30. *Id*. at § 331(a)(3)-(b)(3).
31. *See* GAO - 12-687R, BROADBAND CONDUIT DEPLOYMENT 5 (2012).
32. *Id*.
33. For an example of such fears, *see generally* Susan Crawford, *Handcuffing Cities to Help Telcom Giants*, BACKCHANNEL (Mar. 29, 2017), https://www.wired.com/2017/03/handcuffing-cities-to-help-telecom-giants.
34. Broadband Conduit Deployment Act of 2018, H.R. 4800, 115th Cong. § 331(f) (2nd Sess. 2018).
35. *Id*.
36. *See* Jon Brodkin, *'Dig once' bill could bring fiber internet to much of the US*, ARS TECHNICA (Mar. 22, 2017), https://arstechnica.com/information-technology/2017/03/nationwide-fiber-proposed-law-could-add-broadband-to-road-projects.
37. *See* MOBILE Now Act, S. 19, 115th Cong. § 7 (2017) https://www.congress.gov/115/bills/s19/BILLS-115s19es.pdf.

common-sense practical measures designed to facilitate the deployment of infrastructure necessary to deploy mobile broadband services. For instance, the bill addresses buildings owned by the Federal Government in which parties seek to install, construct, modify, or maintain a communications facility installation.[39] In these situations, the bill requires that federal agencies develop a common application for entities applying for easements, rights-of-way, and leases and requires that applications be approved or denied within 270 days of filing.[40] The bill also requires the states to identify a broadband utility coordinator who would be tasked with "facilitating the broadband infrastructure right-of-way efforts within the State."[41] Additionally, the bill addressees the glaring need for additional spectrum to be made available to support the rapidly growing demand for mobile voice, data, and video services by directing the National Telecommunications and Information Administration and the FCC to make at least 255 megahertz of new spectrum available for licensed and unlicensed use by 2020.[42] Quite apart from ideological differences among policymakers, the practical proposals in the bill are widely appealing, with the bill passing the Senate on a unanimous consent vote in August 2017.[43]

Two new legislatively-based regulatory reform measures have recently emerged, both of which are designed to remove existing regulatory impediments to rapid broadband deployment. In October 2017, Senators Wicker (R-MS) and Masto (D-NV) introduced the Streamlining Permitting to Enable Efficient Deployment of Broadband Act of 2017 Act (SPEED Act).[44] This Act seeks to fast-track the deployment of next-generation broadband technologies by exempting communications providers from duplicative environmental and historical reviews.[45] The bill also would exempt certain new small-cell facilities from environmental review.[46] A complementary bipartisan effort led by Senators Thune (R-SD) and Schatz

38. The bill was introduced by Senator Thune (R-South Dakota) and Bill Nelson (D-Florida).

39. *See* MOBILE Now Act, S. 19, 115th Cong. § 7 (2017) https://www.congress.gov/115/bills/s19/BILLS-115s19es.pdf.

40. *Id*. at 6(b)(1-5).

41. *Id*. at 7(c)(1)(A).

42. *See* MAKING OPPORTUNITIES FOR BROADBAND INVESTMENT AND LIMITING EXCESSIVE AND NEEDLESS OBSTACLES TO WIRELESS ACT, REPORT OF THE COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION ON S.19, S. REP. NO. 115-4, at 13 (2017).

43. *See* MOBILE Now Act, S. 19, 115th Cong. § 7 (2017) https://www.congress.gov/115/bills/s19/BILLS-115s19es.pdf.

44. *See* SPEED Act, S. 1988, 115th Cong. (2017), https://www.congress.gov/bill/115th-congress/senate-bill/1988.

45. *Id.*

46. Such exempt facilities must lie within a public right-of way and not be higher (or substantially higher as determined by the FCC) than existing structures in the right-of-way. *See* S. 1988 § 4(1)(A) (2017).

(D-HI) similarly seeks to accelerate broadband deployment.[47] In particular, the discussion draft of this legislation would require state and local governments to act on wireless facilities applications within a certain timeframe (viz., a shot clock) and would limit the grounds for denying such requests.[48] Additionally, while acknowledging the rights of local authorities to charge for access to poles and local rights-of-way, the proposed legislation would require that such rates be "fair and reasonable," "competitively neutral," "technologically neutral," "nondiscriminatory," publicly disclosed, and "based on actual and direct costs".[49]

Akin to the commonsensical measures identified in proposed legislation, other practical regulatory reforms have been identified by the FCC. In November 2017, the FCC adopted a pair of measures designed to facilitate and accelerate the deployment of next-generation broadband. Specifically, the Commission unanimously adopted a commonsensical Report and Order that will implement steps to streamline the ability of firms to replace certain utility poles with more modern ones that are capable of hosting next-generation, small-cell technologies.[50] At the same time, the Commission also adopted rules that bar utility pole owners from charging companies for certain costs that they have already recouped from others, adopted a policy of allowing local providers equal access to each other's poles, and imposed a 180-day "shot clock" for approval of pole attachments.[51]

Collectively, these proposals before Congress and the FCC provide policymakers the authority to adopt numerous subtle regulatory reforms, which have the potential to substantially remove important barriers to expansion that are currently impeding the deployment of highly demanded broadband infrastructure. These reforms range from measures to expand spectrum availability,[52] to the adoption of dig-once policies,[53] to the adoption of shot clocks for expediting small cell sitings and removal of redundant regulatory siting reviews[54] These commonsense, practical

47. Staff Discussion Draft OLL17609, 115th Cong. (as circulated by the offices of Senators Thune and Schatz, October 2017).

48. *Id*. § 1(a)(4)(V).

49. *Id*. § 1(a)(6)(I).

50. *Accelerating Wireless Broadband Deployment by Removing Barriers to infrastructure Investment*, REPORT AND ORDER, 32 FCC Rcd. 9760 (2017), https://www.fcc.gov/document/fcc-streamlines-requirements-utility-pole-replacements-0.

51. *Accelerating Wireline Broadband Deployment by Removing Barriers to Infrastructure Investment*, REPORT AND ORDER, DECLARATORY RULING, AND FURTHER NOTICE OF PROPOSED RULEMAKING, 32 RCC Rcd. 11128 (2017).

52. *See* MOBILE Now Act, S. 19, 115th Cong. § 7 (2017) https://www.congress.gov/115/bills/s19/BILLS-115s19es.pdf.

53. *See* Broadband Conduit Deployment Act of 2018, H.R. 4800, 115th Cong. (2nd Sess. 2018).

54. *See* FCC, *supra* notes 50 and 51.

reforms offer the low-hanging fruit to be picked to advance the America's 21st century infrastructure.

IV. CONCLUSION

There are, to be sure, some areas of strident disagreement about regulatory policies that should govern the broadband sector.[55] To date, these disagreements have consumed a massive amount of energy with little progress to show for it. At the same time, there are simple, less visible reforms to regulations which govern this sector that create the prospect for both accelerated investment in and adoption of new broadband technologies. These reforms create the real prospect of improving consumers' lives and enhancing the nation's competitiveness without sacrificing necessary consumer protections. In the matter of regulatory reform, the practicality of these benefits should provide a platform that trumps our broader ideological differences.

55. *See generally* the massive debate over the rules and regulations that should apply to maintain a free and open internet. For a recent discussion, see Federal Communications Commission, REPORT & ORDER ON REMAND, DECLARATORY RULING & ORDER, GN Docket No. 14-28 (Mar. 12, 2015), https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf.

The Privacy of "Things": How the Stored Communications Act Has Been Outsmarted by Smart Technology

Donald L. Crowell III *

TABLE OF CONTENTS

* J.D. Candidate, The George Washington University Law School, May 2018. Senior Managing Editor, *Federal Communications Law Journal*, Vols. 69–70. B.A. Political Science, *cum laude*, University of California, Riverside, 2015. This Note is dedicated to both of my loving parents, whose support and sacrifices throughout my life have made it possible for me to pursue a career in law; to my inspiring friends and family who encourage the best in me; and to the Staff of the *Federal Communications Law Journal* who have been exceptional with their editorial work this year, and with whom I've had a sincere pleasure in having worked with.

I. INTRODUCTION

Meet Barbara, a modern business professional who is one of three managing partners at a well-known investment firm. Working from home, she prepares for a meeting with a client by connecting to her firm's Cloud-based remote desktop application on Amazon's S3 platform. The application replicates her work computer's desktop and allows her to access all her files just the same as if she was at the office. At the same time, her firm enjoys the benefit of having all its documents maintained in a secure backup location. Barbara finishes reviewing her client's documents and gets into her car—a BMW 3 Series. She opens Google Maps on her iPhone to get directions to her client's office, and, meanwhile, her phone has automatically connected via Bluetooth to her car's infotainment system and has begun synchronizing her contacts list, emails, and text messages. As she pulls out of the driveway—just far enough to disconnect from her home Wi-Fi network—her Nest smart-home system notes that she has left. Immediately, the thermostat adjusts to save energy, and the camera system turns on its motion sensors.

Meanwhile, unbeknownst to Barbara, one of the other partners at her investment firm has just made some illegal investments based on inside information. The partner's trades automatically triggered alarms at the Securities and Exchange Commission ("SEC"), Enforcement Division, based on his position at the investment firm. The SEC does a routine investigation into the trades over the next 90 days, ultimately finding a high probability that Barbara's partner made trades using inside information. However, their investigation thus far has only produced enough to muster "reasonable suspicion" that a crime has been committed; further information would be necessary to meet the standard of "probable cause" required to issue a search warrant against Barbara and her firm. The enforcement team, through their counsel, learns of the ability to issue an administrative subpoena under the Stored Communications Act ("SCA"). While it does not allow them to request any digital content newer than 180 days without having probable cause, they are able to request content from service providers for content that has been in storage for 180 days or longer.

The enforcement team first issues a subpoena to the Cloud service provider for Barbara's firm, Amazon, requesting all the electronic documents held in storage by the provider that are older than 180 days. They also make two other requests under the statute: (1) that the firm not be notified of the subpoena request for a minimum of 90 days, and (2) that the provider preserve the entirety of the firm's electronic documents, also for a period of 90 days.

As the team reviews the documents, including sifting through client lists, business strategies, and emails between the firm and its attorney, among other things, it discovers two sets of emails that it finds particularly interesting, although unrelated to their initial investigation against Barbara's partner. The first is a conversation between Barbara and her attorney. The discussion included questions about what constituted insider trading, and whether Barbara could be liable for trading on information that she receives

from a client. The second email is a message that Barbara had forwarded herself from her personal e-mail. While the substance of the second e-mail is irrelevant, the team now had the domain of Barbara's personal email account.

The investigators issue a subpoena to Barbara's personal email provider, Google, identical to the one sent to Amazon. What they receive from Google in return is far more than just her e-mail communications. Because of Google's multifaceted list of services, they receive her e-mails, GPS navigation history, web search history, photographs, and personal documents in her Google Drive storage. Her navigation history shows the specific dates and times she navigated to her client's office, in addition to regular visits to a nearby mosque, the local Democratic National Committee offices, her psychiatrist, a hotel, and an abortion clinic. Her photograph backups included those with family, friends, and on vacation trips, but also deeply private, fully-nude photos of Barbara. Similarly, her Google Drive records contained seemingly harmless collections of internet pages and random web-musings, but among them was a collection of scanned purchase receipts, tax records, private contracts, and her personal diary.

The investigation team thoroughly reviewed all the documents before issuing a final administrative subpoena to Barbara's smart-home system provider, Nest. The electronic records they received from Nest included a history of every single time, to the second, when Barbara either left or arrived home. More importantly, provided to the SEC were video recordings of Barbara's home beginning from when the system was installed 6 years ago, essentially capturing every person that has ever been inside her home, and all activities that have taken place inside of it.

They continued reviewing Barbara's personal electronic records until just before the 90-day delay notice and preservation request expired, after which they issued a 90-day extension for both requests, as allowed by the statute. A few days later, just after the 181-day mark since the start of their investigation, the SEC re-issues subpoenas to each of the original providers, this time capturing all electronic records leading to the incident. Reviewing the new navigation history production from Google Maps, as well as the calendar records stored in Amazon's Cloud, they see that Barbara had a meeting with her client on the day of the incident. Audio and video security camera footage from the night before the incident revealed that a client of Barbara's had been over at her home for dinner, during which highly confidential information was discussed regarding her client's expected product release. None of this information was enough to bring formal charges against Barbara, although her partner was ultimately prosecuted. However, Barbara's very intimate and confidential information was now in the public's hand because of her tangential relationship to someone under investigation.

This illustration with Barbara is just one very possible example of the shortcomings that digital privacy law faces under an outdated Stored Communications Act ("SCA"). This Note argues a three-pronged solution to resolve these shortcomings through a case-study analysis of different

technologies: (1) extending a broader application of *Riley v. California*,[1] (2) legislative amendments to the SCA,[2] and (3) private-sector data encryption advancements. Part II will consider the current jurisprudence of privacy in electronic records and communications by first exploring the foundational elements of modern privacy law, before diving into the more field-specific cases and circuit splits relating to expectations of privacy in digital information. Part III will look at the Electronic Communications Privacy Act ("ECPA") and SCA, examining both their legislative history and amendments, as well as the contradictions and flaws that are revealed when considering their applicability to modern Cloud-based technologies. Part IV will analyze three different Cloud technologies, specifically ones that have the capability of holding the most confidential information of individuals, and demonstrate how the use of administrative subpoenas under the SCA, as well as the delay and preservation notice provisions, directly violate Fourth Amendment protections and are in conflict with prior court rulings that have prohibited the same type of information gathering by other means.

Part V will lay out the three-pronged federal solution to establish new standards for businesses and the government to follow. The first prong will argue why it is necessary to extend the *Riley* Court's decision (finding constitutional protections in information stored in the Cloud)[3] to situations beyond arrests. The second prong will propose an amendment or replacement to the ECPA and SCA that limits the ability of law enforcement to perform warrantless searches of individuals who are not under investigation, as well as eliminating the time restriction requirements of the acts. Further, the proposed amendments enable National Telecommunications & Information Administration ("NTIA") to regulate electronic communications service providers ("ECSPs") and remote computing service providers ("RCSPs"). This will include a more technical determination of their definitions, as well as requiring those categories of providers to register with NTIA, thereby limiting the discretionary use of administrative subpoenas by law enforcement. The third prong is not a government solution, but rather a proposal that ECSPs and RCSPs eliminate or reduce their own ability to access sensitive consumer data. This, along with continuing advancements in encryption technology, will allow law enforcement access to encrypted data, but not necessarily to the content of the data itself.

1. *See generally* Riley v. California, 134 S. Ct. 2473 (2014).
2. *See* Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012).
3. *See Riley*, 134 S. Ct. at 2491–93.

II. FOURTH AMENDMENT JURISPRUDENCE RELATING TO DIGITAL COMMUNICATIONS

A. Katz v. United States Establishes the Foundation for Modern Privacy Expectations

Modern-day Fourth Amendment jurisprudence finds its foundation in *Katz v. United States*, which laid the groundwork for what is now referred to as the "reasonable expectation of privacy" test.[4] In *Katz*, FBI agents attached an electronic listening device to a public phone booth that they suspected Katz was using to gamble across state lines.[5] Unaware of the device, Katz made phone calls placing bets with contacts in Miami and Boston—unaware that the call was being recorded.[6] The Government introduced the telephone recordings as evidence to successfully convict Katz of the wagering charges in district court.[7]

On appeal, the U.S. Supreme Court reconsidered its previous reliance on the "trespass doctrine"[8] and held that the Fourth Amendment grants a right to "privacy against certain kinds of governmental intrusion…."[9] This protection follows a person wherever they go, and is not limited to particular places or things.[10] However, it was Justice Harlan, in a concurring opinion, who enunciated the two-part "reasonable expectation of privacy" test that the Court would rely on in a handful of Fourth Amendment cases following *Katz*.[11] This test requires that an individual have a "subjective expectation of privacy" in their belongings and/or information, and that society would objectively find the individual's subjective expectation of privacy to be reasonable.[12]

4. *See* Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 987–89 (2016).

5. *See* Katz v. United States, 389 U.S. 347, 348–49 (1967).

6. *See id.*

7. *See id.*

8. The "trespass doctrine" was based on the common law tort of trespass, requiring the Government to physically trespass on to property before Fourth Amendment protections could be invoked. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 31 (2001); Olmstead v. United States, 277 U.S. 438, 463–65 (1928).

9. *See Katz*, 389 U.S. at 350.

10. *See id.* at 359 ("Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.").

11. *See Katz*, 389 U.S. at 360–62 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual subjective expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

12. *See id.*

B. Miller and Smith Evolve Katz into the "Third-Party Disclosure Doctrine"

The Court in *United States v. Miller*, weighing both prongs of the *Katz* test, determined that the Fourth Amendment does not protect an individual's privacy interest in non-confidential information that was voluntarily conveyed to a third-party.[13] In *Miller*, law enforcement had gathered, over the course of several months, evidence of illegal that Miller was engaging in distilling activity.[14] Included in this evidence were bank records that the Treasury Department had recovered under grand jury subpoenas issued to Miller's bank.[15] Miller sought to suppress the bank records, arguing successfully at the appellate court level that the Government had illegally acquired access to those records from his bank.[16]

The Court reversed, finding that there was "no intrusion into any area in which [Miller] had a protected Fourth Amendment interest."[17] Essentially, there was no intrusion into a "zone of privacy."[18] The Court found that while it had previously held the Fourth Amendment protects people from "compulsory production of a man's private papers,"[19] the bank records in question in *Miller* did not actually belong to the defendant.[20] Rather, they belonged to the bank, who maintained those records as a party to the transactions between it and Miller.[21] When Miller participated in transactions with the bank, he knowingly took the risk that the bank could reveal any resulting information to the Government.[22] The Court ruled, therefore, that Miller held no "Fourth Amendment interest" in the bank records, even if it were assumed that they would only be used for a specific purpose.[23] The Government's subpoena, as well as the bank's action in turning over the records, was constitutionally permissible.[24]

---

13. *See* United States v. Miller, 425 U.S. 435, 441–43 (1976).
14. *Id.* at 436.
15. *Id.*
16. *Id.* at 439 ("[T]he court [of appeals] held that the Government had improperly circumvented *Boyd's* protections of [Miller's] Fourth Amendment right against 'unreasonable searches and seizures' by 'first requiring a third party bank to copy all of its depositors' personal checks and then, with an improper invocation of legal processes, calling upon the bank to allow inspection and reproduction of those copies.'" (citations omitted)).
17. *Id.* at 440.
18. *Id. at* 440 ("'[N]o interest legitimately protected by the Fourth Amendment' is implicated by governmental investigative activities unless there is an intrusion into a zone of privacy, into 'the security a man relies upon when he places himself or his property within a constitutionally protected area.'" (quoting *Hoffa v. United States*, 385 U.S. 293, 301–02 (1966))).
19. *Id.* (citing *Boyd v. United States*, 116 U.S. 616, 528 (1886)).
20. *Id.*
21. *Id.* at 441–42.
22. *Id.* at 443 (citing United States v. White, 401 U.S. 745, 751–52 (1971)).
23. *Id.* at 445–46.
24. *Id.*

The Court in *Smith v. Maryland* developed the third-party disclosure doctrine to encompass the use of pen registers[25] in determining both that its use was not a "search" within the meaning of the Fourth Amendment, and that no legitimate expectation of privacy existed in phone numbers.[26] Similar to *Katz*, law enforcement identified Smith as their prime suspect in a robbery.[27] Without first acquiring a warrant, law enforcement installed a pen register with the telephone company used by Smith to record all phone numbers that he dialed, which ultimately showed that only a few days earlier he had dialed the robbery victim's phone number.[28] This evidence was used to acquire a search warrant for Smith's home, where police found evidence that identified him as the robber.[29]

Like in *Miller*, the Court in *Smith* found that the defendant had no expectation of privacy in his telephone records because he did not own them.[30] Smith had "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[31] By doing so, Smith "assumed the risk that the company would reveal to the police the numbers he dialed."[32] Smith could, therefore, hold no legitimate expectation of privacy in those records.[33] *Smith* reaffirmed the Court's decision in *Miller*, and the validity of the third-party disclosure doctrine, which would control the decisions of other similar Fourth Amendment cases until only very recently.[34]

25. *See* Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979) ("A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed. A pen register is 'usually installed at a central telephone facility [and] records on a paper tape all numbers dialed from [the] line" to which it is attached.'" (citations omitted)).

26. *Id.* at 745–46.

27. *Id.* at 737.

28. *Id.*

29. *Id.*

30. *Id.* at 741 ("Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner obviously cannot claim that his 'property' was invaded or that police intruded into a 'constitutionally protected area.'").

31. *Id.* at 744.

32. *Id.*

33. *Id.*

34. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 948 (2012) (monitoring of an individual's location patterns over the course of an extended period of time—in this case 28 days—by attaching a GPS device to track an individual's vehicle movements constituted a "search" within the meaning of the Fourth Amendment); United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (applying Voluntary/Third-Party Disclosure Doctrine to e-mail metadata); United States v. Forrester, 512 F.3d 500, 509 (9th Cir. 2008) (finding that computer surveillance of an individual, and introduction of website history information gathered through such surveillance, did not amount to a search under the Fourth Amendment).

C. Courts are Conflicted as to Whether a Reasonable Expectation of Privacy Exists in Electronic Communications

In 2010, the Sixth Circuit in *United States v. Warshak* strengthened Fourth Amendment protections over digital technologies when it held that individuals have a "reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial[internet service provider] ["ISP"]."[35] Applying the two-part *Katz* test, the court first found it highly likely that the defendant did not expect his e-mail communications to be public, given their "sensitive and sometimes damning substance."[36] As to the second part of the test, the court analogized an e-mail to a "letter or a phone call," and noted that simply because an ISP can access the content of those e-mails is not enough to "extinguish a reasonable expectationof privacy."[37] Similarly, the "rented space" that a subscriber uses to store the e-mail on the ISP's server is similar to the renting of a hotel room or apartment, where guests and tenants have a reasonable expectation of privacy even though maids or maintenance workers may enter on occasion.[38]

This case is distinguishable from *Miller* for several reasons.[39] *Miller* dealt with the disclosure of very particular business records, as opposed to the "potentially unlimited variety of 'confidential communications'" that might be contained in e-mail and electronic content.[40] And although in *Miller* the bank needed to use the information in their ordinary course of business, the ISP in *Warshak* was simply an "*intermediary* and not the intended recipient of the e-mails."[41]

The Eleventh Circuit's decision in *Rehberg v. Paulk* came at nearly the same time as *Warshak*, but delivered an opposite ruling: that "[a] person … loses a reasonable expectation of privacy in emails, at least after the email is sent to and received by a third party."[42] *Rehberg*'s analysis is similar to the earlier line of "voluntary/third-party disclosure doctrine" cases.[43] Citing several other circuit decisions, the Eleventh Circuit found that "Rehberg's voluntary delivery of emails to third parties constituted a voluntary relinquishment of the right to privacy in that information" once the third party had received them.[44]

---

35. *Warshak*, 631 F.3d at 288 (internal citation and quotation omitted).

36. *Id.* at 284 ("[Defendant's] entire business and personal life was contained within the . . . emails seized.") (citation omitted).

37. *Id.* at 286.

38. *Id.* at 287 (citing United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1997) and United States v. Washington, 573 F.3d 279, 284 (6th Cir. 2009)).

39. *Id.* at 288.

40. *Id.*

41. *Id.* (emphasis in original) (citations omitted).

42. Rehberg v. Paulk, 598 F.3d 1268, 1281 (11th Cir. 2010), *vacated*, 611 F.3d 828 (11th Cir. 2010).

43. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 745–46 (1979); United States v. Miller, 425 U.S. 435, 444–45 (1976).

44. *Rehberg*, 598 F.3d at 1282.

More recently, it appears that the Supreme Court has tipped the discussion in favor of protecting digital content, when in *California v. Riley* it ruled that "a warrant is generally required before [searching information on a cell phone], even when a cell phone is seized incident to arrest."[45] The Court considered many factors, but relied heavily on the distinction between cell phones and their content from "other objects that might be kept on an arrestee's person."[46] A cell phone allows individuals to carry around "every piece of mail they have received . . . every picture they have taken, [and[every book or article they have read."[47] Keeping this quantity of records on one's person is not something that previously was feasible, and, even if done, would have likely required storing them in a container that a police officer would need a warrant to search.[48] This, coupled with the nature of content stored on cell phones—including internet search history,[49] as well as the types of mobile applications one uses[50]—potentially allows for broad and pervasive intrusions into one's privacy.[51]

These factors, however, only address content that is physically stored on a cell phone. The Court also found the argument in favor of searching cell phones incident to arrest to be essentially futile when accessing data in the Cloud:[52]

> Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen. This is what cell phones, with increasing frequency, are designed to do by taking advantage of "cloud computing.". . . Cell phone users often may not know whether particular information is stored on the device or in the [C]loud, and it generally makes little difference. Moreover, the same type of data may be stored locally on the device for one user and in the [C]loud for another.[53]

While *Riley* did appear to broadly expand privacy rights to digital information, the Supreme Court found it necessary to limit its holding. For

45. *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014).
46. *See id.* at 2489.
47. *Id.*
48. *Id.* at 2491 ("[A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house.").
49. *See id.* at 2490. ("An Internet search and browsing history . . . could reveal an individual's private interests or concerns–perhaps a search for certain symptoms of diseases, coupled with frequent visits to WebMD.").
50. *Id.* ("There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life.").
51. *See id.*
52. *See id.* at 2491.
53. *Id.* (citations omitted).

example, before making its analogy between cell phone content and physical records, it noted, albeit in a footnote, that *Riley* only addresses searches of cell phones incident to arrest.[54] Further, the limitations on law enforcement do not apply in cases where exigent circumstances necessitate the expedited retrieval of information from a cell phone, such that "a warrantless search is objectively reasonable under the Fourth Amendment."[55] Therefore, it is not entirely clear whether *Riley* amounts to more than *persuasive* authority when applied to situations other than cell phone searches incident to arrest—such as in the scenario with Barbara demonstrated above.[56]

III. THE STORED COMMUNICATIONS ACT

In 1986, Congress enacted the Electronic Communications Privacy Act ("ECPA"), which included, in part, the Stored Communications Act ("SCA"), which governs the privacy of electronic data.[57] Although its main purpose was to provide protection for "new forms of [ ] communications . . . against improper interception," a secondary goal was to assist law enforcement by providing them with "investigative techniques which involve the interception of communications."[58] The following discussion will focus on section 2703 of the SCA, which requires businesses that provide particular types of electronic services to the public to disclose a customer's records to law enforcement when requested, after meeting certain procedural requirements.[59]

Yet, Section 2703 of the Act, in particular, has failed to develop in tandem with the digital technology market. The results have revealed an economic and constitutional vulnerability that will grow with the increasing use of digital technology by consumers in the coming years. Section 2703 allows government agencies, at both the state and federal level, to issue administrative subpoenas to electronic service providers for essentially all types of stored electronic information held on behalf of consumers.[60] These administrative subpoenas do not require the agency to show probable cause

54. *Id.* at 2489 n.1 ("Because the United States and California agree that these cases involve searches incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.").

55. *Id.* at 2494 (quoting Kentucky v. King, 131 S. Ct. 1849, 1856 (2011)).

56. *See supra* Part I (Introduction).

57. *See* Electronic Communications Privacy Act of 1986, Pub L. No. 99–508, 100 Stat 1848 (codified as amended in scattered sections of 18 U.S.C.); Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012); *see also* Erik C. Shallman, *Up in the Air: Clarifying Cloud Storage Protection*, 19 INTELL. PROP. L. BULL. 49, 66 (2014); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

58. *See* 132 Cong. Rec. H8977–02 (1986) (statement of Rep. Kastenmeier).

59. *See* 18 U.S.C. § 2703 (2012).

60. *See id.*

that an act was being committed, nor do they require that the administrative subpoena be issued against the specific person being investigated.[61]

A. Applicability of the Required Disclosure Section of the SCA is Broad as to the Entities and Records It Governs

The types of records governed under the SCA ranges from those containing actual content—e-mails, electronic documents, pictures, etc.—to basic subscriber information, such as name and contact information.[62] The SCA distinguishes between records containing substantive information and records containing basic subscriber information by referring to the records in two different categories–content and non-content information ["records concerning" ECS or RCS customers].[63] Compelling disclosure of the two categories varies, for example, can use state or federal administrative subpoena power to access non-content information, such as credit numbers, usernames, network addresses, physical addresses, among other information.[64] In most cases, the use of administrative subpoenas do not require any suspicion of a crime being committed, and, depending on the state, can be used by local governments.[65]

Of equal importance is the SCA's distinction between electronic records that are in storage for under and for over 180 days.[66] For documents in storage under 180 days, "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction" is always required to compel disclosure.[67] Records that have been in storage for longer than 180 days are subject to far less burdensome requirements.

---

61. Lacking in § 2703 is language indicating that *any* of the methods used by law enforcement to gather records may only be used to obtain records of the person that is actually being investigated. *See generally* § 2703. The only consistent requirement in the statute relates to notification of the *customer* of the records, which may not necesarilly be the individual under investigation. *Id.*

62. *See* §§ 2510, 2711.

63. *See* § 2703.

64. *See id.* § 2703(c)(1)(E), (c)(2) (to compel disclosure the government must only "seek[] [non-content] information").

65. *See, e.g.*, NEWPORT BEACH, CAL., MUN. Code § 5.04.300 (2018) ("The Finance Director, or any authorized employee, is hereby authorized to examine the books, papers and records of any person subject to this chapter . . . . Every licensee or supposed licensee is hereby directed and required to furnish to the Finance Director the means, facilities and opportunity for making such examination and investigation as are hereby authorized. The Finance Director is hereby authorized to examine any person, under oath, for the purpose of verifying the accuracy of any return made, or, if no return is made, to ascertain the license fees due under this title, and for this purpose may compel the production of books, papers and records and the attendance of all persons before him or her, whether as parties or witnesses, whenever he or she believes such persons have knowledge of such matters.").

66. *See id.*

67. *See* § 2703(a).

Under § 2703(b), a governmental entity can compel disclosure of documents stored longer than 180 days in two different ways:

> (A) [W]ithout required notice to the subscriber or customer, if the governmental entity obtains a warrant . . . by a court of competent jurisdiction; or
> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—
> (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
> (ii) obtains a court order for such disclosure under subsection (d) of this section;
> except that delayed notice may be given pursuant to Section 2705 of this title.[68]

Therefore, it is important to determine who exactly is required to comply with these provisions of the SCA. The Act provides two types of service providers that must disclose customer records–(1) electronic communications service providers ("ECSP"),[69] and (2) remote computing service providers ("RCSP"),both of which are required to disclose content and non-content records.[70] One significant difference between the two categories is that if a provider is classified as an ECSP, then the government can only acquire documents that are less than 180 days old through the use of a warrant.[71] If the provider is classified as an RCSP, or the documents sought from an ECSP are older than 180 days, then the government can use other methods to compel disclosure (such as an administrative subpoena).[72]

These categories appear very broad, encompassing an increasing number of businesses when considering the definition of "electronic communication,"[73] and how common it is for businesses to provide services

68. *See* § 2703(b)(1). Additionally, § 2705 allows governmental entities attempting to compel disclosure under § 2703(b) to delay giving required notice to subscribers for renewable 90-day periods where an adverse outcome may occur as a result of giving notice. *See* § 2705(a). An adverse result includes "endangering the life or physical safety of an individual; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation or unduly delaying trial." *Id.*

69. *See* 18 U.S.C. § 2510(15) (2012) ("'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications.").

70. *See* 18 U.S.C.§ 2711(2) (2012) ("the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.").

71. *See* § 2703(a).

72. *See id.*

73. *See* §2510(12) ("'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, or electromagnetic, photoelectronic or photooptical system….").

that involve electronic communications today.[74] As electronic communication technologies continue to advance, companies and consumers are increasingly transitioning to the use of the Cloud to store information.[75] This growth is one particularly strong reason why SCA reform is so pressing, and critical to ensuring equal application of the Fourth Amendment's property protections.

IV. THE FOURTH AMENDMENT OFFERS PROTECTION FOR INFORMATION STORED IN THE CLOUD—FEDERAL LAW MUST REPRESENT THIS

For both consumers and businesses, the trend seems to be heading to a default of using the Cloud for storage of documents and other media, such as music, pictures, and even medical records.[76] The Cloud provides many advantages over other forms of data storage, including increased accessibility, security, and backup redundancy.[77] Developing a framework for constitutional protections of digital property and information is difficult, in part because there is still debate over what kind of protections e-mail deserves, which is a more basic form of electronic communication compared to the multitude of products on the market today.

Applying the *Katz* framework to Cloud storage services ultimately demonstrates that electronic media storage should be protected by the Fourth Amendment, although ambiguities remain as with *Katz*'s application to similar digital technologies. Initially, the Supreme Court assumed that the Fourth Amendment framework used to analyze the propriety of physical searches applies similarly to searches of electronic property or information.[78] Taking this assumption as valid, it is still necessary to analogize the use of Cloud storage to something physical for Fourth Amendment's protection over "persons, houses, papers, and effects"[79] to be properly applied.

74. *See* S. Rep. 99–541, at 10-11 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555 ("Today businesses of all sizes—hospitals, banks and many others—use remote computing services for computer processing.")

75. *See* Leo Sun, 10 *Cloud Computing Statistics That Will Blow You Away*, MOTLEY FOOL (Nov. 29, 2016, 3:08 PM), https://www.fool.com/investing/2016/11/29/10-cloud-computing-stats-that-will-blow-you-away.aspx [https://perma.cc/EH5Q-Y2FY].

76. *See, e.g.*, *Are Consumers Better Off Putting Everything in the Cloud?*, WALL ST. J.:J. REPORTS: LEADERSHIP (May 11, 2014, 5:05PM ET), http://www.wsj.com/articles/are-consumers-better-off-putting-everything-in-the-Cloud-1399644099 [https://perma.cc/2S2A-ZBMA].

77. *See* Ian Paul, *Why you need a cloud backup service, and how to use one*, PCWORLD (Jan. 12, 2016, 3:30 AM PST), https://www.pcworld.com/article/3020270/security/why-you-need-a-cloud-backup-service-and-how-to-use-one.html [https://perma.cc/V3VM-M45K].

78. *See* City of Ontario, Cal. v. Quon, 560 U.S. 746, 748 (2010).

79. *See* U.S. CONST. amend. IV.

A. Classifying Cloud Document Storage Services under the SCA

One of the first steps in using a Cloud storage service, such as Google Drive or Dropbox, is uploading files into the Cloud.[80] This action, in and of itself, falls neatly within the definition of an electronic communication under the SCA.[81] By providing the public with the ability to upload documents into the Cloud, the Cloud storage provider allows users to send or receive wire or electronic communications, not to mention the numerous tools that are available for users to send documents in the Cloud to other individuals.[82] When users begin to "collaborate" with others on documents stored in the Cloud, they are also sending and receiving "electronic communications" through the Cloud storage service provider. Thus, looking at the most basic function of uploading files to Cloud storage, in addition to the more advanced functions of Cloud storage devices, it is evident that Cloud storage providers can fall within the ECSP category of the SCA.

Yet, one highly technical question regarding the timeliness requirement remains: what does it mean for a document to be in electronic storage for 180 days? Often, users of Cloud storage services upload documents and work on them from the Cloud. Every time a user saves a change to the document, the file is no longer the same original one. Currently, there is no guidance as to whether a document would need a warrant if it had been originally uploaded more than 180 days prior to law enforcement's request, but had been updated within that time period. In strictly technical terms, it can be argued that anytime a document has been edited this countdown resets because the process of saving an edited document involves deleting the original and replacing it with the changed version.[83]

Cloud storage services also can just as easily fall under the definition of "remote computer service providers." To qualify as a remote computer service provider, the business must provide computer storage or processing services to the public "by means of an electronic communications system."[84] As discussed earlier, the use of Cloud storage services inherently falls under the definition of electronic communication services.[85] As the main function of Cloud storage providers is to allow individuals to store documents on remote servers, they appear to fall even more neatly within this second category of the SCA.

---

80. *See generally Meet Google Drive*, GOOGLE DRIVE https://www.google.com/intl/en_us/drive/ [https://perma.cc/YKX3-PD3K](last visited Jan. 15, 2018).

81. *See* 18 U.S.C. § 2510 (2012).

82. *See generally How Dropbox Works*, DROPBOX https://www.dropbox.com/help/sign-in/how-security-works [https://perma.cc/L5CC-VY74] (last accessed Mar. 19, 2018)

83. *See View Activity & File Versions*, GOOGLE, INC., https://support.google.com/drive/answer/2409045?co=GENIE.Platform%3DDesktop&hl=en [https://perma.cc/U4FQ-FTRE] (last visited Jan. 15, 2018).

84. *See* 18 U.S.C. § 2711 (2012).

85. *See supra*, Part III (The Stored Communications Act).

What this means for users of Cloud storage services is that their documents are more vulnerable to government-compelled disclosures because they fall under both categories. Remote computer service providers can be compelled by the Government to hand over user data, regardless of whether it is older/newer than 180 days, without the use of a warrant.[86] The Government can simply use a subpoena or court order to access the data as long as they give notice to the subscriber. [87]Yet, the Government can delay this notice for multiple 90-day periods, even while receiving access to the information held by the subscriber's service provider.[88] Unfortunately, the state does not address whether a provider may be classified under one or both categories of the SCA.[89] However, the lack of such a limitation indicates that potentially the least-restrictive category with regard to law enforcement's ability to access records would apply.

B. Classifying Mobile Applications Under the SCA

More common than the use of Cloud storage is the use of mobile applications on smartphones. These applications range from news, politics, and healthcare, to almost anything else.[90] While its content and use may vary dramatically, a commonality among "apps" is that they collect and store information both gathered from, and owned by, the user. [91] Often this information is not stored on the local memory of a cell phone, for both technological and economic reasons.[92] Regardless of where the information used by the app is stored, most apps transmit data from the cellular device to the company that owns the app.[93] This data is then analyzed and processed to accomplish a particular task, such as fulfilling a search request in a news app for "Washington, D.C."[94]

Classifying mobile applications is a very fact-specific analysis that largely depends on the particular application in question. For example, an application that does not store or process any data in the Cloud would not likely fall under either category of the SCA. Take, for example, a game application that functions entirely from the data stored on the cell phone (offline)—it would not qualify under either category. If the same application

86. *See* 18 U.S.C. § 2703(b)(1) (2012).
87. *Id.*
88. *See* § 2703(b)(1)(B)(ii).
89. This is likely due to the state of e-mail technology present at the time the SCA was enacted, which was very simplistic and not at all like the multi-functional software technologies that currently exist. *See* Outlook.com, *The* 41*-Year History of Email*, MASHABLE (Sept. 20, 2012), http://mashable.com/2012/09/20/evolution-email/#DWPJqRdF7sq2 [https://perma.cc/L9BC-U4A5].
90. *See generally Choosing A Category*, APPLE, INC., https://developer.apple.com/app-store/categories/ [https://perma.cc/B22U-3456] (last visited Mar. 12, 2017).
91. *See generally Understanding Mobile Apps*, FTC (Feb. 2017), https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps#basics [https://perma.cc/JP7W-2PWC].
92. *See id.*
93. *See id.*
94. *See id.*

allowed you to purchase additional features, or stored user data in the Cloud, then that would change how the game application is classified. The ability to purchase additional features within the game app, for example, would mean that some sort of transmission occurred between the cell phone and the developer's server. Records of these transactions are likely stored with the developer, and at minimum, are stored with the purchase facilitator (e.g., Apple or Google). Similarly, a game requiring an online connection communicates information to and from the device in order to allow the game to function. A mobile application of this type would likely fall under both categories, as some sort of processing likely occurs on the remote servers, and there likely is some information stored relating to any account or profile made by the consumer for the game.

The application store from which user download an application (e.g., the App Store or the Google Play Store) is likely to fall under the ECSP category of the SCA, because there are electronic communications transmitted between the device and the store when purchasing an application. In contrast, the application store would likely not be considered an RCSP because it is not processing any information for the user—unless one considers the processes involved in facilitating the download of the application to fall under the definition.

Generally, however, it can be argued that if an application functions entirely from the files it stores locally on a person's cell phone, and requires no further online access, then it would not fall under either category. Such an argument seems appropriate, as the application would fail to send electronic communications, which is an essential part of both ECSP and RCSP classifications.[95] But, if an application requires access to the internet (more than just needing it to access online content, like a web browser might), it would likely fall under one or both categories of the SCA because of the broad language, although classification as an RCSP might be difficult depending on what is done with the data in the Cloud. This distinction is important because if a provider falls under the category of an RCSP, any records, even those less than 180 days–old, are subject to compelled disclosure without a warrant.

C. Classifying Security and Smart Home Services under the SCA

Smart home services, such as Nest throw an interesting wrench into the mix of Cloud service providers, both because they require a physical existence within the home of an individual, and because of the uniqueness of the businesses that own them.[96] These services can work in many ways. For example, Nest sells "smart" security cameras, thermostats, and smoke detectors that can link together with other smart-home technologies, including

95. *See* 18 U.S.C. § 2510 (2012).

96. Here, uniqueness is meant to describe the vast portfolio of companies and holdings owned by major technology companies, as well as the variation and multitude of services that they provide.

Google devices, Nest's parent company.[97] Technologies like Apple's Siri, or Amazon's Alexa, function similarly by requiring a connection to a Cloud server to process verbal requests made by the user.[98] Based on the definitions provided in the SCA, these companies seem to neatly fall under both categories of service providers, as they both transmit data electronically between the local device in a person's home and Cloud servers, and then process the data in the Cloud to recognize things like camera movement, sounds, smoke levels, and even the user's location.[99]

What is most interesting about these products is how the SCA's framework can be applied to their parent companies. The statute is silent as to whether a certain percentage of a company's services must be in devoted to electronic communications in order to be classified as an ECSP or RCSP. This becomes tricky when a company is involved in many types of business areas. Take Amazon as an example—Its Alexa device is one of its first devices in the smart-home category. However, Amazon's major business is retail through its e-commerce website.[100] It is not entirely clear if a company that provides Cloud services as one small part of its business—say five percent—would be classified as an ECSP or RCSP, or whether the government can request documents from such a company relating to products or services that are unrelated to SCA jurisdiction. With some companies, like Google, it may not matter because generally all of its products or services are in the form of electronic communications. However, for companies like Amazon, or any other business that only provides a miniscule amount of service or products as electronic communications, it is not entirely clear how the SCA would be applied. Because of the lack of technical language and guidance in the SCA, it appears that any company that provides those types of services at all, would be considered under either category, regardless of the percentage that Cloud services make up of its business.

D. A General Analysis of Cloud Service Providers Under the Fourth Amendment Framework

In *City of Ontario v. Quon*, the Supreme Court presented the idea that digital property should be treated identical to its physical counterparts with regard to Fourth Amendment protections.[101] Some commentators, as well as the Sixth Circuit in *Warshak*, have likened electronic media storage to the renting of physical property, although it differs slightly, because with most

97. *See generally Get more from you Nest with Google*, GOOGLE, INC. (last visited Mar. 12, 2017), https://workswithnest.google.com/ [https://perma.cc/Z9EM-EHMX].

98. *See, e.g.*, Brian Barrett, *What Amazon Echo and Google Home Do With Your Voice Data*, WIRED (Nov. 24, 2017, 7:00 AM), https://www.wired.com/story/amazon-echo-and-google-home-voice-data-delete/.

99. *Id.*

100. Amazon is particularly unique because it has been marketing and developing other services that primarily serve as a benefit to its "Prime" membership base including music and video streaming services, as well as Cloud storage.

101. *See geneally* City of Ontario v. Quon, 560 U.S. 746 (2010)

Cloud services, the data can reside in multiple locations aside from servers owned by the provider.[102] Using the rental property analogy, users can expect to have a reasonable expectation of privacy because courts have determined that such an expectation exists in physical rental properties.[103] The analogy highlights the direct conflict with provisions of the SCA that allow the government to access both content and non-content data through less restrictive mechanisms (e.g., administrative subpoenas and court orders), as that would be akin to allowing the use of administrative subpoenas to search an individual's home.[104]

Even when using the rental property analogy, the third-party disclosure doctrine continues to raise issues and is likely one of the main factors for the failure of courts to reach a consensus. Setting aside agreements on the comparison between Cloud storage and physical records, some courts still choose to apply the third-party disclosure doctrine's analysis, which weakens the argument for constitutional protections.[105] The third-party disclosure doctrine is premised on the notion that an individual's right to privacy in certain information is waived when that information is collected by a service provider or other third-party businesses as a necessary means to provide services or to comply with the law.[106] The equivalent to this waiver occurs either by means of voluntary disclosure when uploading documents for use with an ECSP or RCSP, or through signing user license agreements that have the effect of a waiver.[107]However, this argument is flawed, because in many cases when one uses a Cloud service, the service provider does not necessarily have access to the contents of the records due to encryption.[108]

Even when a service provider does have access to the content of information stored in its Cloud service,[109] there is no reason the Fourth Amendment would not require a warrant to be issued before the government could access any of the content. As mentioned previously,[110] several circuit courts have found that a reasonable expectation of privacy exists in a storage unit.[111] Under this line of thinking, it would be a violation of the Fourth Amendment for the government to access a rental storage unit without a warrant in the same way it would be impermissible for it to access a person's

---

102. *See, e.g.*, Shallman *supra* note 57, at 54; *See also* United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010).

103. *See, e.g.*, United States v. Washington, 573 F.3d 279, 284 (6th Cir. 2009); United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1997).

104. *See* 18 U.S.C. § 2703 (2012).

105. *See, e.g.*, Rehberg v. Paulk, 611 F.3d 828, 843 (11th Cir. 2010).

106. *See* United States v. Miller, 425 U.S. 435, 444–45 (1976).

107. *See Rehberg*, 611 F.3d at 843.

108. *E.g.*, *Security, Trust + Compliance*, CODE 42 (last visited Mar. 12, 2017), http://www.code42.com/security/ [https://perma.cc/P6RY-P7Q2].

109. *See* Jose Pagliery, *Apple Promises Privacy—But Not on iCloud*, CNN: TECH (Feb. 22, 2016, 1:28PM EST), http://money.cnn.com/2016/02/22/technology/apple-privacy-icloud/ [https://perma.cc/YC4B-M3AW].

110. *Supra* Part IV, Section D.

111. *See E.g.*, United States. v. Johnson, 584 F.3d 995, 1001 (10th Cir. 2009) ("People generally have a reasonable expectation of privacy in a storage unit, because storage units are secure areas that 'command a high degree of privacy.'" (citations omitted)).

digital locker.[112] By using administrative subpoenas and court orders under Section 2703(b), which does not require the same degree of inference that a crime is being committed, the government may violate the Constitution.[113]

V. A THREE-PRONGED SOLUTION TO ESTABLISH CLEAR CONSTITUTIONAL PROTECTIONS FOR INFORMATION STORED IN THE CLOUD

There are several ways to improve the privacy protections for digital information stored in the Cloud. Along with the private sector, each of the three branches of government may offer a different way of establishing clear constitutional protections for digital information. The courts, for example, can determine what limits must be placed on law enforcement's ability to search and seize digital content, in order to comply with the Fourth Amendment. Congress, on the other hand, can amend the current Act to implement the changes this Note proposes. The Executive Branch, through the Department of Justice, or a specialized agency, like the National Telecommunications and Information Administration, can use its expertise to determine how to classify ECSPs and RCSPs, and when warrantless compelled disclosure is appropriate.[114] Finally, the private sector can continue to develop technologies that rely on stronger and novel encryption methods, as well as providing services that cannot be accessed by the provider itself.

A. The Supreme Court Should Expand Riley v. California to Require Warrants for Any Government Access of User Data Held in the Cloud

Riley v. California was a substantial step in setting the limitations of Fourth Amendment protections as they relate to property stored in the Cloud. By holding that police officers did not have a right to access the contents of an individual's phone, even in a search incident to arrest, the Supreme Court held there was an inherent value in one's digital records.[115] Of further importance was the Court's discussion relating to information stored in the Cloud, where it found significant privacy interests existed in digital data that

112. Such as a monthly subscription service like Google Drive, which is used to store electronic information remotely. *See, e.g.*, *Using Drive*, GOOGLE, https://www.google.com/drive/using-drive/ (last visited Apr. 18, 2018).

113. *See* U.S. CONST. Amend. IV; 18 U.S.C. § 2703(b) (2012); Fed. R. Civ. P.41(d).

114. Should an agency like the FCC be used, these determinations would remain independent from the President's policy directions.

115. *See* Riley v. California, 134 S. Ct. 2473, 2485 (2014) ("We therefore decline to extend Robinson to searches of data on cell phones, and hold instead that officers must generally secure a warrant before conducting such a search.").

is accessible from a cell phone, but physically located elsewhere.[116] Unfortunately, the Court failed to extend the holding to situations other than searches incident to arrest, which is why it is now necessary to do so.

What is particularly unusual about the holding in *Riley* is that the Court seemedto reason that digital content stored in the Cloud deserves more constitutional protection in instances of a search incident to arrest than physical objects in possession of an individual.[117] This is unconventional because, generally, the Court has found that less constitutional protections exist incident to arrest, especially when officer safety is at issue.[118] In fact, this was the reasoning for the holding in the *Chimel v. California* series of cases that allow officers to rightfully search an individual's person incident to an arrest. The Supreme Court held:

> When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction.[119]

It may be that the Court does not expect the contents of a cell phone to be of significant risk to an officer's safety. However, it does not explain why a search of the cell phone's contents would not be permissible after an individual is arrested. Searches already occur regularly with cars that need to be impounded because of an individual's arrest.[120] In fact, one of the arguments made by the Court in *Riley* was that an individual would need a particularly large storage box to carry the number of records stored in a cell phone, and accessing such a box would require a warrant anyway.[121]

---

116. *Id.*at 2491 ("Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter.; See New York v. Belton, 453 U.S. 454, 460, n. 4, (1981) (describing a 'container' as 'any object capable of holding another object'). But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen.").

117. *Id.* at 2491 ("The United States concedes that the search incident to arrest exception may not be stretched to cover a search of files . . . stored in the cloud. Such a search would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house." (citations ommitted)).

118. *See generally, e.g.*, United States v. Robinson, 414 U.S. 218 (1973)

119. *Robinson*, 414 U.S. at 226 (quotation marks omitted) (quoting Chimel v. California, 395 U.S. 752, 762–763 (1969)).

120. *See e.g.*, *Belton*, 453 U.S. at 460–62 ("[W]e hold that when a policeman has made a lawful custodial arrest of the occupant of an automobile, he may, as a contemporaneous incident of that arrest, search the passenger compartment of that automobile.").

121. *See Riley*, 134 S. Ct. at 2489 ("Most people cannot lug around every piece of mail that they have received for the past several months, every picture they have taken, or every book or article they have read . . . if they did, they would have to drag behind them a trunk of the sort held to require a search warrant . . . .").

However, a car could easily fit this type of description and is searched regularly without a warrant.

In *Riley*, he Court is limits its holding to a very particular set of circumstances, possibly to limit the restrictions that it places on law enforcement's efforts. However, the Court's detailed analysis of why information stored in the Cloud requires such significant protections is inconsistent with its decision to limit the holding. Applying *Riley*'s holding much more broadly would set clear standards as to the protections digital information held in the Cloud should receive. In essence, this type of information should be treated the same way that most other property is treated under the Fourth Amendment: requiring a warrant to "search and seize." As noted in *Riley*, the argument in favor of allowing officers access to even the local contents (i.e. content stored on the phone as opposed to in the Cloud) of a cell phone in emergency situations requires extraordinary and even life-threatening circumstances.[122] The Court does not appear to apply the same logic to data accessible from a cell phone, but stored remotely.[123]

Apart from extending the holding in *Riley* to other situations, it is also time for the Supreme Court to hear any one of the number of cases dealing with electronic data, and set some type of precedent as to how different digital communications will be protected under the Fourth Amendment. The Court should look to the concurring opinion by Justice Sotomayor in *United States v. Jones*, which discusses the need to reconsider *Miller's* third-party disclosure doctrine in response to the use of modern technology.[124] The Court should also draw upon its assumptions in *City of Ontario v. Quon*, that digital property should be treated the same as its physical counterparts, to find in favor of equal protection for digital communications more generally.[125] In setting a standard, the Court will likely guide any legislative amendments to the SCA, as well as designate the limits of warrantless searches and seizures of digital property. If these changes had been implemented for Barbara in the earlier scenario,[126] she most likely would not have suffered from the public embarrassment and aftermath of the dissemination of her sensitive, private

122. *Id.* at 2493–94 ("[T]here is no reason to believe that law enforcement officers will not be able to address some of the more extreme hypotheticals that have been suggested: a suspect texting an accomplice who, . . . is preparing to detonate a bomb, or a child abductor who may have information about the child's location on his cell phone.").

123. *See id.* at 2491.

124. *See* United States v. Jones, 565 U.S. 400, 417 (2012) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." (citation omitted)).

125. *See* City of Ontario, Cal v. Quon, 560 U.S. 746, 760 (2010) ("Quon had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City . . . . [P]rinciples applicable to a government employer's search of an employee's physical office apply with at least the same force . . . in the electronic sphere.").

126. *Supra* Part I.

records because the SEC would not have been able to access the firm's records held by Amazon in the first place.[127]

B. Legislating to Replace or Amend the SCA

The Email Privacy Act is one piece of legislation circulating through Congress, which would amend the SCA.[128] Among other things, the bill amends the SCA such that a warrant would be required for every disclosure of content-based information held by a "third party [service provider] for any length of time."[129] The bill has been passed in the House of Representatives at the time this Note was written, and it is currently being considered by the Senate Committee on the Judiciary.[130] Should it pass, the bill would be an important step towards improving the current state of the SCA, but would not be a complete solution.

While an amendment requiring a warrant for every content-based disclosure may prove effective to significantly increase privacy rights, it would not limit law enforcement from using blanket warrants to access all digital content in possession of a service provider, even when the records are entirely irrelevant to the investigation. A better approach would be to also require some identifying information of the digital content being requested. For example, law enforcement can currently obtain any content-based information from RCSPs through administrative subpoenas, court orders, and with a warrant.[131] Additional requirements should be added that require warrants to specify certain properties of the digital records (e.g. file name, size, type, etc.) before a service provider would be compelled to disclose them. For example, if a bookie was under investigation, the government might list spreadsheet files as the document type in an attempt to find the suspect's client list. Adding this prerequisite would be more consistent with the Fourth Amendment's requirement that the government specify the places and things to be searched and seized.[132] The Email Privacy Act's warrant requirement is a favorable change to the current statute, but it would still need the additional requirements suggested here to ensure that law enforcement is not simply accessing documents through a catch-all method, as is currently allowable.

---

127. At least through the use of Section 2703, although the SEC may have other methods through which it can obtain records from regulated entities.

128. *See* Email Privacy Act, H.R. 387, 115th Cong (2017). At the time this Note was written, the Bill has passed the House of Represantatives, and has been referred to the Senate Judiciary Committee for further action. *See H.R.*387*—Email Privacy Act*, CONGRESS.GOV https://www.congress.gov/bill/115th-congress/house-bill/387/all-actions?q=%7B%22search%22%3A%5B%22email+privacy+act%22%5D%7D&r=1 [https://perma.cc/KT39-DFL7] (last visited Apr. 11, 2017).

129. *See* H.R. 387; *see also, e.g.*, James Stiven, *ECPA Reform Will Protect Privacy and Meet Law Enforcement Needs*, THE HILL:PUNDITS BLOG (June 02, 2016, 3:00 PM EST), http://thehill.com/blogs/pundits-blog/technology/281987-ecpa-reform-will-protect-privacy-meet-law-enforcement-needs [https://perma.cc/3ARW-BA5M].

130. *See See* Email Privacy Act, H.R. 387, 115th Cong (2017).

131. *See* 18 U.S.C. § 2703(b) (2012).

132. *See* U.S. CONST. amend. IV.

Additional amendments should be made to the SCA (or by enacting a new law) that gives NTIA the authority to regulate and classify who is considered as an ECSP or RCSP. Granting such authority to NTIA would create flexibility in regulation and enable the definition of ECSPs and RCSPs to adapt as technology continues to evolve. It would also serve as a way to limit law enforcement from overreaching in its use of warrantless searches and seizures. The NTIA, in particular, would be well suited to handle the classification of providers as it is an agency specializing in communications technology, and already regulates other areas of the Internet and communications law.[133] The SCA and ECPA categories overlap with the use of mobile phones and Internet, both of which are within NTIA's policy purview.[134] Also significant is that NTIA already works with public safety personnel, including law enforcement, through the FirstNet program to regulate emergency telecommunications networks, among other things.[135]

C. An Industry Effort to Promote Privacy Rights

Possibly the most effective solution to solve the lack of Fourth Amendment protection in developing technologies is a formal coalition among technology companies and Cloud service providers to encrypt data, such that not even the providers themselves can access it. This practice is already occurring on occasion, including some instances where the consumer is allowed to use his or her own private encryption key for data access and synchronization with the Cloud.[136] The encryption key is only known to the customer, and the company cannot access it even if it wanted to.[137] Apart from the privacy aspect of this solution, it would also have a secondary benefit of highly increased security for digital information, as the common mantra is that if a backdoor exists, it will eventually be accessible by more people than by which it was intended to be (e.g., hackers).

---

133. *See, e.g.*, *About NTIA*, NAT'L TELECOMM & INFO. ADMIN., https://www.ntia.doc.gov/about (last visited Apr. 18, 2018) ("[NTIA], located within the Department of Commerce, is the Executive Branch agency that is principally responsible by law for advising the President on telecommunications and information policy issues. NTIA's programs and policymaking focus largely on expanding broadband Internet access and adoption in America, expanding the use of spectrum by all users, and ensuring that the Internet remains an engine for continued innovation and economic growth. . . . Specific NTIA activities include: . . . Developing policy on issues related to the Internet economy, including online privacy, copyright protection, cybersecurity, and the global free flow of information online . . . In addition to working with other Executive Branch agencies to develop Administration positions, NTIA represents the Executive Branch in both domestic and international telecommunications and information policy activities.").

134. *See* 47 U.S.C. § 902 (2012).

135. 47 U.S.C. § 1424 (2012) (titled "Establishment of the First Responder Network Authority").

136. *See, e.g.*, *Features*, CRASHPLAN, https://www.crashplan.com/en-us/features/ [https://perma.cc/9MAF-AYC5] (last visited Apr. 04, 2017).

137. *See Public and Private Keys*, COMODO GROUP, INC., https://www.comodo.com/resources/small-business/digital-certificates2.php [https://perma.cc/F5YQ-8Q4W] (last visited Apr. 2, 2017).

This solution does have its flaws. For one, it would require broad acceptance across the technology and Cloud communities. For those companies that do have access to the Cloud content information of their clients, it would mean losing valuable, marketable information that is often sold or used to improve and develop products—and for smaller companies, such a practice would likely be economically unfeasible. Second, as seen with the Department of Justice breaking into the iPhone of the San Bernardino shooter, [138] it is likely that the government may find its own way to break the encryption.[139] However, the industry may respond by developing stronger encryption standards. Overall, this solution appears to be more of an ideal objective for Cloud service providers to continue working towards rather than a comprehensive solution to resolve the issues with the SCA. This type of solution may also serve as a competitive advantage for companies that can provide privacy assurances to its customers, and even sell them for a fee.

VI. CONCLUSION

When the Stored Communications Act was originally enacted in 1986, digital technology was much simpler than in today's world. Where e-mail was at the frontier of communications technology then, it is now commonplace, and is, for the most part, beginning to overtake mail as the primary form of official communication. Today, people use apps, messaging services, web pages, and other technologies to communicate, both formally and informally, with one another—most of which rely on Cloud technology in some way. Lacking in this technological evolution have been revisions to the SCA that take into consideration how older technologies are being used in new ways, and how new technologies change the behavior of society. Elucidated by the lack of reform is just how vulnerable an individual's private and sensitive information is to intrusion by the government, and to dissemination to the public. It is vital that SCA reform be implemented immediately, so that situations like Barbara's do not prevent individuals from embracing technology and all the benefits that it brings to society.

138. Kevin Johnson et al., *FBI hacks into terrorist's iPhone without Apple*, USATODAY (Mar. 28, 2016) https://www.usatoday.com/story/news/nation/2016/03/28/apple-justice-department-farook/82354040/ [https://perma.cc/8W3E-78U5]

139. Cloud service providers would still likely be accountable for providing the encrypted files to the government without amending the current form of the SCA.

Brace Yourself, Voluntary Commitments Are Coming: An Analysis of the FCC's Transaction Review

Michael Farr *

TABLE OF CONTENTS

* J.D. Candidate, The George Washington University Law School, May 2018. Associate, *Federal Communications Law Journal*. B.A., UCLA 2014. I want to thank my parents, Harvey and Elizabeth, for their love and support, and raising me to be the person I am today.

I. INTRODUCTION

Imagine you walk into the offices of an unelected regulatory body tasked with setting policy at the highest levels. They've been busy crafting rules and regulations, but the slow process has reached a boiling point. Some are willing to do whatever it takes to speed up the process – including throwing the rulebook out altogether. You tell the regulators they don't need to look beyond its enabling statute, which allows them to make policy in an alternative fashion without the mess of following statutorily prescribed procedures or subjecting their decisions to the courts. The regulators say it sounds too good to be true, and asks if this is limitless authority. You reply with an emphatic "yes!" They then ask a follow-up question. Can we coerce American businesses in transactions to bend to our policy at-will? You once again reply in the affirmative and leave them with a newfound purpose and way of doing business.

As stakeholders who care deeply about the rule of law, this situational exaggeration of an example would be just how it sounds – fictional and silly. However, some have argued that it is closer to reality than we would like to think, particularly when it comes to the Federal Communications Commission ("FCC"). Over the course of many years, the independent agency has relied upon a single statutory provision to carve out for itself a role in reviewing communication industry transactions valued in the tens of billions of dollars, and in the process, imposes binding obligations ranging from digital literacy programs to mandated disaster relief donations. The agency has become more interested in using its ancillary antitrust authority as a first option to craft policy, rather than through their primary powers prescribed in the Administrative Procedures Act ("APA").

As a vast majority of the American legal community has come to accept, the administrative state must fit comfortably within the executive branch under Article II of the United States Constitution in order to survive a basic constitutional inquiry.[1] That is not to say that administrative agencies have always stayed in their lane.[2] Skeptics are often quick to label the administrative state as a "headless [f]ourth [b]ranch" of government when there is a perception of agency overreach.[3]

---

1. Morton Rosenberg, *Congress's Prerogative over Agencies and Agency Decisionmakers: The Rise and Demise of the Reagan Administration's Theory of the Unitary Executive*, 57 GEO. WASH. L. REV. 627, 651 (1989).

2. *See generally*, A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495 (1935); Panama Refining Co. v. Ryan, 293 U.S. 388 (1935) (both finding a violation of the non-delegation doctrine).

3. F.C.C. v. Fox Television Stations, Inc., 556 U.S. 502, 525-26, 129 S. Ct. 1800, 1817, 173 L. Ed. 2d 738 (2009) (Scalia, J., opinion) ("There is no reason to magnify the separation-of-powers dilemma posed by the headless Fourth Branch by letting Article III judges—like jackals stealing the lion's kill—expropriate some of the power that Congress has wrested from the unitary Executive.").

The FCC's transaction review authority embodies this skepticism as it is tied to a vague public interest standard.[4] Among the FCC's statutory powers, reviewing transfers of licenses is unlike some other agencies that tend to review major transactions.[5] In applying this standard, the FCC has developed a unique tool – the voluntary commitment –to extract broad commitments from communications companies in transactions.[6] This, in turn, enables the FCC to use voluntary commitments as a mechanism to achieve public policy goals without going through the APA processes, and without sufficient judicial review.

The FCC circumvents the built-in checks and balances of the APA by achieving public policy goals through the imposition of voluntary commitments. This Note asserts that voluntary commitments are coercive because the FCC's approval of a transaction hinges on the acceptance of these terms. These voluntary commitments become conditions or effectively consent decrees, exempted under the APA or not, upon which noncompliance would result in the serious harm of revocation of a deal. This yields enormous discretion on the part of the FCC to further its own policy goals while circumventing procedural protections and adding an element of uncertainty about whether these conditions can be the subject of judicial review.

Therefore, this Note argues that the FCC's public interest standard, the preferred mechanism in achieving public policy goals, has been used to extract voluntary commitments from parties to a transaction, and this process for policy formation falls outside of lawful policymaking. In order to curb this overreach, Article III courts must have the final say on whether parties should contest to a commitment's imposition. At least one antitrust authority allows for judicial review in consent decree cases and there is no reason to think that voluntary commitments should operate any differently.[7]

Accordingly, Section II of this Note provides the basic underpinnings of the FCC's transaction review authority. Section III offers examples that illustrate the FCC's overreach in imposing voluntary commitments to circumvent agency law, and the hurdles for reviewability of these commitments. Finally, Section IV contends that this abuse must be checked by the courts and offers arguments for why judicial review is appropriate in transaction review.

II. THE FCC'S LEGAL FRAMEWORK FOR REVIEWING COMMUNICATION INDUSTRY TRANSACTIONS

The FCC has statutory authority to review transfers of licenses it has issued, including in the case of a merger or acquisition among licensees, all

4. *See infra* note 17.
5. *See infra* note 9.
6. *See infra* note 39.
7. Antitrust Procedures and Penalties Act (Tunney Act) Pub. L. 93–528, 88 Stat. 1708, enacted December 21, 1974, 15 U.S.C. § 16

of which are reviewed based on a public interest standard.[8] The traditional manner in which the FCC achieves its policy goals is through formal APA rulemaking. Typically, Article III courts can review agency actions in promulgating policy this way. Another way in which the FCC crafts policy is through imposing voluntary commitments on transactions involving licenses in order to win its approval. A rich amount of case law has developed on whether courts can review agency "no action" decisions (like not prosecuting a case), as opposed to traditional actions (like rulemaking). Reviewability depends on the characterization of the decision. It is not clear whether the imposition of voluntary commitments is an action or no action. In order to properly understand the constitutional issues surrounding the FCC's transaction review authority, it is necessary to understand how the FCC crafts rules and regulations to enact policy.

A. Overview of the FCC's Antitrust Mandate to Review Transactions

In most industries, either the Federal Trade Commission ("FTC") or the Department of Justice ("DOJ") reviews big transactions to assess their compliance with antitrust laws.[9] Under the Hart-Scott-Rodino Act, the FTC and DOJ review proposed transactions that affect interstate commerce and may take legal action to prevent mergers that the agencies think "substantially lessen competition." [10] By contrast, the FCC reviews transactions relating to its jurisdiction, including the transfer of licenses granted to communications companies, under the Communications Act of 1934.[11] If there are no transfers of licenses, the FCC is without jurisdictional authority to approve or deny the merger, as the FTC or DOJ would instead be the relevant agency to conduct the review.[12] While the statute does not explicitly grant transaction or merger review authority, the FCC has treated incidental license transfers as a means to evaluate and approve communication industry transactions and mergers.[13] The FCC approves the transaction as long as it serves "the public interest, convenience, and

8. 47 U.S.C. § 309-10.

9. James R. Weiss, Martin L. Stern, *Serving Two Masters: The Dual Jurisdiction of the FCC and the Justice Department over Telecommunications Transactions*, 6 COMM. LAW CONSPECTUS 195 (1998)

10. FTC, Merger Review. Last accessed April 3, 2017. https://www.ftc.gov/news-events/media-resources/mergers-and-competition/merger-review

11. 47 U.S.C. § 151 et seq.; *see also* Weiss, *supra* note 9, at 197.

12. Lawrence M. Frankel, *The Flawed Institutional Design of U.S. Merger Review: Stacking the Deck Against Enforcement*, 2008 UTAH L. REV. 159, 200 (2008).

13. *Novel Procedures in FCC License Transfer Proceedings: Hearing Before the Subcomm. on Commercial and Administrative Law Oversight of the H. Comm. on the Judiciary*, 106th Cong. (1999) (statement of Harold W. Furchtgott-Roth, FCC Commissioner), https://transition.fcc.gov/Speeches/Furchtgott_Roth/Statements/sthfr925.html#N_1_ ("[M]ost orders involving mergers do not even identify the radio licenses or section 214 authorizations at issue or discuss the consequences of their conveyance, but instead move directly to a discussion of the merger…").

necessity."[14] Those seeking approval bear the burden of proving the transaction enhances the public interest.[15]

In transactions involving telecommunications firms, agencies ranging from public utility commissions to international antitrust authorities could be involved to review a wide array of potential concerns.[16] Arguably, no government agency has more discretion in their review than the FCC.[17] This is so because the FCC reviews big transactions under a "public interest standard"[18] – a more expansive standard of review than the FTC or DOJ's competition-based review.[19]

The broad scope of the FCC's standard in transaction review is well understood. The Supreme Court has characterized the FCC's public interest standard as a "supple instrument for the exercise of discretion by the expert body which Congress has charged to carry out its legislative policy."[20] The FCC claims that the public interest standard focuses on maintaining "competition, diversity, localism," encouraging advancements in technology, and the potential benefits to the public that a transaction would bring about.[21] In giving its approval or disapproval of transactions, the FCC inherently makes policy decisions.

Under its governing statutes, the Communications Act of 1934 and the APA, the FCC formally makes policy through its delegated rulemaking authority.[22] However, under the public interest standard, the FCC has carved out an alternate path of policymaking, outside the confines of APA rulemaking procedures. The FCC accomplishes this alternate policymaking through the extraction of "voluntary" commitments (or conditions for FCC approval) from the parties to a transaction under review.[23]

B. How the FCC Achieves the Public Interest: Modes and Actions

There are three ways in which the FCC applies its public interest standard in transaction review under the APA: through rulemaking, non-legislative rules, and adjudication. Rulemaking is an agency statement of

14. 47 U.S.C. § 252 (e)(2)(A)(ii)

15. 47 U.S.C. § 157 (a).

16. David A. Curran, *Rethinking Federal Review of Telecommunications Mergers*, 28 OHIO N.U. L. REV. 747, 748 (2002)

17. J. Brad Bernthal, *Procedural Architecture Matters: Innovation Policy at the Federal Communications Commission*, 1 TEX. A&M L. REV. 615, 635 (2014)

18. 47 U.S.C. § 310(d) ("[U]pon application to the Commission and upon finding by the Commission that the public interest, convenience, and necessity will be served thereby.").

19. Rachel E. Barkow, Peter W. Huber, *A Tale of Two Agencies: A Comparative Analysis of FCC and DOJ Review of Telecommunications Mergers*, 2000 U. CHI. LEGAL F. 29, 29 (2000).

20. F.C.C v. WNCN Listeners Guild, 450 U.S. 582, 593, 101 S. Ct. 1266, 1274, 67 L. Ed. 2d 521 (1981).

21. Federal Communications Commission, Frequently Asked Questions. https://www.fcc.gov/reports-research/guides/mergers-frequently-asked-questions (last visited Apr. 7, 2017) [https://perma.cc/F4HZ-BQ73].

22. *See supra* note 17 at 635-36.

23. *See infra* Sec. III.A.

policy that is designed to implement, interpret or preserve a law or existing policy.[24] Rulemaking can either be a formal, on the record proceeding or an informal procedure requiring notice and comment, depending on the organic act.[25] Although not binding, the agency may also publish non-legislative rules that interpret existing rules, issue general statements of policy, or are rules of agency organization, practice, or procedure.[26] These non-legislative rules are exempt from notice and comment procedures.[27] The FCC traditionally conducts informal rulemaking but may also adjudicate claims as a means of exercising their investigatory and/or enforcement powers.

Adjudication is the whole or part of a final disposition, whether affirmative, negative, injunctive, or declaratory in form, of an agency in a manner other than rulemaking but including licensing.[28] Adjudication is usually a formal, on the record proceeding but can also be informal, requiring fewer formalities than a hearing. When the FCC uses adjudication, it is normally formal adjudication. Lastly, the public has an important role in making their grievances heard with regards to policymaking. Therefore, under 5 U.S.C. § 553(c), an interested person has the right to petition for the issuance, amendment or repeal of a rule.

C. Policymaking Through Voluntary Commitments in Communication Industry Transactions

The easiest way to explain policymaking through the imposition of voluntary commitments in communications industry transactions is by imagination. Suppose for a moment that you are an executive at a major communications company in Los Angeles and you are making a proposal to the acquisitions team to purchase a large amount of local television and radio stations in Chicago. Expect to prepare for your proposal how this purchase will ultimately positively impact the public interest. If you can't see how this purchase will positively shape the community-at-large, don't worry – the FCC will propose a host of actions your communications company may take and maintain, for years, in order to win their approval of your transaction. It remains your choice to abide by these commitments, as the FCC says they are just voluntary. But be careful, if you don't accept their terms and abide by them for the duration of the commitment, the deal is off.

This is the scenario that most communications companies face in a given transaction– the imposition of voluntary commitments in order to win approval of a merger or large-scale transaction involving the transfer of licenses. By invoking its public interest standard, the FCC pursues a different form of policymaking when conducting transaction reviews. The

24. 5 U.S.C. § 551 (5).
25. 5 U.S.C. § 553 (c).
26. 5 U.S.C. § 553 (b)(A).
27. 5 U.S.C. § 553 (b)(A).
28. 5 U.S.C. § 554 (a).

FCC pounces on the chance for quick and easy policymaking when negotiating with parties, particularly on the extent to which the communications companies must make commitments that are often outside the merits of the transaction itself. Some have expressed concern about the FCC's use of the public interest standard to effectuate policy.[29] Harsher critiques have coined it "jawboning," coercing companies using informal regulation and threats under vague standards.[30] Using these informal enforcement mechanisms hides what, in reality, is state action cloaked in private choice. Such regulation in case-by-case transactions has produced harsh legal and constitutional effects.[31]

Since these voluntary commitments are not enacted in accordance with the APA, the issue of whether a party to a transaction may later contest the imposed conditions is unclear. Aside from complaints that can arise when parties sit down to negotiate a deal (such as fraud in inducement or bad faith that can normally give rise to litigation), it is unsettled whether a condition imposed by the FCC would constitute a final agency action that is reviewable. The question remains, should transactions ending in voluntary commitments be thought of more as agency actions subject to judicial review, or more like no action decisions that are presumptively unreviewable? If the latter is true, can we analogize to any other agency decision-making powers where judicial review is available even in the absence of the APA?

III. ESTABLISHING THE OVERREACH OF VOLUNTARY COMMITMENTS AND THE ROAD TO REVIEWABILITY

The FCC's overreach is proven by the imposition of voluntary commitments that are wholly outside, or ancillary at best, to the merits of a communications industry transaction. A snapshot of a few transactions listed below highlights this notion. In order to remedy these perceived abuses, the actions must be reviewable by a court of law. Classifying transaction review under the public interest standard, either as an agency action or no action, remains a hurdle towards reviewability. While decisions committed to agency discretion by law are presumptively unreviewable, case law has emerged that could rebut this presumption for voluntary commitments. Lastly, these commitments could also be seen in a light akin to settlement negotiations or consent decrees in order to obtain reviewability.

---

29. Tim Wu, *Agency Threats*, 60 DUKE L.J. 1841, 1855 (2011).

30. Christopher Yoo, *Merger Review by the Federal Communications Commission: Comcast–NBC Universal*, 45 REV. IND. ORGAN. 295, 312 (2014) (noting that since 2004, "conditions have become increasingly common features of [FCC] merger clearances); *see also* Derek E. Bambauer, *Against Jawboning*, 100 MINN. L. REV. 51, 126 (2015) ("Jawboning of Internet intermediaries is increasingly common, and it operates beneath the notice of both courts and commentators."); T. Randolph Beard et al., *Eroding the Rule of Law: Regulation as Cooperative Bargaining at the FCC* 5 (Phoenix Center, Policy Paper No. 49, 2015), http://www.phoenix-center .org/pcpp/PCPP49Final.pdf.

31. Derek E. Bambauer, *Against Jawboning*, 100 MINN. L. REV. 51, 65 (2015).

A. The FCC's Imposition of Voluntary Commitments is De Facto Rulemaking

According to the FCC's then-General Counsel Jon Sallet, transaction review starts with a thorough review of the proposed transaction to determine whether it serves the public interest.[32] Approval of the deal may be conditioned on the parties taking on voluntary commitments to please the public interest standard.[33] Violating the voluntary commitments after agreement may result in fines or revocation of the deal.[34] If the FCC is unable to approve the transaction, the agency assigns the case to an administrative hearing.[35] After the hearing, the FCC makes a final decision that is subject to judicial review.[36] However, the costs associated with the pre-hearing approval process usually deters parties from ever getting to an administrative hearing.[37] Nevertheless, under the public interest standard, the FCC uses its transaction authority to engage in de facto rulemaking.

If an agency can increase its jurisdiction and ease the way it creates regulations, then the FCC's reliance on the public interest standard to create rules would be the most effective way for agencies to maximize power.[38] The FCC's use of this legal standard to achieve policy goals unrelated or ancillary to a transaction represents de facto rulemaking. The below examples illustrate the following two fundamental considerations. First is to consider how closely related the conditions related to the transaction are, and second, whether the FCC could have equally accomplished what the commitments set out to address through the formalities of the APA. While there is a lot of uncertainty as to why the FCC chooses de facto rulemaking

---

32. Jon Sallet, *FCC Transaction Review: Competition and the Public Interest*, FCC (Aug. 12, 2014), https://www.fcc.gov/news-events/blog/2014/08/12/fcc-transaction-review-competition-and-public-interest.

33. Mergers and Acquisitions, FCC, https://www.fcc.gov/proceedings-actions/mergers-and-acquisitions (last visited Mar. 12, 2017) ("The Commission reviews applications for the transfer of control and assignment of licenses and authorizations to ensure that the public interest would be served by approving the applications. The vast majority of transfer of control and assignment applications are simple and unopposed and are processed quickly. Some transactions, however, present more complex legal, economic or other public interest issues and are likely to elicit a significant amount of public comment, thus requiring more extensive Commission review.").

34. Georg Szalai, *FCC Fines Comcast for Violation of NBCUniversal Deal Condition*, HOLLYWOOD REPORTER (June 28, 2012), http://www.hollywoodreporter.com/comcast-fcc-fine-broadband-nbcuniversal-13353 [https://perma.cc/NL6D-H2QS].

35. Practically speaking, such a hearing rarely sees the light of day as this step is akin to a death sentence for the deal. Parties cut their losses at this point and back away.

36. Jon Sallet, *FCC Transaction Review: Competition and the Public Interest*, FCC (Aug. 12, 2014), https://www.fcc.gov/news-events/blog/2014/08/12/fcc-transaction-review-competition-and-public-interest ("Although such hearings have been rare, the Commission has been ready to use them as the statute requires. For example, at the time that the applicants in the AT&T/T-Mobile merger withdrew their applications, the Commission's staff had prepared a report recommending that the transaction be designated for hearing.").

37. Brent Skorup & Christopher Koopman, *How FCC Transaction Reviews Threaten Rule of Law and the First Amendment*, 77 GEORGE MASON U. 35, 66 (2016)

38. *Id.*

over APA rulemaking, it is important to judge them on a sliding scale. On one extreme is a blatant disregard for APA procedures and a clear unconstitutional overreach of power. On the other is an entirely appropriate and necessary component to their statutory authority to review transactions in the public interest.[39]

1. AT&T/BellSouth

In 2006, AT&T purchased BellSouth for $86 billion and signed on to 11 pages of voluntary commitments.[40] Some of the commitments directly addressed the FCC's concerns regarding competitiveness, which arguably is the primary issue in transaction review.[41] AT&T agreed to adhere to net neutrality principles for two years and divest from BellSouth's spectrum holding.[42] However, other commitments were completely unrelated to the transaction itself. For instance, AT&T agreed to make disaster recovery capabilities available in BellSouth's territory and to donate $1 million toward supporting public safety initiatives.[43] The public safety initiatives stemmed from a 2006 FCC panel recommendation on how telecommunications firms could more effectively address potential disaster relief.[44] In addition, the agreement required AT&T to report to the FCC on how it serves customers with disabilities. This was an issue the FCC had problems implementing since the passage of the American with Disabilities Act ("ADA") in 1990.[45] Lastly, AT&T agreed to bring some outsourced jobs back to America and cut rates charged to competitors requesting to lease high-speed data lines.[46] The latter commitment was instrumental for the FCC because it failed to reform special access feels across telecommunications firms.[47]

---

39. This Note doesn't challenge the FCC's determination that these actions actually were in the public interest, and in fact the companies might have taken these steps anyway. However, the point of this assessment is to illustrate how the FCC is achieving these policy goals outside of the normal process.

40. Julie Vorman, *AT&T closes $86 billion BellSouth deal*, REUTERS (Jan 21, 2017), https://www.reuters.com/article/businesspro-bellsouth-fcc-dc/att-closes-86-billion-bellsouth-deal-idUSWBT00636120061230.

41. *See AT&T Inc. and BellSouth Corporation Application for Transfer of Control*, WC Docket No. 06-74, Memorandum Opinion and Order, FCC 06-189 (rel. Mar. 26, 2007) (AT&T/BellSouth Merger Order) (Commissioner McDowell not participating).

42. *Id.*

43. *Id.* at 148.

44. WILEY REIN & FIELDING, REPORT AND RECOMMENDATIONS OF THE INDEPENDENT PANEL REVIEWING THE IMPACT OF HURRICANE KATRINA ON COMMUNICATIONS NETWORKS, (June 2011), http://transition.fcc.gov/pshs/docs/advisory/hkip/karrp.pdf.

45. Gwen Lisa Shaffer & Scott Jordan, *Classic Conditioning: the FCC's use of merger conditions to advance policy goals*. 35 MEDIA CULTURE AND SOCIETY 392, 396 (2013).

46. *See supra* note 41, at 147.

47. Surely there are financial and business benefits for AT&T and others to provide Internet access and other services to the disabled and other groups of people. However, the issue is about parties coming to terms with these ideas on their own volition.

It is clear that commitments to ensure competitiveness was an appropriate use of the FCC's power. With AT&T's purchase of BellSouth, AT&T would assume too much power in spectrum access and lead to anti-competitive concerns. The divestiture requirement was closely related to the merits of the transaction and could be effectively and legally required through the FCC's transaction authority. This particularized divestiture requirement was more appropriate to go through with their transaction review authority than an APA adjudication for the sake of efficiency, and because there were no facts in dispute.

However, some of the remaining conditions show the relative ease with which the FCC utilizes its transaction review authority when it cannot accomplish policy goals through the rulemaking process. This is illustrated in the disaster relief donation, which has nothing to do with the merger's merits but stemmed from a recommendation of an earlier panel on how best to address public safety the FCC wouldn't issue an industry-wide rule mandating donations, considering corporations play a special role in social reform. Instead, the FCC reserved the donation mandate in order to bend parties to its particular charitable interests. [48]

2. Ameritech/SBC

One particular example of the FCC's choice of transaction authority over traditional rulemaking procedures was the Ameritech and SBC merger at the turn of the millennium. In negotiating with the FCC, Ameritech and SBC agreed to provide advanced services to customers through a separate affiliate in order "to ensure that competing providers of advanced services receive effective, nondiscriminatory access to the facilities and services of the merged firm's incumbent local exchange carriers."[49] While on its face this looks like a perfectly legitimate exercise of transaction authority on the part of the FCC, a further inquiry reveals the FCC's true motives. At the time the FCC was negotiating this deal, a similar policy was being considered for rulemaking, which was to apply to the entire industry.[50] Presumably foreseeing a stall in the enactment of the regulation, the FCC anticipatorily attached it as a condition to the Ameritech/SBC merger.[51]

---

48. Gwen Lisa Shaffer & Scott Jordan, *Classic Conditioning: the FCC's use of merger conditions to advance policy goals*. 35 MEDIA CULTURE AND SOCIETY 392, 396 (2013).

49. Applications of Ameritech Corp., Transferor, and SBC Communications, Inc., Transferee, For Consent to Transfer Control of Corporations Holding Commission Licenses and Lines Pursuant to Sections 214 and 310(d) of the Communications Act and Parts 5, 22, 24, 25, 63, 90, 95, and 101 of the Commission's Rules, CC Docket 98-141.

50. *See* Deployment of Wireline Services Offering Advanced Telecommunications Capability, *Memorandum Opinion and Order and Notice of Proposed Rulemaking*, 13 FCC Rec 24011, 24051-64, 85-117 (1998).

51. Rachel E. Barkow, Peter W. Huber, *A Tale of Two Agencies: A Comparative Analysis of FCC and DOJ Review of Telecommunications Mergers*, 2000 U. CHI. L.F. 64 (2000).

In his concurrence, then-Commissioner Harold Furchtgott-Roth criticized the FCC's position of imposing these conditions in many ways that this Note aims to do. For instance, he warned that imposing conditions to alleviate "harms so vague and speculative that the actual nexus between those harms and the remedies imposed is difficult to ascertain[,] . . . creates problems of fair notice, increases the potential for arbitrary decision-making, and implicates the non-delegation doctrine."[52] More importantly, Furchtgott-Roth points out that the conditions require conduct by the parties "that it could not require outright in a rulemaking[,] creates new processing schemes to suit [the FCC's] fancy in individual transfer proceedings, [and] raise[s] questions about the neutrality of [the FCC's] decision-making."[53]

3. Comcast/NBC Universal

The imposition of voluntary commitments on media transactions reached an apex in the Comcast and NBC-Universal merger. In January 2011, the DOJ and FCC imposed one of the most onerous voluntary commitments of any cable deal in its history in approving the Comcast/NBC-Universal merger. In negotiating with the FCC, Comcast and NBC-Universal agreed to a host of conditions requiring it to purchase new weekly business news programs, expand local and public interest programing, enter into agreements with local nonprofit news organizations, provide 1500+ choices of video-on-demand children's programming, and spend $15 million yearly on digital literacy, FDA nutritional guidelines, and childhood obesity on networks that have young family audiences.[54] Undeniably, the list is extensive. It is worth noting that the FCC would later fine Comcast $800,000 for noncompliance with one of these conditions.[55] While it is almost indisputable that these conditions have sufficient public interest benefits, it is clear that the FCC went wild with their transaction review authority.

For example, "the 'Internet Essentials' program incorporated into the merger agreement ensures that every household in Comcast's footprint with children eligible for the federal free lunch program qualifies for 'economy' broadband service for $10 per month, a $150 PC, and access to digital

52. Applications of Ameritech Corp., Transferor, and SBC Communications, Inc., Transferee, For Consent to Transfer Control of Corporations Holding Commission Licenses and Lines Pursuant to Sections 214 and 310(d) of the Communications Act and Parts 5, 22, 24, 25, 63, 90, 95, and 101 of the Commission's Rules, CC Docket 98-141.

53. *Id.*

54. Applications of Comcast Corp. and NBCUniversal, For Consent to Transfer Control of Licenses, MB Docket No. 10-56, FCC 11-4 (Jan. 18, 2011), https://www.fcc.gov/proceedings-actions/mergers-transactions/comcast-corporation-and-nbc-universal-mb-docket-10-56.

55. Georg Szalai, *FCC Fines Comcast for Violation of NBCUniversal Deal Condition*, HOLLYWOOD REPORTER (June 28, 2012), http://www.hollywoodreporter.com/comcast-fcc-fine-broadband-nbcuniversal-13353.

literacy training." [56] It is clear that this condition did not relate to competitiveness, which should dominate merger review by the FCC. Instead, it directly advanced the FCC's digital inclusion goals incorporated in the National Broadband Plan in 2010 and was wholly outside the merits of the transaction itself.[57] Additionally, the company's promise to "establish three-year partnerships between non-profit news organizations and at least five NBC-owned television affiliates" was not based on the merits of the transaction.[58] In fact, this condition stems from a 2009 Senate hearing on journalism and was previously introduced in the Newspaper Revitalization Act.[59] Lastly, the parties agreed that 10 NBC-owned stations would produce an additional 1000 hours of original local news programming, with Telemundo (Spanish) getting a new multicast channel.[60] The focus on increasing Spanish stations' airtime could be traced not to the merits of the transaction, but to then-FCC Commissioner Kevin Martin, who in front of the Congressional Hispanic Leadership institute called for the FCC's "special responsibility" to engage Spanish-speaking viewers.[61] Most, if not all, of the conditions imposed on this merger should have been enacted under the APA because they were so far outside the merits of the deal. Evidently, the FCC's overreach was more prominent and blatant than previously thought possible.

B. The Concept of Reviewability: Agency Action and No-Action

For the purposes of this Note, whether agency decisions are subject to judicial review largely hinges on the characterization of the agency decision to act or not to act. For the most part, the courts have held that agency actions are presumptively reviewable, while agency no action is presumptively unreviewable, if those decisions are committed to agency discretion by law. However, there is a small possibility of getting judicial review of agency no actions. Characterizing where voluntary commitments lie on the spectrum of agency actions or no actions is therefore fundamental in order to understand which legal framework to apply.

---

56. Applications of Comcast Corp., Gen. Elec. Co., and NBC Universal for Consent to Assign Licenses and Transfer Control of Licenses, *Memorandum Opinion and Order*, FCC 11-4, para. 6 (2011) [hereinafter *Comcast Order*], https://www.fcc.gov/proceedings-actions/mergers-transactions/comcast-corporation-and-nbc-universal-mb-docket-10-56.

57. Gwen Lisa Shaffer & Scott Jordan, *Classic Conditioning: The FCC's Use of Merger Conditions to Advance Policy Goals*, 35 MEDIA, CULTURE & SOCIETY 392, 399 (2013).

58. *Id.*

59. *Id.*

60. Applications of Comcast Corp. and NBCUniversal, For Consent to Transfer Control of Licenses, MB Docket No. 10-56, FCC 11-4 (Jan. 18, 2011), https://www.fcc.gov/proceedings-actions/mergers-transactions/comcast-corporation-and-nbc-universal-mb-docket-10-56.

61. Gwen Lisa Shaffer & Scott Jordan, *Classic Conditioning: The FCC's Use of Merger Conditions to Advance Policy Goals*, 35 MEDIA, CULTURE & SOCIETY 392, 400 (2013).

1. Decisions Committed to Agency Discretion by Law are Unreviewable

Under § 551 of the APA, agency action is an "agency rule, order, license, sanction, [grant or denial of] relief, . . . or a failure to act."[62] An agency action is final when there is a final disposition of a matter,[63] which the Supreme Court in *Bennett v. Spear* more fully defined as, "the 'consummation' of [an] agency's decisionmaking process . . . and when 'rights or obligations have been determined,' or from which 'legal consequences will flow.'"[64] The issuance of a rule or an order, or the denial of a petition, is considered a final agency action that is ripe for judicial review by any person adversely affect or aggrieved by the agency action.[65] [66]

The APA provides two exceptions to the general rule on reviewability. Section 701(a)(1) provides that an agency's organic statute can preclude review and § 701(a)(2) states that agency action committed to agency discretion by law is unreviewable.[67] Section 701(a)(2) is contentious, in part, by the inconsistency presented in the "scope of review" section of the APA. The "scope of review" section, § 706(a)(2), allows for judicial review of agency abuse of discretion.[68] The obvious question is: how can the courts review an agency's abuse of discretion if § 701(a)(2) precludes review of agency action committed to agency discretion by law?

The courts have wrestled with this idea first in *Citizens to Preserve Overton Park, Inc. v. Volpe*, 401 U.S. 402 (1971). In *Overton Park*, plaintiffs alleged that the Secretary of Transportation did not take "feasible and prudent" measures as required by the governing statute before approving the construction of a highway through a public park.[69] The citizen group claimed that not making formal findings was a violation of the Secretary's organic statute. The Supreme Court found this to be an "action" by an agency and entitled it to judicial review because the "feasible and prudent" standards established that there was "law to apply."[70] The Court latched on to legislative history to hold that when a statute has "no law to apply," agency actions would be unreviewable under § 701(a)(2), as that would be committed to agency discretion by law.[71] However, the circuit courts were confused over whether the "no law to apply" test only applied in

62. 5 U.S.C. § 551(13).

63. Jason Fowler, *Finality, What Constitutes Final Agency Action*, 24 J. NAT'L ASSN. ADMIN L. JUDICIARY 311,315 (2004).

64. Bennett v. Spear, 520 U.S. 154, 178 (1997).

65. 5 U.S.C. §§ 702, 704.

66. While other elements (such as mootness, ripeness, and standing) must be met in order to satisfy reviewability, such considerations are assumed for the purposes of this note, as they are not the focus here.

67. 5 U.S.C. § 701(a).

68. 5 U.S.C. § 706 (a)(2).

69. *Overton Park*, 401 U.S. at 405–06.

70. *Id.* at 413.

71. *Id.* at 410.

cases relating to an agency's organic statute, or whether the presence of an abuse of discretion standard, such as the APA's, would be considered a "law to apply." The Third and Ninth circuits would find that as long as there was an abuse of discretion standard, there will always be "law to apply."[72] Conversely, the Eleventh circuit ruled that if the statute or other sources of law do not limit an agency's discretion, then there is "no law to apply."[73] The Supreme Court would later step in to reaffirm its "no law to apply" standard but would also introduce an independent factor analysis to help guide its decision on whether no-action decisions are presumptively unreviewable.

2. Heckler v. Chaney: Four Factors to Overcome the Presumption of Unreviewability in Decisions Committed to Agency Discretion by Law

In *Heckler v. Chaney*, the Supreme Court articulated four factors to overcome the presumption of unreviewability in decisions committed to agency discretion by law. In the case, prisoners on death row had petitioned the Food and Drug Administration ("FDA") to remove drugs used for lethal injects from the safe drug list, as such listings violated the Food, Drug, and Cosmetic Act.[74] The petitioners asked the FDA to step in to stop the use of these drugs, but the agency denied the request.[75] This made the action reviewable in federal court. The Supreme Court, however, found that denying a request to take an enforcement action was presumptively unreviewable under § 701(a)(2), and that all no-action decisions are therefore presumptively unreviewable.[76] The Court arrived at this decision first by reiterating its "no law to apply" standard from *Overton Park*, holding that when a "statute is drawn so that a court would have no meaningful standard against which to judge the agency's exercise of discretion," that action is unreviewable.[77] Then, without providing a clear relationship to the "no law to apply" standard, the Court laid out four principles to help decide if agency action is committed to agency discretion by law. The considerations were whether there was a complicated balancing of agency interest (such as resource allocations), refusals to act generally are not coercive and infringe on private interests, lack of focus for judicial review, and an analogy to prosecutorial discretion.[78]

---

72. Chehazeh v. Attorney Gen. of the U.S., 666 F.3d 118, 128–30 (3d Cir. 2012); Pinnacle Armor, Inc. v. United States, 648 F.3d 708, 720 (9th Cir. 2011).

73. Conservancy of Sw. Fla. v. U.S. Fish & Wildlife Serv., 677 F.3d 1073, 1082 (11th Cir. 2012).

74. 470 U.S. 821, 823-24 (1985).

75. *Id.*

76. *Id.* at 832-33.

77. *Id.* at 830.

78. *Id.* at 831-32; *See also infra* note 79.

The first factor of whether there was a complicated balancing of agency interest is the factor most frequently employed and discussed of the four.[79] Courts traditionally defer when they feel that the agency is more equipped to pick and choose how to use its resources in carrying out its mandate. For instance, in *Heckler*, the Court looked favorably upon the FDA being able to choose how it allocates its resources by focusing on new drugs and unhealthy foods, rather than products that were not controversial, such as the lethal injection drugs. However, at least one court has not as readily accepted a resource allocation argument when an action requires a determination to be made "in the interest of justice."[80] Justice, the D.C. Circuit reasoned, does not lie exclusively within the expertise of an agency.[81]

The second factor, of whether coercive force was taken by the agency, will only weigh in favor of review when the agency action has a "direct influence" on the parties. For instance, in *Heckler*, the denial of the death row inmate's petition was an indirect influence because it was only "through allowing the drugs to be used that the prisoners themselves were influence by the agency action."[82] The denial of a rulemaking didn't directly influence anyone. Likewise, the D.C. circuit court has held that decisions that amount to a "rescissions of commitments" are reviewable due to the fact that it's a "direct influence" on the parties.[83]

The third factor in determining whether agency decisions are reviewable is when there is a focus for review. Denials of citizen petitions under § 553(c), for instance, have a focus for review in that the APA requires agencies to give a brief explanation for their refusals.[84] Likewise, when an agency's organic act requires the agency to examine its decision, there is a focus for review. Even when an agency is not compelled by its statute to examine a decision but does so, that decision becomes a focus for review in subsequent, analogous situations.

The fourth factor in determining whether agency decisions are reviewable is whether courts have traditionally been reluctant to intervene, particularly with regard to prosecutorial discretion and national security.[85] Courts stay in their realm here so as to not offend a basic structure of the Constitution that leaves enforcement actions of the law and national security

79. Eric Biber, *Two Sides of the Same Coin: Judicial Review of Administrative Agency Action and Inaction*, 26 VA. ENVTL. L.J. 461, 486 (2008).

80. *See* Dickson v. Sec'y of Def., 68 F.3d 1396, 1403 (D.C. Cir. 1995).

81. *Id.*

82. Dustin Plotnic, *Agency Settlement Reviewability*, 83 FORDHAM L.R. 1367, 1388 (2013).

83. Robbins v. Reagan, 780 F.2d 37, 47 (D.C. Cir. 1985).

84. 5 U.S.C. § 553(c).

85. *See, e.g.*, N.D. *ex rel.* Bd. of Univ. & Sch. Lands v. Yeutter, 914 F.2d 1031, 1038 (8th Cir. 1990) (Larson, J., concurring in part and dissenting in part) (identifying prosecutorial discretion and national security); Shearson v. Holder, 865 F. Supp. 2d 850, 866 (N.D. Ohio 2011) (relating prosecutorial discretion and national security).

within the executive branch of the government.[86] However, whether prosecutorial discretion is an action by an agency or a no-action is unclear.[87]

C. Voluntary Commitment's First Cousins: Settlement Negotiations and Consent Decrees

Voluntary commitments are comparable to both settlement negotiations and consent decrees because all are agency negotiations that result in legal obligations. There is an argument that perhaps settlement negotiations should be free from judicial review because it is inherently the province of the prosecuting office to exercise discretion normally vested in executive functions. After all, discretion allows agencies to decide what is best for their resource allocation. However, too much discretion could lead to arbitrary decision-making and abuses. Nevertheless, there is a circuit split on whether settlements are subject to judicial review.

The D.C. circuit court is the only court to hold that settlements are presumptively unreviewable as essentially prosecutorial discretion.[88] Other courts, including the Third and Ninth Circuits, have held otherwise.[89] For instance, in *U.S. v. Carpenter*, the court found that an agency no-action (settlement) was effectively an action subject to judicial review.[90] Likewise, in *Mahoney v. U.S. Consumer Prods. Safety Comm'n*, a third party was able to sue a BB gun manufacturer after a settlement was reached with the defendant for damages because the settlement was a final agency action.[91] However, there is no true consensus among the circuit courts.[92]

Voluntary commitments are also essentially a preliminary consent decree. A consent decree is "an agreement between the parties to end a lawsuit on mutually acceptable terms which the judge agrees to enforce as a

86. Shearson v. Holder, F.Supp. 2d, 850, 866 (N.D. Ohio 2011).

87. *See* Ctr. for Auto Safety v. Dole, 828 F.2d 799, 819 (D.C. Cir. 1987) (Bork, J., dissenting) (arguing that decisions to deny a petition to reopen enforcement investigations should be unreviewable because it was similar to prosecutorial discretion). *Contra* Alliance to Save Mattaponi v. U.S. Army Corps of Eng'rs, 515 F. Supp. 2d 1, 9 (D. D.C. 2007) (holding than agency decision not to review a permit issuance was reviewable because it was not similar to prosecutorial discretion enough to be a no-action decision).

88. Ass'n of Irritated Residents v. EPA, 494 F.3d 1027, 1031 (D.C. Cir. 2007).

89. *See* United States v. Carpenter, 526 F.3d 1237, 1241 (9th Cir. 2008); Portland Gen. Elec. Co. v. Bonneville Power Admin., 501 F.3d 1009, 1013, 1031–32 (9th Cir. 2007); Mahoney v. U.S. Consumer Prods. Safety Comm'n, 146 F. App'x 587, 590 (3d Cir. 2005).

90. *See* U.S. v. Carpenter, 526 F.35 1237 (9th Cir. 2008).

91. *See Mahoney*, 146 F. App'x at 590.

92. *See, e.g.*, Williams v. Vukovich, 720 F.2d 909, 920 (6th Cir. 1983) ("A consent decree is essentially a settlement judgment subject to continued judicial policing."); United States v. City of Miami, 664 F.2d 435, 441 (5th Cir. 1981) ("'[T]he [consent] judgment is not an *inter partes* contract . . . when [the court] has rendered a consent judgment it has made an adjudication.'" (quoting 1B JAMES WM. MOORE ET AL., MOORE'S FEDERAL PRACTICE, para. 0.409[5], at 1030 (2d ed. 1980))); *see also* 46 AM JUR. 2D. *Judgments* §§ 183, 200 (2006).

judgment."[93] The DOJ and FTC are subject to judicial review for consent decrees relating to competition.[94] For instance, in the DOJ's antitrust division, challenges that are settled before litigation result in a consent decree subject to public comment and judicial review under the Tunney Act.[95] However, the FCC's statutory framework does not provide for such judicial review under its public interest standard.[96] If "compliance with the Commission['s] orders is not optional,"[97] then these are essentially consent decrees. In order to remedy the abuses in the absence of judicial review, an alternative would be for Congress to reform the FCC and adopt a Tunney Act-like amendment to the FCC's enabling statute.

IV. JUDICIAL REVIEW AS THE REMEDY FOR THE FCC'S OVERREACH IN TRANSACTION REVIEW

The FCC may levy exorbitant fines and revoke their approval if parties to a transaction fail to live up to their voluntary commitments.[98] However, there is uncertainty about whether this is a two-way street. If the parties to a transaction feel that the FCC coerced them to make concessions, it is unclear whether the parties may seek judicial review of the transaction for arbitrary or capricious coercion. This uncertainty exists because it is unsettled where voluntary commitments fit within the APA. It is argued in this Note that the imposition of commitments is an agency action because voluntary commitments have all the attributes of a final agency action but without any of the procedural protections of the APA. In the alternative, Congress should act by passing a Tunney Act-like amendment for the imposition of voluntary commitments because they are essentially consent decrees. What is clear is that having no check on this type of agency

93. *See* Larry Kramer, *Consent Decrees and the Rights of Third Parties*, 87 MICH. L. REV. 321, 325 (1988). Professor Kramer notes there is no consensus view on the precise meaning of a consent decree.

94. *See* Michael J. Zimmer & Charles A. Sullivan, *Consent Decree Settlements by Administrative Agencies in Antitrust and Employment Discrimination: Optimizing Public and Private Interests*, 1976 DUKE L.J. 163, 177-224 (arguing all agencies should abide by principles and procedures similar to those established by the Tunney Act).

95. Donald J. Russell & Sherri L. Wolson, *Dual Antitrust Review of Telecommunications Mergers by the Department of Justice and the Federal Communications Commission*, 11 GEO. MASON L. REV. 143, 147 (2002).

96. *Id.*

97. Georg Szalai, *FCC Fines Comcast for Violation of NBCUniversal Deal Condition*, HOLLYWOOD REPORTER (June 28, 2012), http://www.hollywoodreporter.com/comcast-fcc-fine-broadband-nbcuniversal-13353.

98. *Id.*

decision-making jeopardizes the legitimacy and integrity of the APA and our constitutional structure.[99]

After reviewing the above examples of how voluntary commitments exemplify agency overreach, it is clear that some reforms must be taken to remedy the FCC's abuse in transaction review. One option is to advocate for the FCC itself to refrain from imposing merger conditions that are not closely related to specific concerns raised by the transaction, thereby exercising restraint. As seen above, the FCC superficially already operates under this assumption, but voluntary commitments are still being imposed that are irrelevant to the merits.[100] Therefore, this option most likely will not alleviate any concerns.[101]

A second option is to analyze voluntary commitments like agency actions that are subject to judicial review. Under the APA, the imposition of voluntary commitments acts like agency decision-making that has all the same rulemaking attributes because there is "law to apply" by virtue of the public interest standard and, once imposed, the parties have a legal obligation to comply with the order, which essentially makes the imposition a final agency action.[102] Further, should a dispute arise about whether this is an action or no action, the *Heckler* factors cut in favor of rebutting the presumption of unreviewability. Lastly, we should treat voluntary commitments akin to settlement negotiations and consent decrees that some circuit courts have found to be reviewable under the APA.

Finally, in the alternative, Congress must provide an avenue for judicial review of voluntary commitments. An idea of this nature was already proposed in 2011. At a hearing in front of the House Subcommittee on Communications and Technology, under the Committee on Energy and Commerce, a bill was considered that would require "any condition imposed be narrowly tailored to remedy a transaction-specific harm, coupled with the provision that the [FCC] may not consider a voluntary commitment offered by a transaction applicant unless the agency could adopt a rule to the same

---

99. This note acknowledges the difficulty of obtaining judicial review in practice. One is quite sure that after parties spend millions of dollars and thousands of hours trying to push a deal through the FCC only to get rejected, these parties all would cut their losses and never litigate. Practically speaking, judicial review of transactions may need to be automatically given post-FCC approval, but this could bog-down the process and parties would not want to litigate this either. Here represents a purely economic reality when it comes to procedural protections. Sometimes, parties would rather waive rights in the name of economic efficiency. However, the law must prevail.

100. *See* Applications of AT&T Inc. and Centennial Communications Corporation for Consent to Transfer Control of Licenses, Authorizations, and Spectrum Leasing Arrangements, FCC 09-97, WT Docket No. 08-246, Memorandum Opinion and Order, released November 5, 2009, at 55, para. 133 ("AT&T-Centennial Order") (The Commission will "impose conditions only to remedy harms that arise from the transaction (i.e., transaction-specific harms) . . . ."), https://apps.fcc.gov/edocs_public/attachmatch/FCC-09-97A1.pdf.

101. While a pro-business Trump Administration could sway the independent agency to adopt the President's will, there is no evidence to suggest the FCC will change course at this time.

102. 5 U.S.C. § 704.

effect."[103] However, efforts to get Congress involved on a comprehensive FCC reform bill have remained at a standstill.[104] An argument can be made that these voluntary commitments act like consent decrees and that any reform should reflect the Tunney Act's granting of judicial review of consent decrees pursuant to the DOJ and FTC's competition review authority. Calling on Congress to act in reforming the FCC's transaction review in light of analogous legislation is an entirely appropriate and feasible alternative. In the end, either the agency or Congress needs to curb these abuses by making voluntary commitments subject to judicial review.

A. Obtaining Judicial Review by Virtue of the APA

Article III courts should be able to review the FCC's overreach because voluntary commitments are final agency actions not presumptively unreviewable under the APA, and are akin to settlement negotiations that some circuit courts find to be reviewable under the APA. Whether these voluntary commitments often positively affect the public interest should be irrelevant. Agencies have limited delegations of power and Congress enacted the APA to keep agencies in check. There is no reason to believe that the FCC should be exempted from such statutorily prescribed procedures to enact policy. When agencies violate the APA, they are subject to the review of Article III courts in order to preserve separation of powers and to keep legislative efforts the province of Congress.[105] Therefore, the FCC's imposition of voluntary commitments must be afforded the same remedy as agency law dictates today and be subjected to judicial review by Article III courts.

In order for voluntary commitments to be appropriate for judicial review, they must be reviewable final agency actions where there is "law to apply." Further, voluntary commitments should be treated as settlement negotiations that both the Third and Ninth circuit courts find to be reviewable.

1. Article III Courts are Necessary and Appropriate to Adjudicate Claims of the FCC's Overreach in Transaction Review

Article III courts are well-suited to adjudicate claims of the FCC's overreach in imposing voluntary conditions that fall outside the merits of the

---

103. TESTIMONY OF RANDOLPH J. MAY, HEARING ON "REFORMING FCC PROCESS" BEFORE THE SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY, COMMITTEE ON ENERGY AND COMMERCE, U.S. HOUSE OF REPRESENTATIVES 4 (June, 22, 2011), http://www.freestatefoundation.org/images/Testimony_of_Randolph_J._May_-_Hearing_on_FCC_Reform_-_June_22,_2011.pdf [https://perma.cc/QWE5-SQV3].

104. Randolph J. May, Seth L. Cooper, *The FCC Threatens the Rule of Law: A Focus on Agency Enforcement and Merger Review Abuses*, 17 FEDERALIST SOC'Y REV. 54, 59 (2016).

105. 5 U.S.C. § 702.

transaction. It is clear that Congress, in passing the APA, wanted the judiciary to be able to resolve agency abuses of power.[106] While certain classes of decisions enjoy a level of discretion, this is an area that evades the bounds of constitutionally delegated power to the agency.

One answer is that voluntary commitments are plainly outside of the APA, and are enforced purely under the agency's public interest standard of review in transactions. If that is the accepted view, does that mean that these actions cannot be challenged? Why should the FCC be able to enforce these conditions, but the parties cannot reciprocate suit if the imposition of the commitments was arbitrary and capricious? This notion cannot be correct as voluntary commitments have all the attributes of a final agency action but without any of the procedural protections of the APA. Pointing to a different authority to invoke policy cannot be the end of the matter because that lessens our ability to hold our agencies accountable for arbitrary and capricious regulations -- the principal reason for APA's enactment. Therefore, these actions must be reviewed under the APA and courts must be involved in this process because they have unique expertise in adjudicating administrative agency law claims.

2. Voluntary Commitments Are Not Presumptively Unreviewable under 5 U.S.C. § 701(a)(2) Because It Weighs in Favor of the Heckler's Factors

Judicial review under the APA requires a final agency action that is reviewable.[107] The easy hurdle to get over is whether transactions ending in voluntary commitments are final agency actions. It's clear that the FCC's acceptance or refusal of a transaction is a final agency action. As articulated in *Overton Park*, for an agency action to be reviewable, there must be "law to apply."[108] Here, there is law to apply, namely, the FCC's public interest standard.[109] While the courts have acknowledged it as a "supple instrument," others have found that there is a manageable and working framework to guide the agency in carrying out its transaction review authority.[110] Therefore, under an *Overton Park* analysis, there is law to apply to survive and rebut the "committed to agency discretion by law" standard.

Transactions ending in voluntary commitments should not be considered presumptively unreviewable under § 701(a)(2) because they survive the *Heckler* factors in a totality of the circumstances review. In the first consideration of complicated balancing, agency efficiency and expertise in handling transaction review comes at the expense of government

106. *See* 5 U.S.C. § 701.
107. *See* 5 U.S.C. § 704.
108. *See Overton Park*, 401 U.S. at 413–14.
109. *See* 47 U.S.C. § 151 et seq.
110. F.C.C v. WNCN Listeners Guild, 450 U.S. 582, 593, 101 S. Ct. 1266, 1274, 67 L. Ed. 2d 521 (1981); s*ee* J.W. Hampton Jr., & Co. v. United States, 276 U.S. 394, 409 (1928).

exceeding its statutory authority. It is easy to concede that normally, courts side with the agency on this balancing factor, as this is a specialized arena for agencies to review potential harms and improve public benefits through transaction review.[111] However, that is not the end of the analysis. The three remaining *Heckler* factors weigh in favor of judicial review.

Under the second *Heckler* factor, these voluntary commitments are coercive. Refusing to accept the conditions effectively renders a denial of a merger. As stated by then-Commissioner Furchtgott-Roth, these voluntary commitments are a legally troublesome. [112] Under the third *Heckler* consideration transactions ending in voluntary commitments weighs in favor of judicial intervention because the courts know that the focus for the review of the conditions should be based on the merits to the transactions, as it relates to the "public interest, convenience, or necessity."[113] Courts could use the FCC's own statement of policy, such as promoting competition, localism, and diversity, as its focus for reviewing transaction conditions that are not sufficiently tied to the merits and do not further the FCC's stated objectives.[114] As the above five transaction examples show, there is a clear departure from imposing conditions solely on the merits. Lastly, under *Heckler's* fourth consideration of prosecutorial discretion, no prosecution is taking place. Discretion is not removed from using the material facts of the transaction to remedy a problem it should address through APA procedures. Therefore, the imposition of the FCC's voluntary commitments should be considered final agency actions that survive the presumption of unreviewability by the courts.

3. Voluntary Commitments are Settlement Negotiations Reviewable by Article III Courts

Voluntary commitments could be treated as settlement negotiations that some circuit courts find to be reviewable under the APA. Settlements are different than no-action decisions because no-action decisions are decisions whether to *initiate* actions, whereas settlements are decisions to conclude them.[115] Even though settlement negotiations may be more akin to prosecutorial discretion than final agency actions, the end result of a

111. *See* Heckler v. Chaney, 470 U.S. 821 (1985).

112. *See Novel Procedures in FCC License Transfer Proceedings: Hearing Before the Subcomm. on Commercial and Administrative Law Oversight of the H. Comm. on the Judiciary*, 106th Cong. (1999) (statement of Harold W. Furchtgott-Roth, FCC Commissioner), https://transition.fcc.gov/Speeches/Furchtgott_Roth/Statements/sthfr922.html [https://perma.cc/LU5H-QNKG].

113. 47 U.S.C. § 252.

114. *Frequently Asked Questions*, FCC, https://www.fcc.gov/reports-research/guides/mergers-frequently-asked-questions (last visited Apr. 17, 2017) [https://perma.cc/F4HZ-BQ73].

115. Dustin Plotnick. *Agency Settlement Reviewability*. 82 FORDHAM L. R. 1367, 1396-98 (2013); *see also* N.Y. State Dept. v. FCC, 984 F.2d 1209 (D.C. Cir. 1993).

settlement negotiation places legal obligations on the parties.[116] Therefore, there is little distinction between voluntary commitments and settlements. In fact, settlements probably represent more choice for companies to escape lengthy and expensive litigation. Voluntary commitments, on the other hand, are so coercive because if parties disagree with the conditions, their merger or transaction fails.[117] In settlement negotiations, the parties can dispute the term of a settlement themselves or fight their claims on the merits in court. However, for voluntary commitments, the commitments that parties would challenge are the ones that are unrelated to the merits of the transaction. Both the Third and Ninth circuit courts agree that settlements are final agency actions subject to judicial review, while the influential D.C. Circuit has placed this notion in utmost uncertainty by finding continuously for supreme agency discretion.[118] Nevertheless, we should treat voluntary commitments no different because the end result is the same.

B. Obtaining Judicial Review through Congress: The Tunney Act as a Blueprint

In the alternative, if voluntary commitments are not final agency actions subject to APA procedures, are presumptively unreviewable under § 701(a)(2), or the D.C. Circuit's line of reasoning prevails, voluntary commitments nonetheless must be able to obtain judicial review because they are analogous to consent decrees. Congress has afforded special protections for the review of consent decrees with respect to antitrust concerns in enacting the Tunney Act.[119] If the FCC's public interest standard truly focuses on competition, and the Tunney Act is implemented to check the amount of power antitrust authorities had in imposing consent decrees relating to competition, then there is no reason to think that a Tunney Act-like amendment to the Communications Act of 1934 would be so incredulous. Perhaps the previously failed effort by Congress to enact legislation to bring voluntary commitments to a screeching halt has left advocates skeptical of Congressional action. However, using the Tunney

116. *See* United States v. Carpenter, 526 F.3d 1237, 1241 (9th Cir. 2008); Portland Gen. Elec. Co. v. Bonneville Power Admin., 501 F.3d 1009, 1013, 1031–32 (9th Cir. 2007); Mahoney v. U.S. Consumer Prods. Safety Comm'n, 146 F. App'x 587, 590 (3d Cir. 2005).

117. Christopher Yoo, *Merger Review by the Federal Communications Commission: Comcast–NBC Universal*, 45 REV. IND. ORGAN. 295, 312 (2014) (noting that since 2004, "conditions have become increasingly common features of [FCC] merger clearances); s*ee also* Derek E. Bambauer, *Against Jawboning*, 100 MINN. L. REV. 51, 126 (2015) ("Jawboning of Internet intermediaries is increasingly common, and it operates beneath the notice of both courts and commentators."); T. Randolph Beard et al., *Eroding the Rule of Law: Regulation as Cooperative Bargaining at the FCC* 5 (Phoenix Center, Policy Paper No. 49, 2015), http://www.phoenix-center .org/pcpp/PCPP49Final.pdf.

118. *See* United States v. Carpenter, 526 F.3d 1237, 1241 (9th Cir. 2008); Portland Gen. Elec. Co. v. Bonneville Power Admin., 501 F.3d 1009, 1013, 1031–32 (9th Cir. 2007); Mahoney v. U.S. Consumer Prods. Safety Comm'n, 146 F. App'x 587, 590 (3d Cir. 2005).

119. Antitrust Procedures and Penalties Act (Tunney Act) Pub.L. 93–528, 88 Stat. 1708, enacted December 21, 1974, 15 U.S.C. § 16.

Act as a foundational blueprint could more effectively allow Congress to pass legislation subjecting voluntary commitments to the review of the courts. Therefore, the legislature must turn their focus to the FCC's transaction review authority in order to afford judicial review to parties contesting to voluntary commitments.[120]

Voluntary commitments and consent decrees are similar enough to warrant a Tunney Act-like proposal. When the FCC approves a transaction, it essentially leaves the door open for agency enforcement after the fact. This is a hallmark attribute of a consent decree, but goes one step further. It creates the same benefit for the agency as a consent decree but without the formality of a judicial seal. The approval is final for all intents and purposes as there is no other procedure or involvement by the agency, except to the extent that it acts as an enforcer. As noted above, the FCC may enforce the commitments by either revoking the deal or levying a fine. However, whether the obligating parties may sue for arbitrary and capricious commitments that are wholly irrelevant to the merits of the transaction remains in doubt. In order to provide clarity and consistency to transaction review among the various antitrust authorities, a Tunney Act-like solution may be our last line of defense to our constitutional structure.

V. CONCLUSION

In sum, the FCC crafts policy under the APA and its transaction (merger) review authority. The FCC has abused its power by formulating policy through the imposition of voluntary commitments unrelated or ancillary to the merits of the transaction at hand. This de facto rulemaking wholly offends the APA and our constitutional structure. In order to curb this overreach by the FCC, judicial review is a necessary and appropriate solution to the problem. Voluntary commitments are final agency actions that must be reviewable by Article III courts. In the alternative, a comparison of voluntary commitments to settlement negotiations and consent decrees pragmatically defends obtaining judicial review outside of the APA. Our constitutional structure depends on the power of the judiciary and the bravery of Congress to act now.

120. *See* Michael J. Zimmer & Charles A. Sullivan, *Consent Decree Settlements by Administrative Agencies in Antitrust and Employment Discrimination: Optimizing Public and Private Interests*, 1976 DUKE L.J. 163, 177-224 (arguing that all agencies should abide by principles and procedures similar to those established by the Tunney Act).

Double Trouble: Why Two Internet Privacy Enforcement Agencies Are Not Better Than One for Businesses or Consumers

Alison M. Cheperdak *

TABLE OF CONTENTS

* J.D. Candidate, The George Washington University Law School, May 2018. Senior Notes Editor, *Federal Communications Law Journal*, Vols. 69–70. B.A., Communications, Villanova University. I thank the entire staff of the Federal Communications Law Journal for their assistance in this Note's production. I am deeply grateful to GW Law Journal Adjunct Professor Jodie Griffin and Reference Librarian Lori Fossum for their instrumental guidance. Thank you also to Brooke Ericson, Nathan Halford, and Howard Waltzman for their invaluable insights, and the many Senate and House staff who provided helpful comments. I dedicate this Note to my husband, Jason, and parents, Tom and Paula, for their unending support.

I. INTRODUCTION

In 1890, a formative *Harvard Law Review* article developed "the basic principle of American privacy law" that privacy is the "right to be let alone."[1] Samuel D. Warren and Louis D. Brandeis' *The Right to Privacy* was published "in response to invasions of personal privacy caused by the technological [advances] of newspapers and photographs".[2] Much has changed since Warren and Brandeis' article influenced American privacy common law jurisprudence.[3] In the digital era, the right to privacy may be more appropriately characterized as "knowing what data is being collected and what is happening to it, having choices about how it is collected and used, and being confident that it is secure."[4] Given the ubiquitous nature of collection, retention, and dissemination of data in the digital age, appropriate privacy regulations are required.[5]

The Internet is critical to virtually all aspects of life throughout the U.S., especially economically and socially.[6] For instance, through the use of networked technologies, people are able to express themselves in infinite ways, establish "social connections, transact business, and organize politically."[7] "An abundance of data, inexpensive processing power, and increasingly sophisticated analytical techniques drive innovation in our increasingly networked society."[8] The U.S. government has two strong interests in establishing and enforcing appropriate privacy policies;[9] privacy is important to Americans and they expect their privacy to be protected from intrusion by the government or private entities,[10] and strong privacy

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 5 (1890).

2. *Id.* at 195-96.

3. *See* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), https://perma.cc/78VD-Z7MJ [hereinafter WHITE HOUSE PRIVACY FRAMEWORK] (statement of President Barack Obama). "Never has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones. In just the last decade, the Internet has enabled a renewal of direct political engagement by citizens around the globe and an explosion of commerce and innovation creating jobs of the future."

4. *The State of Online Consumer Privacy: Hearing Before S.Comm. on Commerce, Science, and Transportation*, 112th Cong. 4, pg. 32 (2011) (statement of Erich Andersen, Deputy Gen. Counsel, Microsoft Corp.).

5. *See generally* WHITE HOUSE PRIVACY FRAMEWORK at 5.

6. *Id.* at 5.

7. *Id.* at 5.

8. *Id.* at 5.

9. *Id.*

10. *See generally The State of Privacy in Post-Snowden America*, PEW RES. CTR. (Sept. 21, 2016), https://perma.cc/R5HR-Q6KC (86% of Internet users have taken steps online to remove or mask their "digital footprints," and many would like to take additional steps to protect their online privacy and are unaware of how to do so. 74% of Americans surveyed said it is "very important" to them that they be in control of *who* can get information about them, and 65% said it is "very important" to them to control *what* information is collected about them.); WHITE HOUSE PRIVACY FRAMEWORK at 4-5.

protections are essential to sustaining the trust necessary for Internet commerce, which consequentially fosters innovation and economic growth.[11]

Consumers should not have to be a lawyer or a network engineer to understand whether the information they provide via the Internet will or will not be protected.[12] However, the current rules and regulations governing Internet data security are just that—needlessly complex and confusing.[13] The current Internet data security legal landscape is complicated primarily because "there is no comprehensive federal privacy statute that protects personal information."[14] Instead, federal privacy rules are disjointed; both the FTC and the FCC have authority to regulate different parts of the Internet, and states also have authority to enact and enforce their own privacy laws despite the inherently interstate elements of online transactions.[15]

Significantly, the FTC and the FCC's frameworks differ in that the FTC's priority is security, whereas the FCC's priority is privacy.[16] The FTC appropriately focuses more on security, including personally identifiable information (PII), whereas the FCC focuses more on privacy, [17] which is considerably more subjective and personal versus security which is primarily about safety.

This Note explores the ways in which the FCC's Broadband Privacy Order is harmful to both businesses and consumers, and the ways in which the regulations that apply to Edge Service Providers (ESPs) and Internet Service Providers (ISPs) can be legally harmonized. The Note begins with a discussion of the harms the uneven privacy models of the FCC and the FTC impose on customers and businesses, including confusion and increased transactional costs. Next, the Note discusses how the FCC failed to adequately explain why it chose not to follow the FTC's preexisting and successful approach to data security, including an analysis of the numerous ways in which the FCC needlessly diverged from the FTC's reasonable model. While the FTC is the ideal enforcer of Internet data security because of its long

---

11. WHITE HOUSE PRIVACY FRAMEWORK at 4-5.

12. *See* Dissenting Statement of Ajit Pai, Comm'r, FCC, at 1, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 16-106 (Nov. 2, 2016), https://perma.cc/6MSN-7GMN [hereinafter Pai Dissenting Statement].

13. *See generally*, Dissenting Statement of Michael O'Rielly, Comm'r, FCC, at 5, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 16-106 (Nov. 2, 2016), https://perma.cc/Q3GE-UL8K [hereinafter O'Rielly Dissenting Statement].

14. *See* GINA STEVENS, CONG. RESEARCH SERV., PRIVACY PROTECTIONS FOR PERSONAL INFORMATION ONLINE 5, 7 (2011), https://perma.cc/E866-HJ3R; *see also* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY forward, (2012) ("White House Privacy Framework") ("neither consumers nor companies have a clear set of ground rules in the commercial arena. As a result, it is difficult today for consumers to assess whether a company's privacy practices warrant their trust.").

15. *See generally*, The Federal Trade Commission Act 15 U.S.C. § 45(a) ("FTC Act"); Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Report and Order*, 16-101 FCC Rcd 16-148, para. at 1 (2016), https://perma.cc/F7EW-PCKN [hereinafter *Privacy Order*]; *see generally*, *State Laws Related to Internet* Privacy, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 5, 2016), https://perma.cc/X53G-JADT/.

16. *See generally*, *Privacy Order*; FTC REPORT.

17. *See* FTC REPORT at 18; *Privacy Order* at para. 1, 92, 134.

history of providing consumer protection and online data security, the FTC must provide a clearer description of what BIAS and ESPs must do to adequately protect consumers' privacy and security. Finally, the Note will explain the ways in which ESP and ISP privacy regulations can be legally harmonized after the Privacy Order's recent repeal.

II. BACKGROUND

A. Components of the Internet

The Internet is comprised of four major actors: "end users, broadband providers [(also known as ISPs)], backbone networks, and edge [service] providers [(ESPs)]."[18] Many customers, also known as end users, access the Internet "using an ISP, which delivers high-speed Internet access using technologies, such as cable modem service, digital subscriber line (DSL) service, and fiber optics."[19] ISPs "interconnect with backbone networks," which are the "long-haul fiber-optic links and high-speed routers" that transmit "vast amounts of data."[20] ESPs are content, "application, service, and device" providers, and their name comes from the position that they operate "at the edge of the network rather than the core of the network."[21] Examples of ESPs include Netflix, Google, and Amazon.[22] Under the current privacy legal landscape, the FTC has authority over ESPs, and the FCC has authority over ISPs.[23]

B. FTC's Strong History of Internet Privacy Regulation

The FTC derives its authority for enforcement actions against ESPs under The Federal Trade Commission Act 15 U.S.C. § 45(a) (FTC Act), which prohibits "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[24] The FTC Act does not provide industry-specific duties, but instead applies a technology-neutral approach.[25] However, while the FTC Act does not provide specific duties for ESPs (or any other type of company that falls under its jurisdiction), the FTC's 2012 report, *Protecting Consumer Privacy in an Era*

18. U.S. Telecom Association v. FCC 825 F.3d 674, 690 (D.C. 2016), https://perma.cc/KQ4C-JATN [hereinafter U.S. Telecom Association.

19. *See,* Protecting and Promoting the Open Internet, *Report and Order on Remand, Declaratory Ruling, and* Order, 14-28 FCC Rcd 15-24, at para 5 (2015), https://perma.cc/4TLY-74MB [hereinafter *2015 Open Internet Order*].

20. *See* U.S. Telecom Association.

21. *See* Preserving the Open Internet Broadband Industry Practices, *Report and Order*, 07-52 FCC Rcd 10-201, para. 4, 20, n.2 (2010), https://perma.cc/K4PX-3VGQ (2010) [hereinafter *2010 Open Internet Order*].

22. *See* U.S. Telecom Association.

23. *See generally* http://adage.com/article/privacy-and-regulation/ftc-regain-isp-privacy-oversight-easy/308487/.

24. *See* 15 U.S.C. § 45(a) (2012).

25. *Id.*

of Rapid Change (FTC Report), provides more specific recommendations for Internet businesses and policymakers.[26] The FTC Report set forth a final privacy framework after taking into consideration more than 450 public comments from stakeholders.[27] Although the FTC Report by its nature does not consist of binding rules, it urges companies to implement "best practices" to protect consumers' private information immediately, such as "making privacy the 'default setting' for commercial data practices" and increasing "consumers' control over the collection and use of their personal" information.[28] The FTC Report also stipulates that "companies should view the comprehensive privacy programs mandated by consent orders as a roadmap as they implement privacy by design in their own organizations."[29] Perhaps most importantly, the FTC's "proposed framework is not a one size fits all model for consumer choice mechanisms."[30] Instead, the FTC urges companies to offer "clear and concise choice mechanisms that are [both] easy to use and delivered at a time and context that is relevant to the consumer's decision about whether to allow data collection or use."[31]

The FTC, which regulates ESPs, "has brought numerous legal actions against organizations that have violated consumers' privacy rights, or misled [consumers] by failing to maintain security for [their] sensitive information."[32] In most of these cases, "the FTC has charged the defendant with violating Section 5 of the FTC Act," which prohibits "unfair and deceptive acts and practices in or affecting commerce."[33] For example, the FTC "brought enforcement actions against mobile applications that violated

26. *See generally*, FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESS AND POLICYMAKERS (2012) [hereinafter FTC REPORT], https://perma.cc/L53D-5QJY; In keeping with the White House Privacy Framework terminology, throughout this Note, "'company' means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture established to make a profit, or nonprofit entity, that collects, uses, discloses, stores, or transfers personal data in interstate commerce, to the extent such organizations are not subject to existing Federal data privacy laws." WHITE HOUSE PRIVACY FRAMEWORK at 5.

27. FTC REPORT at i.

28. *Id.*

29. *Id.* at 31.

30. *Id.* at 49;13 (FTC calls on Congress to enact "baseline privacy legislation that is technologically neutral and sufficiently flexible to allow companies to continue to innovate").

31. *Id.* at 49-50.

32. *Protecting Consumer Privacy: Enforcing Privacy Promises*, FTC, https://perma.cc/4UQE-JKY4 (last accessed Apr. 11, 2017).

33. *Id.*

the Children's Online Privacy Protection Act,[34] as well as against entities that sold consumer lists to marketers in violation of the Fair Credit Reporting Act" (FCRA).[35] During the first 40 years of the FTC's enforcement of the FCRA, "the FTC brought 87 enforcement actions against [consumer reporting agencies] (CRAs)."[36]

C. The FCC's New Role in Internet Privacy Regulation

The Privacy Order establishing the FCC's privacy enforcement power was passed in 2016 during the final year of the Obama Administration.[37] However, on April 3, 2017, President Donald J. Trump signed a joint resolution that repealed the FCC's Privacy Order.[38] The passage of S.J. Res. 34 came less than a month after the Republican majority FCC voted 2-1 to issue a temporary stay on the data security obligations of the Privacy Order, which were to take effect March 2, 2017.[39] This action indicates that the new Republican leadership at the FCC disfavored the prior Democratic-leaning Commission's previous plans.[40]

The Privacy Order is problematic because without a uniform technology-neutral standard for all, or at the very least, most Internet activity, under the current rules and regulations it is incumbent upon an Internet user to understand (1) the specific type of Internet businesses she uses; (2) the corresponding legal obligations of those businesses; and (3) how to opt-in or

---

34. *See* https://www.ftc.gov/news-events/press-releases/2015/12/two-app-developers-settle-ftc-charges-they-violated-childrens; Mobile game company TinyCo Inc. and online review site Yelp settled separate Department of Justice charges that they improperly collected information from children via their mobile applications. According to the FTC's complaint against TinyCo, the app which had been downloaded more than 34 million times, was targeted at children and some of the company's apps included an optional feature that collected email addresses from all users, including those younger than 13. In its complaint against Yelp, the FTC alleged that Yelp Inc. collected personal information from children without first notifying parents and obtaining their consent. *United States v. Yelp Inc.*, 3:14-cv-04163, *proposed stipulated order filed* (N.D. Cal. Sept. 16, 2014); *United States v. TinyCo Inc.*, No. 3:14-cv-04164, *proposed stipulated order filed* (N.D. Cal. Sept. 16, 2014); Fair Credit Reporting Act (FCRA) violations by FTC-regulated entities are considered unfair and deceptive practices and are subject to the remedies provided by Section 5 of the FTC Act. Section 621(a); *see also* 15 U.S.C. §§ 41 *et seq*. The FTC also has authority to file civil actions in federal court to recover civil penalties of up to $3,500 per violation for a "knowing violation, which constitutes a pattern or practice of violations." FTC, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATION 4 (2011).

35. https://www.ftc.gov/news-events/press-releases/2016/05/debt-collector-settles-ftc-charges-it-violated-fair-credit.

36. FTC, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATION 4 (2011).

37. *See generally Privacy Order*; *see also* https://www.reuters.com/article/us-usa-internet-trump/trump-signs-repeal-of-u-s-broadband-privacy-rules-idUSKBN1752PR.

38. https://www.reuters.com/article/us-usa-internet-trump/trump-signs-repeal-of-u-s-broadband-privacy-rules-idUSKBN1752PR; FN 38 on annotated sources.

39. *See generally* S.J. Res. 34.

40. *See generally O'Reilly dissenting See generally, id.*; Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Order Granting Stay Petition in Part*, 16-106 FCC 17-19 (2017).

opt-out of the collection, retention, and dissemination of her personal information based on relevant legal authorities.[41] The steps required to understand Internet data security laws are too complicated for the average person.[42] The Internet data security framework should, therefore, be amended so the average, non-attorney Internet user can understand the laws that apply.[43]

Although consumer protection is chief among the goals of privacy regulations, the lack of uniform laws in this area is far too confusing for the average customers to possibly understand how the regulations may be helpful to them.[44] Under the Privacy Order, for a consumer to understand the privacy laws that apply to her Internet activity, she must understand both the distinction between ISPs and ESPs, as well as the differences between the FCC and the FTC's privacy policies, and how those policies apply to her personal browsing activity.[45] The following scenario demonstrates the inherent complexity of relatively basic Internet use. A customer purchases an Internet service plan from Verizon FIOS (an ISP) to access the Internet. This transaction would be governed by the FCC because the FCC has jurisdiction over ISPs. While browsing the Internet, the user reads several articles on *The New York Times* website and watches a program on Netflix. These activities would be governed by the FTC because the FTC has jurisdiction over ESPs.[46] Here, both *The New York Times* and Netflix's websites are ESPs because they provide content and services in the form of news and entertainment online.[47]

Buttressing the inherent complexity of having "two cops" on the Internet privacy "beat", an ESP's liability may be different according to the way a customer uses the service.[48] For example, Google is an ESP that can be accessed via an ISP, but the company has begun connecting directly to broadband providers' networks, thus eliminating the need to interconnect with

41. O'Rielly Dissenting Statement at 5; Pai Dissenting Statement at 1 (For the last two decades, the Federal Trade Commission applied the same privacy framework to all internet businesses, so consumers had a reasonable uniform expectation of privacy. "[C]onsumers should not need to be network engineers to understand who is collecting their data and they should not have to be lawyers to determine if their information is protected.").

42. *See generally* Smith, What Internet Users Know about tech and web.

43. *See* Pai Dissenting Statement at 1.

44. *See generally* Pai Dissenting.

45. *Id.* Internet activity using an ISP, also known as a broadband internet access service (BIAS) is governed by the FCC pursuant to the *Privacy Order* para. 1. ESPs are exempt from FCC regulation and are instead regulated by the FTC pursuant to its broad consumer protection authority found in Section 5 of the FTC Act.

46. Id. *See* also 15 U.S.C. § 45(a) (2012).

47. *See* U.S. Telecom Association.

48. *See* Maureen K. Ohlhausen, Commissioner, FTC, Address at the 33rd Annual Institute on Telecommunications Policy & Regulation 4 (Dec. 4, 2015) [hereinafter Ohlhausen address] ("Consumers will be worse off if overlapping efforts unnecessarily divert resources from more pressing issues. When two cops are on one beat, another beat may be left vulnerable. Additionally, if enforces fail to leverage their comparative advantages, consumers will be worse off.").

a backbone network, as is typical in transactions involving ISPs and ESPs.[49] Moreover, some ISPs, "such as Comcast and AT&T[] have begun developing their own backbone networks."[50] The blurred lines between ISPs, ESPs, and backbone networks illustrate the technical differences that determine which parts of the Internet are governed by the FCC versus the FTC.[51]

D. The Major Impacts of Differing Consumer Consent Models and Privacy Definitions

The most significant difference between the FTC and the FCC's approaches to data security concerns when a company must obtain "opt-in" versus "opt-out" permission from individual consumers before using contextual information for advertising and related purposes.[52] The FCC and the FTC both use "sensitivity-based customer choice frameworks", but the agencies make judgements using different definitions of sensitive data.[53]

The FCC defines sensitive customer proprietary information ("PI") as "financial information, health information, Social Security numbers, precise geo-location information, information pertaining to children, content of communications, web browsing history, application usage history, and the functional equivalents of web browsing history or application usage history."[54] The Privacy Order also requires ISPs to provide customers with a "mechanism to adjust their choice options."[55]

Contrarily, the FTC's definition of sensitive customer data is narrower. It includes "Social Security numbers [,] financial, health, children's and geographical information", but does *not* include content of communications, web browsing activity or application usage history, as delineated in the FCC's Privacy Order.[56] The Privacy Order also applies to more than merely sensitive data; the scope of information covered by the FCC's rules includes "Customer Proprietary Network Information (CPNI), [customer proprietary information

49. Jon Brodkin, *Google Fiber Makes Expansion Plans for $60 Wireless Gigabit Service, Ars Technica* (Feb. 22, 2017, 11:44 AM), https://arstechnica.com/information-technology/2017/02/google-fiber-makes-expansion-plans-for-60-wireless-gigabit-service/; 15 U.S.C. § 45(a) (2012); *2010 Open Internet Order* at n.2; U.S. Telecom Association.

50. *See generally* U.S. Telecom Association.

51. *Id.*

52. *See Privacy Order* at para. 9 (carriers must obtain opt-in approval for use and sharing of sensitive PI). In contrast, the FTC generally requires opt-in approval for use and sharing of sensitive personal information. The FTC staff made this point in its comment to the *Privacy Order* NPRM. The FTC Staff recommended that the FCC require opt-in consent for the use and sharing of sensitive data and opt-out consent for the use and sharing of non-sensitive data. Bureau of Consumer Protection of the FTC Comment, https://perma.cc/YND2-X6WR; FTC Report at vii-viii; FTC REPORT at 15; Bureau of Consumer Protection of the FTC Comment, https://perma.cc/YND2-X6WR.

53. *Id.*

54. *See Privacy Order* at para. 9; FTC Report at vii-viii, 15.

55. *See* Privacy *Order* at para. 167.

56. *See* FTC REPORT at 15.

(PI)], personally identifiable information (PII), and content of communications."[57]

The FTC and the FCC also differ on consumer consent policies. The FCC's Privacy Order adopts three categories of approval with respect to the use of customer PI obtained by ISPs, including: (1) opt-in approval; (2) opt-out approval; and (3) congressionally-recognized exceptions to customer approval requirements.[58] The Privacy Order also adopts "heightened disclosure and affirmative consent requirements for BIAS that offer its consumers financial incentives, [such as sales and promotions], in exchange for the right to use the customers' confidential information."[59]

Instead of establishing *per se* categories, the FTC's "framework sets forth best practices" designed to "work in tandem with existing privacy and security statutes."[60] The FTC's approach is more flexible.[61] For instance, the FTC does not require "entities that collect limited amounts of non-sensitive data from under 5,000 [customers] to comply with the framework, as long as they do not share the data with third parties."[62] This policy is designed to prevent regulating smaller entities out of business, like a "cash-only-curb-side food truck business that offers to send messages announcing [deals]."[63] The FTC's flexible standard also recognizes that "some business practices create fewer potential risks to consumer information" than others. The FTC believes that for some business transactions, "the benefits of providing choice are reduced—either because consent can be inferred or because public policy makes choice unnecessary."[64]

The FTC's "opt-out" approach recommends in most instances that ESPs allow consumers to "opt-out" of their data being used for advertising and related purposes, unless the use is consistent with the consumer's relationship with the business and thus does not necessitate consumer choice.[65] The FTC believes that "whether a practice requires" consumer consent depends "on the extent to which the practice is consistent with the context of the transaction or [user's] existing relationship with the business, or is required or specifically authorized by law."[66] Therefore, companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the particular transaction, or the parties' relationships, or required or authorized by law.[67] The FTC also continues to believe that there are "five categories of data practices that

57. *See Privacy Order* at para. 6.
58. *See Privacy Order* at para. 9.
59. *Id.* at para. 12.
60. FTC REPORT at 16.
61. FTC REPORT at 16-17.
62. *Id.* at 16.
63. *Id.*.
64. *Id.* at 38.
65. *Id.* at 39-40.
66. *Id.* at 38-39; *see also*, WHITE HOUSE PRIVACY FRAMEWORK at 1 (Obama Administration's Privacy Bill of Rights requirements include: "Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.").
67. FTC REPORT at 48.

companies can engage in without offering consumer choice," because the "data collection and use" in the particular contexts are "either obvious" or "sufficiently acceptable or necessary for public policy reasons."[68] The categories include: "(1) product and service fulfillment; (2) internal operations; (3) fraud prevention; (4) legal compliance and public purpose; and (5) first-party marketing."[69]

Both the FCC and the FTC require affirmative express consent from customers for the data collection and use of certain types of information in particular contexts, but the agencies have different standards.[70] The FCC requires ISPs to obtain opt-in consent to track a user's Internet browsing activity.[71] The FTC does not require consent for such activity.[72] However, the FTC does require affirmative express consent in the following circumstances: (1) ESPs should obtain consent before making material retroactive changes to privacy representations; and (2) ESPs should obtain consent before collecting sensitive data.[73] Here, it is legally significant that the FTC employs a narrower definition of "sensitive" compared to the FCC.[74]

The opt-out policy of the FTC means that an Internet user does not have an expectation of privacy with respect to her online activities as they relate to ESPs, unless she affirmatively opts-out of the collection, retention, and/or dissemination of her Internet browsing history.[75] However, regardless of an Internet user's opt-out or opt-in preference with the ESPs it interfaces with, a user does have an expectation of privacy concerning the information her ISP, the entity that provides online access to her home, collects on her Internet usage.[76] This is because ESPs like Google, YouTube, and Amazon are ESPs and are therefore governed by the FTC under the FTC Act; ISPs like Comcast, Charter Communications, and Verizon are instead governed by the FCC and consequentially have different legal obligations.[77]

Numerous broadband providers, their associations, and other stakeholders submitted comments to the Notice of Proposed Rulemaking for the Privacy Order arguing that because broadband providers are part of a larger online ecosystem that includes ESPs, they should be subject to the same

68. *Id.* at 36-39.

69. *Id.*at 36.

70. *Id.* at 47 ("affirmative express consent is appropriate when a company uses sensitive data for marketing to a first- or third-party." Due to heightened privacy risks associated with sensitive data, like health or children's information, first parties should provide a consumer choice mechanism at the time of data collection); *Privacy Order* at para. 9.

71. *Privacy Order* at para. 9. *Conf.* FTC REPORT at 15.

72. FTC REPORT at 15; Based on its expertise, the FTC staff submitted a comment to the *Privacy* NPRM, indicating its recommendation that the FCC require opt-in consent for the use and sharing of sensitive data and opt-out consent for the use and sharing of non-sensitive data. Bureau of Consumer Protection of the FTC Comment, https://perma.cc/YND2-X6WR.

73. *Id.* at 57.

74. *Privacy Order* at para. 9. *Conf.* FTC REPORT at 58.

75. FTC REPORT at 47.

76. ISPs are exempt from Section 5 of the FTC Act. Instead ISPs, which are common carriers, are governed by the Communications Act; *Fact Sheet: The FCC Adopts Order to Give Broadband Consumers Increased Choice Over Their Personal Information*, FCC 4, https://perma.cc/NNT6-G5LF (last accessed Apr. 11, 2017).

77. *Id.*

set of regulations as ESPs.[78] Responding to the commenters' concerns, the Privacy Order maintains that a ISPs should be subjected to stricter standards than ESPs because an ISP "sits at a privileged place in the network, the bottleneck between the customer and the rest of the Internet."[79] The Privacy Order maintains that because ISPs serve as "gatekeepers" to the Internet, whereas ESPs see only a slice of a user's online activity, ISPs should be subject to stricter online privacy standards.[80] The unequal obligations of Internet businesses due to a lack of uniform Internet data security standards are unfair to both ISPs and their consumers because the stricter standards under the Privacy Order increase transaction costs for ISPs, which will ultimately be absorbed by consumers.[81] Additionally, the Privacy Order does not adequately articulate the harm that it seeks to prevent by implementing its new privacy standards.[82]

E. The FCC and FTC Differ in Internet Privacy Enforcement Practices

The FCC and the FTC also have different enforcement philosophies concerning Internet data security.[83] Demonstrating how the FCC's approach to privacy and data security enforcement differs from the FTC's, soon after the Protecting and Promoting the Open Internet Report and Order reclassified

78. *See* generally, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Notice of Proposed* Rulemaking, 16-106 FCC Rcd 16-39 (2016) [hereinafter *Privacy NPRM*]; *Privacy Order* at para. 28.

79. *Privacy Order* at para. 28.

80. *Id.* at para. 36.

81. "The goal of consumer protection enforcement isn't to make headlines; it is to make harmed consumers whole and incentivize appropriate practices. The costs imposed by a regulator on a legitimate, non-fraudulent company are ultimately born by its consumers. If enforcement action imposes costs disproportionate to the actual consumer harm, that enforcement action may make consumers worse off if prices rise or innovation slows." Ohlhausen Address at 5.

82. *Privacy Order* at para 28 (FCC provides that in formulating its rules, the FCC considered the FTC REPORT and the WHITE HOUSE PRIVACY FRAMEWORK. However, the FCC declined to sufficiently explain why it found the "heightened protections" for sensitive customer information was necessary due to the "vast swathes of customer data" available to ISPs). Moreover, the *Privacy Order* expands the definition of "proprietary information" to include information beyond what a customer would "keep secret from any other party." The FCC dismisses multiple strong arguments as to why expanding the definition of proprietary information is appropriate without providing adequate justification. *Privacy Order* at para. 28.

83. Former Obama FTC Chairman Jon Leibowitz disagreed with the FCC's proposal to prohibit ISPs from offering discounted services in exchange for customers opting in to great data collection and use is not optical. In opposition to his fellow-Democrat appointees at the FCC, Leibowitz believed the rules' prohibition of something that consumers don't find problematic would stifle the development of free online services, and other low cost resources, due to increased transactional costs. John Eggerton, *Former FTC Chair Has Issues with FCC's Opt-in CPNI Regime*, MULTICHANNEL (May 11, 2016, 1:45 PM EST), https://perma.cc/PLF7-GTXG.

ISPs, the FCC resolved its first security case against a cable operator.[84] The matter concerned a breach "involving information about 61 of Cox Communication's more than 6 million subscribers."[85] During the case, "amateur hackers social-engineered Cox employees, there was no technical failure involved," and "no payment information accessed."[86] "[H]ackers posted some information about *eight* affected customers on social media," and "Cox detected" and thwarted the breach "within a matter of days."[87] Cox also cooperated with the Federal Bureau of Investigation (FBI) which arrested the hacker.[88] Even though "the FCC's Order and Consent Decree offers no evidence of any resulting identity theft" or other consumer harm, "the FCC settlement imposed a $595,000 fine" (which equals about "$10,000 per affected consumer") and "extensive compliance measures."[89]

In contrast to the FCC's apparent "strict liability" approach, as seen in the Cox matter, the FTC employs a "reasonable security" approach.[90] Since the beginning of the FTC's role in data security enforcement, the FTC "has recognized that there is no such thing as perfect security," and that security is a "continuing process of detecting risks" and adjusting accordingly.[91] Based on this perspective, the touchstone of the FTC's approach to data security has been and continues to be reasonableness—that "a company's data security measures must be reasonable in light of the volume and sensitivity of information the company holds, the size and complexity of the company's operations, the cost of the tools that are available to address vulnerabilities, and other factors."[92]

84. 47 U.S.C. § 222 (2012); *2015*; Cox Communications, *Order*, 0001834696 FCC Rcd 15-1241 (2015), https://perma.cc/Z8ZE-6GP9 [hereinafter *Cox Order*]*; see also* Thomas M. Lenard, *The FCC Flexes Its Privacy Muscles*, THE HILL (Nov. 18, 2015, 7:30 AM EST), https://perma.cc/KF98-YHBY.

85. Ohlhausen Address at 5; *Cox Consent Decree* at para. 9.

86. Ohlhausen Address at 5; *Cox Consent Decree* at para. 2; Thomas M. Lenard, *The FCC Flexes Its Privacy Muscles*, THE HILL (Nov. 18, 2015, 7:30 AM EST), https://perma.cc/KF98-YHBY.

87. Ohlhausen Address at 5; *Cox Consent Decree* at para. 9.

88. Ohlhausen Address at 5; *Cox Consent Decree* at para. 9.

89. Ohlhausen Address at 5; *Cox Consent Decree* at para. 17, 22.

90. Ohlhausen Address at 5; The FTC advocates for policies that ensure strong privacy protections for consumer data. The FTC participated in developing revised guidelines for protecting consumers in e-commerce at the Organization for Economic Co-operation and Development (OECD). The revised guidelines call for companies to implement "reasonable security safeguards and digital security risk management measures." FTC, PRIVACY & DATA SECURITY UPDATE 16 (2016*)*, https://perma.cc/3GSY-BNJ6.

91. Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FTC (Aug. 31, 2016, 2:34 PM), https://perma.cc/M9WM-Y2J8.

92. *Id.*

F. The FTC's Internet Privacy Regulation Stems From its Longtime Leadership in Consumer Protection

The FTC's heavy involvement in data security regulation stems from its longtime role as a leader in consumer protection.[93] In 1938, Congress gave the FTC authority to enforce against "unfair and deceptive acts or practices,"[94] and in 1975 Congress gave the FTC the power to adopt industry-wide trade regulation rules.[95] The FTC's jurisdiction over Internet privacy violations today is based on the agency's authority to proscribe "unfair or deceptive" practices impacting commerce.[96]

The FCC officially interjected itself in the privacy protection space on April 1, 2016, when it published its Privacy Notice of Proposed Rulemaking (NPRM).[97] The Privacy NPRM proposed significant privacy obligations for ISPs, which are the businesses that provide the necessary equipment for the Internet to function, such as Time Warner Cable, Verizon, AT&T, Cox, Charter, and others. [98] However, the notion that the FCC should enforce Internet privacy standards has not been a long-held belief of Democrats.[99] In fact, the Obama Administration's *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* ("Consumer Protection Bill of Rights") which was published in 2012 described the existing consumer data privacy framework as "strong."[100] Moreover, the Obama Administration's Consumer Protection Bill of Rights maintained that the legal landscape prior to the FCC's NPRM of 2016 "rests on fundamental privacy values, flexible and adaptable common law protections and consumer protection statutes, Federal Trade Commission

93. *Our History*, FTC, https://perma.cc/4XUD-KXM5 (since 1915, the FTC's mission has been to protect consumers and promote competition).

94. The FTC was adopted in 1914. Ch. 311, 38 Stat. 719 (1914). Section 5(a)(1) of the Act originally read: "Unfair methods of competition in commerce are hereby declared unlawful." The "unfair or deceptive acts or practices" language was added via the Wheeler-Lea Amendment in 1938. Ch. 49, 52 Stat. 111 (1938). The section was subsequently amended in 2003; Section 5(a)(1) presently provides that "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce are hereby declared unlawful." 15 U.S.C. § 45(a)(1) (2012).

95. *Id.*; Hart-Scott-Rodino Antitrust Improvements Act of 1975 15 U.S.C. § 18(a).

96. FTC, PRIVACY & DATA SECURITY UPDATE 2 (2016), https://perma.cc/3GSY-BNJ6.

97. *See* generally, Privacy *NPRM*.

98. *See* generally, Privacy *NPRM*; *Internet Service Provider Reviews*, TOP TEN REVIEWS, https://perma.cc/YP7E-7RGZ (last accessed Apr. 11, 2017).

99. Former Obama FTC Chairman Jon Leibowitz disagreed with the FCC's proposal to prohibit ISPs from offering discounted services in exchange for customers opting in to great data collection and use is not optical. In opposition to his fellow-Democrat appointees at the FCC, Leibowitz believed the rules' prohibition of something that consumers don't find problematic would stifle the development of free online services, and other low cost resources, due to increased transactional costs. John Eggerton, *Former FTC Chair Has Issues with FCC's Opt-in CPNI Regime*, MULTICHANNEL (May 11, 2016, 1:45 PM EST), https://perma.cc/PLF7-GTXG.

100. WHITE HOUSE PRIVACY FRAMEWORK at forward.

(FTC) enforcement, and policy development that involves a broad array of stakeholders."[101]

The Privacy NPRM demonstrated an expansion of the FCC's authority because it marked the first step of regulating a segment of industry that the FCC recently acquired jurisdiction of in the 2015 Open Internet Order, which reclassified BIAS as a common carrier service, an industry category that the FTC does not have authority over.[102] Section 222 of the Communications Act of 1934 places certain obligations on telecommunications service providers to protect consumer data acquired as a result of providing service.[103] From 1934–2015, BIAS were not considered common carriers, and therefore were subject to FTC regulations.[104] That changed in 2015 when the FCC approved the Open Internet Order, reclassifying BIAS as telecommunications services and finding that the Section 222 privacy requirements apply to BIAS.[105] The Privacy Order, which was adopted on October 27, 2016, clarified that the FCC, not the FTC, has jurisdiction over BIAS providers.[106] The FCC and the FTC thus have separate authority over two crucial categories of business that both directly handle potentially sensitive consumer data.[107] The FCC has jurisdiction over BIAS providers and the FTC has jurisdiction over ESPs.[108] The FCC relied on the FTC's Internet privacy model in part to create its Privacy Order.[109] But, the FCC also relied on its own work in adopting and

101. WHITE HOUSE PRIVACY FRAMEWORK at forward (privacy framework of 2012 is overall "strong" but lacks two elements: a clear statement of basic principles that apply to businesses, and a sustained commitment to all stakeholders regarding consumer data security issues, as needed based on advanced in technologies and business models).

102. 47 U.S.C. § 222 (2012); *see also,* 2015 Open Internet Order, 30 FCC Rcd at para. 193-95.

103. 47 U.S.C. § 222 (2012).

104. *Id.*; U.S. Telecomm. Ass'n v. FCC, 825 F.3d 674, 689 (D.C. 2016) (rejected numerous petitions for review and upheld the 2015 Open Internet Order).

105. *Id.*

106. "Because common carriers subject to the Communications Act are exempt from the FTC's Section 5 authority, the responsibility falls to this Commission to oversee their privacy practices consistent with the Communications Act." *Privacy Order* at para. 24; Order finds that BIAS—like other telecommunications carriers—were already "on notice that they have a duty" to keep private customer information confidential because of the FTC guidance that applied to BIAS *prior to* the FCC's reclassification of BIAS) (emphasis added). *Privacy Order* at para. 87; The Order "does not regulate the privacy practices of websites or apps, like Twitter or Facebook, over which the Federal Trade Commission has authority." *Fact Sheet: The FCC Adopts Order to Give Broadband Consumers Increased Choice Over Their Personal Information*, FCC 4, https://perma.cc/NNT6-G5LF (last accessed Apr. 11, 2017); "By reclassifying BIAS as telecommunications service, we have an obligation to make certain that BIAS providers are protecting their customers' privacy while encouraging the technological and business innovation that help drive the many benefits of our increasingly Internet-based economy." *Privacy Order* at 3.

107. *Privacy Order* at para. 9; FTC Report at vii-viii.

108. *Id.*; U.S. Telecomm. Ass'n v. FCC, 825 F.3d 674, 675 (D.C. 2016) (rejected numerous petitions for review and upheld the 2015 Open Internet Order).

109. *Privacy Order* at para. 9 (FCC provides that in formulating its rules, the FCC considered the FTC REPORT and the WHITE HOUSE PRIVACY FRAMEWORK. However, the FCC declined to sufficiently explain why it found the "heightened protections" for sensitive customer information was necessary due to the "vast swathes of customer data" available to ISPs).

revising rules under Section 222.[110] Even though the Privacy Order was repealed in April 2017, the FCC still has authority over ISPs under Title II.[111] However, the Privacy Order was repealed using the Congressional Review Act, which prohibits the agency from creating a new rule that is "substantially the same" as the one struck down.[112]

Unlike the FCC, the FTC has been involved in online privacy issues since nearly the beginning of the online marketplace.[113] The FTC does not have explicit authority to regulate privacy, but interprets Section 5 of the FTC Act's prohibition on unfair and deceptive trade practices to include, among other practices, violations of a company's stated privacy policy.[114] The FTC has "brought enforcement actions against Google and Facebook;" the court "orders obtained in these cases required the companies to obtain users' affirmative express consent before materially changing certain data practices."[115] The court orders also required the businesses "to adopt company-wide privacy programs that [external] auditors will assess for 20 years."[116] Additionally, the FTC has taken enforcement actions *inter alia* against mobile applications that violated the Children's Online Privacy Protection Act, entities that sold consumers lists to marketers in violation of the Fair Credit Reporting Act, and companies that failed to maintain reasonable data security standards.[117]

While the FTC has more experience in the data security realm than the FCC, the FTC does not employ specific rules like the FCC does.[118] Instead, the underlying reasonableness standard of the FTC's privacy framework is

---

110. *Privacy* Order at para. 4.

111. U.S. Telecomm. Ass'n v. FCC, 825 F.3d 674, 675 (D.C. 2016) (upheld FCC's reclassification of ISPs as telecommunication service in the 2015 Open Internet Order).

112. Congressional Review Act, 5 U.S.C. §§ 801(b)(2) (2012).

113. Press Release, *FTC Releases Report on Consumers' Online Privacy* (June 4, 1998), https://perma.cc/8YJU-J5EH.

https://www.ftc.gov/news-events/press-releases/1998/06/ftc-releases-report-consumers-online-privacy.

114. *See FTC v. Accusearch, Inc*., 570 F.3d 1187 (10th Cir. 2009) (holding the FTC Act was violated when a company sold confidential information).

115. *See United States v. Google Inc.* No. CV 12-04177 SI at *1-3 (N.D. Cal. 2012), https://perma.cc/6RY3-G38G (order approving stipulated order for permanent injunction and civil penalty judgement against Google Inc. ("Google") for violating a consent order with the FTC. Consent order was violated when Google used Gmail users' private information despite telling those users the information would be used only for Gmail services. Google must (1) pay a civil penalty of $22.5 million; (2) must maintain systems that delete cookies from Safari browsers; and (3) must report to the FTC within twenty days, setting forth how it is in compliance with the Proposed order); *In Re: Facebook, Inc.*, F.T.C. No. C-4365 3-7 (requiring Facebook to implement a comprehensive privacy program which is subject to independent third-party audit).

116. FTC REPORT at ii.

117. *Id.*

118. *Compare,* Thomas Pahl, *Your Cop on the Privacy Beat,* FTC BUSINESS BLOG (April 20, 2017, 11:12 AM) https://perma.cc/C9R4-MN2W ("As law enforcers, we walk the walk. To date, we've brought over 130 spam and spyware cases, over 120 Do Not Call cases targeting illegal marketing, over 100 Fair Credit Reporting Act actions, approximately 60 data security cases, more than 50 consumer privacy actions, almost 30 cases for violations of the Gramm-Leach-Bliley Act, and over 20 actions enforcing COPPA"); *with Privacy Order* at para. 1 (FCC began regulating data security with the implementation of the 2015 Privacy Order.

that "[c]ompanies should incorporate substantive privacy protections into their practices, such as data security reasonable collection limits, sound retention and disposal practices, and data security."[119] Holding companies responsible for adhering to their own privacy policies allows companies to craft their privacy policies in accordance with their respective business needs and size.[120] The flexibility that the FTC affords industry is much greater than the black and white rule of the FCC's Privacy Order, which determines a business's duty not based on its respective services or size, but based on the sensitivity of the data the business obtains.[121]

G. Despite Apparent Intent, the FCC's Privacy Order Stifles Innovation and Economic Growth, Ultimately Harming Consumers

The Privacy Order asserts that it gives BIAS consumers "the tools they need to make informed choices about the use and sharing of their confidential information" and ultimately protects consumers from harm.[122] The primary harms that the Privacy Order seeks to address include: (1) ISPs have access to too much data on their user's Internet activity;[123] (2) "truly pervasive encryption on the Internet is still a long way off";[124] and (3) ISPs have a special duty to their customers because of their relationship which is different from those involving ESPs because "consumers generally pay a fee for broadband service, and therefore do not have reason to expect that their broadband service is being subsidized by advertising revenues as they do with other Internet ecosystem participants."[125] The FCC unabashedly recognizes that its Privacy Order is not technology neutral, but it justifies the sector-specific rules with the argument that ISPs have distinctive characteristics and that the Privacy Order will somehow increase consumer confidence in ISPs and consequently improve business for ISPs.[126] Additionally, the FCC relies

119. FTC REPORT at vii.

120. *Id.*

121. *Privacy Order* at para. 3, 9.

122. *Privacy Order* at para. 9.

123. "BIAS providers maintain access to a significant amount of private information about their customers' online activity, including what websites a customer has visited, how long and during what hours of the day the customer visited various websites, the customer's location, and what mobile device the customer used to access those websites. *Privacy Order* at para. 33.

124. *Privacy Order*, at para. 34.

125. *Id.* at para. 35.

126. "[W]e disagree with commenters that argue that BIAS providers' insight into customer online activity is no greater than large edge providers because customers' Internet activity is "fractured" between devices, multiple Wi-Fi-hotspots, and different providers at home and work… 'customers who hop between ISPs on a daily basis often connect to the same networks routinely,' and as such over time, 'each ISP can see a substantial amount of that user's Internet traffic'." *Privacy Order* at para. 29-32, 53.

on a comment from Mozilla, an ESP that stands to gain from the FCC's sector-specific rules, to buttress its argument.[127]

The FCC's position that it should crack-down on ISPs due to the "unprecedented breadth" of data they may have access to does not acknowledge the arguably greater breadth of information that ESPs may have access to, which are not subject to the FCC's rules.[128] The FCC also declined to respond in its *Privacy Order* to the argument that ISPs often have limited insight into consumers' Internet use because consumers regularly switch to different BIAS providers as they use different devices, multiple Wi-Fi hotspots, and generally move from home to work throughout the day.[129]

The FCC requires BIAS providers to provide a way for consumers to affirmatively consent (opt-in) to the use, retention, and sharing of their data, whereas the FTC's privacy model encourages that Internet companies allow consumers to opt-out of the use, retention, and sharing of their data, and places special requirements on sensitive data.[130] The FCC's Privacy Rules require ISPs to ask permission of their customers to collect and use personal information; however, the scope of what constitutes personal information is overly broad.[131] The FTC and the FCC's frameworks differ in that the FTC's priority is security, whereas the FCC's priority is privacy.[132] The FTC appropriately focuses more on security, including PII, whereas the FCC focuses more on privacy, which is considerably more preferential than security which is primarily about safety.[133]

The newly adopted FCC broadband consumer privacy rules and the previously established FTC privacy protection policies, which apply to non-BIAS Internet businesses, appear to present multiple problems. First, it appears at best confusing and at worst unfair to customers for the FCC and the FTC to have inconsistent privacy protection practices.[134] Second, the

---

127. "The strength of the Web and its economy rests on a number of core building blocks that make up its foundational DNA. When these building blocks are threatened, the overall health and well-being of the Web are put at risk. Privacy is one of these building blocks." *Privacy Order* at para. 37.

128. *See, e.g.*, Peter Swire, Associate et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* at 24-25 (May 27, 2016) (The Institute for Information Security & Privacy at Georgia Tech, Working Paper) [hereinafter Swire Working Paper]; *see generally*, Andreea M. Belu, *The Massive Data Collection by Facebook – Visualized*, Data Ethics (June 26, 2017), https://perma.cc/DQ9X-MXJ6.

129. *See generally*, *Privacy Order*; Swire Working Paper at 3 ("[T]he average internet user has 6.1 connected devices, many of which are mobile and connect from diverse and changing locations that are served by multiple ISPs.").

130. *Privacy Order* at para. 9; FTC Report at vii-viii.

131. *Privacy Order* at para. 9; FTC Report at vii-viii, 15.

132. *See generally*, *Privacy Order*; FTC REPORT. Pai Dissenting Statement at 2 (commenting that the order is not "data-driven" but instead creates "corporate favoritism").

133. FTC REPORT at 18; *Privacy Order* at para. 1, 92, 134.

134. "I agreed with my colleague that consumers have a 'uniform expectation of privacy' and that the FCC thus 'will not be regulating the edge providers differently' from ISPs. I agreed that 'consumers should not have to be network engineers to understand who is collecting their data and they should not have to be lawyers to determine if their information is protected.'" Pai Dissenting Statement at 1.

inconsistent rules are unfair to businesses.[135] To the extent a business's ability to collect data on a customer is a problem, ESPs could potentially collect more data than their ISP counterparts.[136] For example, when a user checks her Gmail or uses Instagram multiple times a day, each time the user logs in to either Instagram or Gmail, both ESPs can track the user's browsing activity regardless of the ISP used in the transaction.[137] Conversely, the relevant ISPs involved in an individual's Gmail and Instagram activity are likely exposed to only a fraction of the user's Internet activity.[138] This is because a user may access ESPs using a variety of ISPs as she uses different devices on different Wi-Fi hotspots at home, work, and public spaces throughout the day.[139] Third, the FCC's Privacy Order does not appear to protect consumers' privacy in a substantial way, especially because edge providers, which are not subject to FCC regulations, are likely to have more private information from consumers than ISPs, which do not fall under the FCC's jurisdiction.[140]

Given that Internet data security is important to the government, private companies, and consumers,[141] it is essential that the federal government establish clear and reasonable online privacy policies that adequately protect consumers without needlessly stifling corporate competition or innovation. The Consumer Technology Association argued in its comment to the Privacy NPRM that "[b]y setting such stringent restrictions, consumers likely will miss out on what could otherwise be welcomed opportunities, such as receiving discounts, offerings, and information about new services, or even enjoying customized user experiences based on data collected."[142] The problems presented by the Privacy Order are threefold.[143] The FCC and FTC's respective online privacy rules are inconsistent such that they are confusing

135. Pai Dissenting Statement at 2 (order is not data-driven, and creates corporate favoritism).

136. Swire Working Paper at 4, 8 (non-ISPs have unique insights into "user activity" via "many contexts," including "social networks, search engines, webmail, and messaging, operating systems, mobile apps, interest-based advertising, browsers, Internet video, and e-commerce").

137. *Id*. at 4. This concept is referred to as "cross-context tracking." Cross-context tracking is dominated by non-ISPs. Services provided by non-ISPs that dominate cross-context tracking include social networks, search engines, webmail and messages, operating systems, mobile apps, interest-based advertising, browsers, internet video, and e-commerce.

138. *Id.*

139. *Id.*; "Nothing in these rules will stop edge providers from harvesting monetizing your data, whether it's the website you visit or the YouTube videos you watch or the emails you send or the search terms you enter on any of your devices." Pai Dissenting Statement at 2.

140. Pai Dissenting Statement at 1-2 (ESPs are currently "dominant" in online advertising marketing, and the Privacy Order doesn't stop ESPs from "harvesting or monetizing" data).

141. *See generally*, Alden Abbot, *The Federal Gov't's Appropriate Role in Internet Privacy Regulation*, THE HERITAGE FOUNDATION (Oct. 27, 2016), https://perma.cc/VWJ2-EPMB.

142. Comment of Consumer Technology Association at 9-10, *Privacy NPRM*.

143. *Privacy Order*.

to consumers,[144] unfair to businesses, and harmful to consumers, ESPs, and ISPs.[145] To understand why the Privacy Order is an inappropriate response to an arguably nonexistent harm, one must first understand the legal framework for Internet service businesses, including ISPs, and their respective histories relating to privacy rules and regulations.

1. The Evolution of the Open Internet Order and its Impact on ISP Privacy Rules

The FCC did not have the authority to enact rules applicable to Title II common carriers, which include BIAS, until the agency adopted the Protecting and Promoting the Open Internet Order (Open Internet Order) on February 26, 2015.[146] The Open Internet Order reclassified wired and mobile BIAS as telecommunications services.[147] More specifically, the reclassification subjected BIAS to several new rules and to certain provisions of Title II of the Communications Act.[148] The Open Internet Order did not focus on privacy; however, it provided the necessary legal groundwork for the Privacy Order.[149]

Prior to the Open Internet Order, the FCC treated BIAS as a largely unregulated information service.[150] In *National Cable & Telecommunications Ass'n v. Brand X*, the Supreme Court upheld the FCC's decision to classify cable broadband service as an information service.[151] The Court also found that the definitions of telecommunication service and information service in the Communication Act were ambiguous, and that the FCC reasonably interpreted the ambiguous provisions.[152] However, after reassessing the nature of BIAS, in addition to changes in consumer perception since *Brand X*, the FCC reclassified wired and broadband BIAS as a telecommunication service.[153] This reclassification included interconnection agreements between ISPs and ESPs within the scope of the newly-regulated broadband service.[154]

---

144. "I agreed with my colleague that consumers have a "uniform expectation of privacy" and that the FCC thus "will not be regulating the edge providers differently" from ISP. I agree that "consumers should not have to be network engineers to understand who is collecting their data and they should not have to be lawyers to determine if their information is protected." Pai Dissenting Statement at 1.

145. Pai Dissenting Statement at 3-4 (order is not data-driven, and creates corporate favoritism); Ohlhausen Address at 5.

146. *2015 Open Internet Order*, *supra* note 18, at para. 5, 25.

147. *2015 Open Internet Order*, *supra* note 18, at para. 29.

148. *U.S. Telecomm. Ass'n v. FCC*, 825 F.3d 674, 675 (D.C. Cir. 2016) (rejected numerous petitions for review and upheld the 2015 Open Internet Order).

149. KATHLEEN ANN RUANE, CONG. RESEARCH SERV., R40234, NET NEUTRALITY: THE FCC'S AUTHORITY TO REGULATE BROADBAND INTERNET TRAFFIC MANAGEMENT 6 (2014), https://perma.cc/9KV3-5F8P.

150. *See* Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 976 (2005) (upholding BIAS classification as information service).

151. *Id.* at 974.

152. *Id.* at 986-87.

153. *See 2015 Open Internet Order*., 355.

154. *Id.* at para. 29.

In *U.S. Telecomm. Ass'n v. FCC* the Court of Appeals for the D.C. Circuit upheld the Open Internet Order, specifically the FCC's reclassification of broadband services as telecommunications services subject to common carrier regulation under Title II of the Communications Act of 1934.[155] By upholding the Open Internet Order in its entirety, the D.C. Circuit essentially upheld nearly "open-ended power by the FCC to regulate BIAS", including BIAS rate regulation, regulation of when and how broadband networks exchange traffic, and "general conduct" regulation of network management decisions by broadband providers.[156]

2. The FTC has Long Been the Nation's Premier Privacy and Data Security Enforcement Agency

To understand the inappropriateness of the FCC's new privacy rules, it is instructive to understand the FTC's already existing high-functioning model. The primary law enforced by the FTC is the FTC Act which prohibits "unfair" and "deceptive" acts or practices in or affecting commerce.[157] Under Title 5 of the FTC Act, the FTC has brought data security enforcement actions against *inter alia* major ESPs like Google and Facebook, as well as violators of the FCRA, and online advertising networks that failed to honor consumers' opt-out choices.[158] A misrepresentation or omission under the FTC Act is deceptive if it is both material and likely to mislead consumers acting reasonably under the circumstances.[159] Additionally, an act or practice is unfair under the FTC Act if it causes, or is likely to cause, substantial injury that is not reasonably avoidable by consumers, as well as not outweighed by any benefits to consumers or competition generally.[160]

While the FCC has just begun its ISP regulation, the FTC has long been the nation's premier privacy and data security enforcement agency, bringing over 500 enforcement actions regarding the privacy and security of customer information.[161] Moreover, the FTC has extensive experience with actions against ISPs and against some of the most powerful Internet companies.[162] Some of the many companies under FTC orders include Microsoft, Facebook,

---

155. *See* Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 976 (2005).

156. *2015 Open Internet Order*; Seth L. Cooper, *DC Circuit Upholds Open-Ended Power to Regulate Broadband*, The Federalist Society (June 15, 2016), https://perma.cc/26DJ-39ZS.

157. An act or practice is "unfair" if it causes, or is likely to cause, substantial injury that is not reasonably avoidable by consumers, and not outweighed by other benefits to consumers or competition. 15 U.S.C. § 45(a) (2012); *See* FTC Policy Statement on Unfairness, *appended to Int'l Harvester Co*., 104 F.T.C. 949, 1070 (1984), *available* https://perma.cc/YG4Y-RU2Y; 15 U.S.C. §45(n) (2012).

158. FTC REPORT at ii.

159. *Id.*

160. *Id.*

161. *See* Letter from Edith Ramirez, Chairwoman, FTC, to Věra Jourová, Commissioner for Justice, Consumers, and Gender Equality, European Commission, 3 (Feb. 23, 2016), https://perma.cc/2DJC-LGKQ.

162. https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises.

Google, Equifax, HTC, Twitter, Snapchat, and Wyndham Hotels.[163] The FTC also conducts "extensive consumer and business outreach and guidance, coordinate[s] workshops to foster discussions about emerging privacy and data security issues, coordinate[s] on international privacy efforts, and advocate[s] for public policies that protect privacy, enhance security, and improve consumer welfare."[164] In a broad array of cases, "the FTC has alleged that companies" of varying sizes "made deceptive claims about how they collect, use, and share consumer data; failed to provide reasonable security for consumer data; deceptively tracked consumers online; spammed and defrauded consumers; installed spyware or other malware on consumers' computers; violated … telemarketing rules; shared highly sensitive, private consumer data with unauthorized third parties; and publicly posted such data online without consumers' knowledge or consent."[165] The FTC is so well-versed in the issues of privacy and consumer protection that it distributes educational materials on a host of topics, including mobile applications (apps), children's privacy, and data security.[166] The FTC's most recent business education program is the "Start with Security" initiative, which includes new guidance for businesses on the lessons learned from the FTC's data security cases, as well as seminars across the nation.[167]

3. The Privacy Order Demonstrated the Expanded Scope of the FCC's New Privacy Authority, Including a Broader Definition of the Types of Data Needing Special Protections

The Privacy Order established new legal obligations for ISPs.[168] The new requirements apply to customer proprietary information, a newly defined term which includes "individually identifiable CPNI, personally identifiable information and content of communications."[169] The Privacy Order also

163. *See generally*, Privacy and Security Cases, FTC, https://perma.cc/Y46E-LH6V.

164. *Statement of FTC Commissioner Maureen K. Ohlhausen Regarding Comment of the Staff of the Bureau of Consumer Protection of the FTC , Privacy NPRM* at 1 (May 27, 2016), https://perma.cc/767V-U759 [hereinafter Ohlhausen *Privacy NPRM* Statement]; *see, e.g.*, FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES (Jan. 2016), https://perma.cc/R7FC-MCYL [hereinafter Big Data Report]; FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (June 2015), https://perma.cc/78JP-4XUB.

165. Comment of the Staff of the Bureau of Consumer Protection of the FTC at 2-3, *Privacy NPRM*, https://perma.cc/3EXY-7WRX.

166. *See generally* Press Release, *FTC Kicks Off "Start with Security" Business Education Initiative* (June 30, 2015); FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (June 2015), https://perma.cc/78JP-4XUB; *Mobile App Developers: Start with Security*, FTC, https://perma.cc/8ABD-MSHX; *Protecting Your Child's Privacy Online*, FTC, https://perma.cc/QHQ8-UUYC.

167. *See generally* Press Release, *FTC Kicks Off "Start with Security" Business Education Initiative* (June 30, 2015); FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (June 2015), https://perma.cc/78JP-4XUB.

168. *Privacy Order* at para. 27.

169. *Privacy Order* at para. 85.

broadly defines a customer as any current or former subscriber to a telecommunications service, or an applicant for a telecommunications service, meaning that an ISP's duty to protect customer PI begins before service starts and continues after service is terminated.[170] As defined in Section 222(h)(1) of the Communications Act, CPNI is information that relates to "the quantity, technical configuration, type, destination, location, and amount of use" of telecommunications service that is provided by the customer in the context of a carrier-customer relationship.[171] Consistent with its past binding and guidance documents, the FCC's Privacy Order did not provide a comprehensive list of CPNI, but instead provides that CPNI in the broadband context includes but is not limited to the following: broadband service plans, geolocation, Mac addresses and other device identifiers, IP addresses and domain name information, traffic statistics, port information, application header, application usage, application payload, and customer premises equipment and devise information.[172]

The FTC has developed its privacy program using its long-established principles of combatting unfairness and deception.[173] Due to the FTC's focus on long-established principles of unfairness and deception, the FTC's privacy program focuses on the sensitivity of consumer data and the specific promises made about data collection and use, instead of the type of entity that collects or uses the data.[174] Notably, the FTC's definition of sensitive customer data includes Social Security numbers, financial, health, children's and geographical information, but does *not* include content of communications, web browsing activity or application usage history, which are included in the FCC's Privacy Order.[175]

4. The Privacy Order Sets New Transparency and Notice to Consumer Requirements for ISPs

The Privacy Order places the following new requirements on all ISPs: (1) provide privacy notices that explain what user information they collect, how that information is used, in what context it is shared, and the types of entities it is shared with; (2) "inform customers" of their "rights to opt-in or opt-out of the use or sharing of their information"; (3) "present their privacy notices to customers at [both] the point of sale" and after in an "easily accessible" manner; and (4) "give customers advance notice of material changes" to the ISP's "privacy policies."[176] "Heightened disclosures" are

170. *Id.* at 64.2002(e) (Definition of 'Customer').

171. 47 U.S.C. § 222(h)(1) (2012).

172. *Privacy Order* at para. 53.

173. The FTC's case-by-case application of these general principles has major advantages over a prescriptive rulemaking approach. The FTC's approach minimizes the regulator's knowledge problem, fosters incrementalism, and focuses limited resources on addressing consumer harm. *See* Maureen K. Ohlhausen, *The FCC's Knowledge Problem: How to Protect Consumers Online*, 67 FED. COMM. L.J. 203 (2015), https://perma.cc/Z9XM-U2MC.

174. FTC REPORT at 24.

175. FTC REPORT at 15; *Privacy Order* at para. 9.

176. *Privacy Order* at para. 125.

necessary under the Privacy Order for what the Commission calls "pay for privacy plans," which is when an ISP offers discounts or other incentives in exchange for a customer's express affirmative consent to the use and sharing of their personal information.[177]

H. The Privacy Order Sets New Customer Choice and Consent Rules, which Includes a Three-tiered Approach: Opt-in, Opt-out, and Inferred Consent

Before an ISP can use or share customer PI under the Privacy Order, it must obtain that individual's consent.[178] The three allowable consent mechanisms under the Privacy Order are: opt-in, opt-out, and inferred consent.[179] All the consent mechanisms apply to different types of customer PI. The appropriate method depends on the information's sensitivity and its treatment under the statute. For example, opt-in consent requires affirmative permission from the customer to use or share "sensitive" customer PI.[180] Opt-in consent is also necessary for retroactive changes to an ISP's privacy policies.[181] Secondarily, opt-out consent is required for the use and share of all non-sensitive PI.[182] Thirdly, inferred consent is permissible in limited circumstances. For example, ISPs may infer consent to use customer information to provide the underlying service, bill for that service, to prevent fraudulent use of the ISP's network, and other purposes specified in the statute.[183]

I. The Most Significant Difference Between the FCC's Three-tiered Consent Framework and the FTC's Existing Privacy and Data Security Guidelines is the Privacy Order's Treatment of Web Browsing and Application Usage History

The most significant difference between the consent framework articulated in the Privacy Order and the FTC's existing privacy and data security is the order's treatment of web browsing activity and application usage history.[184] The FTC has never considered this information *per se* sensitive, and therefore, has never required opt-in consent for use or

177. *Id.* at para. 298-303.
178. *Id.* at para.192-195.
179. *Id.* at para. 365.
180. *Id.* at para. 193.
181. *Id.* at para. 195.
182. *Id.* at para. 194.
183. *Id.* at para. 201.
184. *Privacy Order* at para. 9; FTC Report at vii-viii.

sharing.[185] The Privacy Order dramatically diverges from the FTC's position on web browsing and app usage history.[186] In the Order, the FCC asserts that because ISPs have the unique ability to see all of a user's unencrypted traffic, that browsing and app usage history must be considered sensitive in the communications context and be subject to opt-in consent.[187] The FCC declines "to define a subset of non-sensitive web browsing and app usage history."[188] The Privacy Order also dismisses numerous commenters' arguments that the existence of encryption on websites and apps significantly decreases the potential amount of data an ISP may access.[189]

In contrast to the FCC's over-inclusive definition of sensitive data, the FTC considers the application of its privacy framework on a case-by-case basis. The FTC recognizes that Internet companies in the healthcare and financial services industries are also subject to other statutes, like "the Health Insurance Portability and Accountability Act ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the Gramm-Leach-Bliley Act ("GLBA")," which "impose privacy protections and security requirements through legal obligations" on companies.[190] Since the FTC's privacy framework is intended to encourage best practices, rather than create conflicting or duplicative requirements, "to the extent that components of the [FTC's privacy framework] exceed, but do not [contradict] existing statutory requirements, [companies] covered by those statutes should view the [FTC's framework] as best practices to promote consumer privacy."[191]

Thus, according to the FTC's definition of sensitive data, the FCC's rule would require opt-in consent for many uses of non-sensitive consumer data by ISPs, as compared to the FTC's sensitivity framework.[192] The opt-in consent system that the FCC advocates is similar to the standards employed in Europe, where citizens have a "right[s] to make search engines remove

185. FTC REPORT at 16-17; CTIA Comment ("To justify diverging from the FTC's framework and defining Web browsing history as 'sensitive,' the commission… cherry-picked evidence in an attempt to show that ISPs have unique and comprehensive access to consumers' online information."); Rather than finding web browsing *per se* sensitive, the FTC considers if the types of data the software will monitor, record, or transmit are "clearly and prominently" communicated to users. Sears Settles FTC Charges Regarding Tracking Software, FTC (June 4, 2009), https://perma.cc/J4LJ-2CQA.

186. *Privacy Order* at para. 9; FTC Report at vii-viii.

187. *Privacy Order* at para. 134 - 135. .

188. *Id.* at para. 15, 181.

189. *Compare Privacy Order* at para. 186 ("[T]he existence of encryption on websites or even in apps does not remove browsing history from the scope of sensitive information… [E]ncryption is far from fully deployed; the volume of encrypted data does not represent a meaningful measure or privacy protection…"), *with* Swire Working Paper at 3 ("We present new evidence on the rapid shift to encryption, such as the HTTPS ersion of the basic web protocol. Today, all of the top 10 web sites either encrypt by default or upon user log-in, as do 42 of the top 50 stes… Encryption such as HTTPS blocks ISPs from having the ability to see users' content and detailed URLs.").

190. FTC REPORT at 16, 58.

191. *Id.*

192. *Id.* at 47, 58-59; Comment of the Staff of the Bureau of Consumer Protection of the FTC at 2-3, *Privacy NPRM*, https://perma.cc/5SMW-5DCW.

search results about themselves, including links to news articles and other information."[193] The European Union's broad embrace of opt-in policies, and its recognition of the "right to be forgotten" has proven highly problematic for businesses and challenging to execute.[194] However, the FTC recommends, but does not require, opt-in consent for unexpected collection or use of consumers' sensitive data, such as Social Security numbers, financial information, and information about children. [195]

While the FTC's policies are better than those in the FCC's Privacy Order, they are not without fault. The FTC urges that companies adopt industry best practices, but falls short of providing a clear delineation of what duties an ISP owes to its consumers; the gaps in the FTC's privacy framework present opportunities for Congressional action.

Unlike the FCC's approach, the FTC's approach reflects the fact that consumer privacy preferences differ greatly depending on the type of data and its use. The FTC's research and the Pew Research Center have found that consumers overwhelmingly object to entities accessing their sensitive data without permission, but do not object to the access of their non-sensitive data.[196] Notably, to the extent consumers are concerned about entities accessing their financial and medical data without permission, both financial institutions and healthcare entities are subject to heightened statutory standards.[197]

1. The FTC's Online Privacy Rules are Designed to Minimize the Burden on Consumers and Business, Whereas the FCC's Approach Needlessly Creates a Burden

The FTC approach to privacy takes into consideration that obtaining consent can be burdensome for consumers and business. Reading a notice about privacy and making a decision based on that notice takes time, which,

193. Daphne Keller & Bruce D. Brown, *Europe's Web Privacy Rules: Bad for Google, Bad for Everyone*, N.Y.TIMES (Apr. 25, 2016), https://perma.cc/QP4D-PQJT.

194. *Id.*

195. *Compare Privacy Order* at para. 125,*with* FTC REPORT at vii-viii; Comment of FTC Staff of the Bureau of Consumer Protection 2-3, *Privacy NPRM*, https://perma.cc/5SMW-5DCW.

196. See, Remarks of Maureen K. Ohlhausen, 2016 Advertising and Privacy Law Summit (June 8, 2016), 5 n.11, https://www.ftc.gov/system/files/documents/public_statements/955183/160608kellydrye.pdf (A recent Pew survey and focus groups testing consumer privacy preferences with regard to six different scenarios found 17% of polled rejected all the scenarios, 4% accepted all the scenarios, and the substantial majority indicated that at least one of the scenarios was potentially acceptable. Lee Rainie & Maeve Duggan, Privacy and Information Sharing, PEW RESEARCH CENTER (Dec. 2015), http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/).

197. FTC REPORT at 16 (statutes such as HIPAA, HITECH, and GLBA already impose privacy protections and security requirements through legal obligations on companies regulated by the FTC).

"in the aggregate, can be quite substantial."[198] The FTC's policy is based on the theory that regulations should impose costs in a way that maximizes benefits and simultaneously minimizes costs.[199] In its enforcement capacity, the FTC generally urges an opt-out approach for non-sensitive information, and an opt-in approach for uses of sensitive information.[200] Clarifying the FTC's position on regulations and their corresponding transactional costs, former FTC Chairman Tim Muris and former Director of the FTC's Bureau of Consumer Protection Howard Beales stated:

> Consumers rationally avoid investing in information necessary to make certain decisions ... when their decision is very unlikely to have a significant impact on them ... Default rules should be designed to impose those costs on consumers who think they are worth paying. An opt-out default rule means that consumers who do not think that decision making costs are worthwhile do not need to bear those costs. Consumers who care intensely, however, will face the costs of making a decision.[201]

The FTC also chooses not to impose regulation defaults that do not coincide with consumer preferences, because doing so imposes an unnecessary cost to consumers and businesses without improving consumer outcomes.[202] Additionally, a broad opt-in requirement could burden and negatively affect industry innovation, growth, and competition as businesses must reallocate resources to comply with regulations.[203]

Moreover, lumping app usage histories and "their functional equivalents" in the same category of sensitivity as Social Security numbers, as the Privacy Order does, is too broad of a category that will create unnecessary transaction costs for businesses and consumers.[204] For example, under the FCC's approach, a customer's medical and financial records would require the same degree of privacy as a customer's shopping or media preferences if that information is shared with a BIAS, because shopping and

198. Remarks of Maureen K. Ohlhausen, 2016 Advertising and Privacy Law Summit (June 8, 2016), https://www.ftc.gov/system/files/documents/public_statements/955183/160608kellydrye.pdf.

199. Remarks of Maureen K. Ohlhausen, 2016 Advertising and Privacy Law Summit (June 8, 2016), https://www.ftc.gov/system/files/documents/public_statements/955183/160608kellydrye.pdf.

200. Ohlhausen *Privacy NPRM* Statement 2.

201. J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 115 n.20 (2008).

202. Ohlhausen *Privacy NPRM* Statement 2.

203. *See* Daniel Castro & Alan McQuinn, *The Economic Costs of the* European *Union's Cookie Notification Policy*, THE INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (Nov. 2014) at 7, https://perma.cc/5QBL-JRHE; PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE x-xi (May 2014) ("[A] policy focus on limiting data collection will not be a broadly applicable or scalable strategy – nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth.").

204. *Privacy Order* at para. 9.

media preferences fit in the category of "web browsing and application usage history."[205]

III. ANALYSIS

The FCC's Privacy Order provides that "privacy rights are fundamental because they protect important interests" including "freedom from identity theft, financial loss, or other economic harms, as well as concerns [regarding] intimate, personal details."[206] The FTC Bureau of Consumer Protections Board echoed the FCC's sentiment in its Comment on the FCC's Privacy NPRM, maintaining that the FCC's goal of promoting transparency, consumer choice, and security is laudable.[207] The Privacy Order and the FTC's Comment to the Privacy Order provide that there is universal agreement that Internet data security rules are necessary. However, the FCC is wrong in its assessment of the potential risks and harms to businesses and consumers. Manifesting the concerns of many commenters in response to the FCC's Privacy NPRM, the Privacy Order conceives of an exaggerated possible harm and is overly broad in its imposition of burdensome transactional costs on businesses and customers. Requiring ISPs to implement new customer consent platforms in accordance with the Privacy Order will create a new cost, which will ultimately be absorbed by consumers.[208] Even though the FCC and the FTC have jurisdiction over different types of Internet companies, the FCC failed to demonstrate why it was necessary for it to diverge from the long-standing and successful policies of the FTC.

Although the FTC is in a better position than the FCC to enforce Internet data security, neither agency has flawless online privacy policies.[209] While the FCC's consumer protection-focused model employs reasonableness standards and considers industry-wide best practices, it leaves exactly what a company must do to avoid liability somewhat ambiguous.[210] It is unquestionable that Internet data security is important. Americans should be able to use the Internet freely with a reasonable expectation that their confidential information, like financial and medical data, will be kept private and that there is transparency regarding the level of privacy afforded to communication via the Internet. It follows that the government should create

205. *Id.*

206. *Id.* at para. 1.

207. Comment of FTC Staff of the Bureau of Consumer Protection at 2-3, *Privacy NPRM*, https://perma.cc/5SMW-5DCW (acknowledges that FCC recognizes the importance of protecting consumer privacy ands "commends the FCC for its attention to these issues" and provides comments, based on the FTC's decades of experience).

208. "The goal of consumer protection enforcement isn't to make headlines; it is to make harmed consumers whole and incentivize appropriate practices. The costs imposed by a regulator on a legitimate, non-fraudulent company are ultimately born by its consumers. If enforcement action imposes costs disproportionate to the actual consumer harm, that enforcement action may make consumers worse off if prices rise or innovation slows." Ohlhausen Address at 5.

209. See generally, Privacy Order; FTC REPORT.

210. Ohlhausen Address at 5; FTC, PRIVACY & DATA SECURITY UPDATE 16 (2016), https://perma.cc/3GSY-BNJ6.

and enforce standards that protect Internet consumers' privacy while also recognizing the potential burdens that overregulation can place on businesses, primarily in the form of cumbersome and costly unfunded mandates for things like opt-in or out-out platforms. An appropriate data security legal framework will ensure that customers' private information is secure and that consumers are able to choose what types of information they want kept private, aside from the data that is already statutorily classified as sensitive, like financial and medical matters.

Data security breaches can cause serious harms; however, the FCC's Privacy Order goes too far and creates harms in the form of imposing unnecessary transaction costs on businesses and consumers, and potentially confusing customers. Because the FTC provides more of a patchwork common law than a clear set of standards that ESPs must abide by, as will be discussed in subsequent sections, the ideal solution is for Congress to act to streamline Internet data security policies under the FTC's jurisdiction.

A. The FCC's Privacy Order Creates Confusion for Customers

An Internet user should not need to be a lawyer or network engineer to understand how her privacy will or will not be protected. "For the last two decades, the United States has embraced a technology-neutral framework for online privacy," meaning that the framework administered by the FTC applied across all sectors of the Internet.[211] What this meant for customers is that regardless of whether they were using an ESP, like Google or Facebook, or a BIAS provider like Comcast or AT&T, the consumer had a uniform expectation of privacy. Prior to the FCC's entry into online privacy regulation, the FTC's unified approach allowed Internet users to "rest assured knowing that a single and robust regulatory approach" protected online data.[212]

By failing to parallel the FTC's approach, the FCC has created unnecessary confusion for customers. The FCC's recent Privacy Order requires users to opt-in to sharing information with BIAS providers, regardless of the sensitivity of the information. However, because a BIAS simply provides the infrastructure necessary for ESPs to function and interface with consumers, a reasonable customer may wrongly assume that when she opted-in to sharing data with her BIAS, she also opted-in to sharing data with the ESP she used by way of her BIAS provider. This not only will create confusion for customers, but will also likely create a customer service problem for BIAS and ESP companies. Customers will likely call their BIAS and ESPs concerned about their respective compliance because the FCC's opt-in/opt-out model based on the type of entity rather than the type of content is confusing. It is logical for the FCC to parallel the FTC's approach as closely as possible because doing so would allow consumers to better understand how their information is and is not protected under the law. Moreover, consumers

211. Pai Dissenting Statement at 1; *Privacy Order* at 209.
212. *Id.*

have a "uniform expectation of privacy" and an expectation that the FCC will not regulate ISPs differently from ESPs.[213]

B. The FCC's Privacy Order is Unfair to Businesses

It is problematic for the FCC and the FTC to treat ISPs and ESPs differently, especially considering the average Internet user does not understand the highly technical distinction between the two types of businesses. It is unfair to subject one sector of industry to a significantly increased burden compared to another sector of industry. Also, if the FCC is so concerned about privacy and security, it should focus on protecting sensitive information. Not only is it unfair to target BIAS providers and not ESPs, but the Privacy Order also does not serve a purpose of helping customers because it is overly broad in its classification of potentially sensitive data, ultimately making it more difficult for consumers to experience the benefits of subsidized costs by third parties, and the corresponding targeted advertisements and deals that are often associated with third party advertisers. In addition, to the extent BIAS and ESPs should be treated differently under the law, ESPs are technologically able to collect more sensitive information than ISPs. For instance, financial institutions, retail, and social media websites are predominantly ESPs, not ISPs, and are therefore obligated to follow the FTC's more lenient and reasonable approach.[214] The FTC takes a flexible approach to data security, assessing reasonableness based, among other things, on the sensitivity of the information collected, the measures the company has implemented to protect such information, and whether the company acted to address and prevent "well-known and easily addressable security vulnerabilities."[215]

Moreover, the FTC has a track record of enforcing data security. In February 2017, under a Republican-led FTC, "VIZIO, Inc., one of the world's largest manufacturers and sellers of Internet-connected 'smart' televisions, agreed to pay $2.2 million to settle charges by the FTC and the Office of the New Jersey Attorney General that it installed software on its TVs to collect viewing data on 11 million consumer TVs without the consumers' knowledge or consent."[216] In December 2016, Turn Inc., a California-based company which enables sellers to "target digital advertisement to consumers, agreed to settle FTC charges that it deceived consumers by tracking them online and through their mobile applications, even after consumers opted-out of such tracking."[217] As part of the settlement, consumers must be able to limit

213. *Id.*

214. Maureen K Ohlhausen (fn 47 above).

215. FTC REPORT at n.108.

216. Press Release, *VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges it Collected Viewing Histories on 11 Million Smart Televisions without Users'* Consent, FTC (Feb. 6, 2017), https://perma.cc/PS98-KNK9.

217. Press Release, *Digital Advertising Co. Settles FTC Charges it Deceptively Tracked Consumers Both Online and Through Their Mobile Devices*, FTC (Dec. 6, 2016), https://perma.cc/8R54-UYH4.

targeted advertisements on Turn Inc.'s website.[218] Also in December 2016, the operators of AshleyMadison.com, a dating website based in Canada, "agreed to settle [FTC] and state charges that they deceived consumers and failed to protect 36 million users' account and profile information in relation to a [major] July 2015 data breach of their network".[219] These are just a few examples of the FTC appropriately exercising its enforcement capacity to protect consumers.

The Privacy Order attempts to justify its crackdown on ISPs by saying that "edge providers only see a slice of given consumer Internet traffic" whereas "a BIAS provider sees 100 percent of a customer's unencrypted Internet traffic."[220] However, this belief is fundamentally flawed because ISPs' "access to data is not comprehensive" due to "technological developments" that "place substantial limits on ISPs' visibility." Additionally, an ISP's "access to user data is not unique" because "other companies often have access to more information and a wider range of user information than ISPs."[221]

ESPs have a strong interest in studying both identifiable and non-identifiable consumer Internet traffic because doing so allows them to better-cater to prospective and current customers, ultimately helping their businesses as consumers choose to return to their ESPs.[222] The Obama Administration discussed the benefits of ESP's capacity to collect and use "personal information in its 2014 Big Data report."[223] The report maintained that benefits include "improved fraud detection and cybersecurity, and 'enormous benefits' associated with targeted advertising" that allows consumers to reap "the benefits of a robust digital ecosystem that offers a broad array of free content, products, and services."[224]

FCC Chairman Pai maintains that the amount of data collected by ESPs daily is staggering.[225] Pai also asserts that the FCC simply wants to treat ISPs different from ESPs and is, therefore, claiming that ESPs only see a "slice" of

---

218. *Id.*

219. *Operators of AsheleyMadison.com Settle FTC, State Charges Resulting from 2015 Data Breach that Exposed 36 Million Users' Profile Information*, FTC (Dec. 14, 2016),https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting.

220. *Privacy Order* at para. 30.

221. When an ESP encrypts its website, it limits visibility to the ISP. As of 2016, "all of the top 10 websites either encrypt by default or upon user log in, as do 42 of the top 50 sites… There clearly can be no 'comprehensive' ISP visibility into user activity when ISPs are blocked from a growing majority of user activity" due to encryption. Swire Working Paper at 3. ESPs are increasingly gathering commercially valuable information about user activity via multiple contexts, such as: social networks, search engines, webmail and messaging, operating systems, mobile apps, internet-based advertising, browsers, Internet video, and e-commerce. Swire Working Paper at 4.

222. *See generally*, BIG DATA REPORT at 39.

223. "Big Data: Seizing Opportunities, Preserving Values," Executive Office of the President, The White House (May 2014).

224. BIG DATA REPORT at 40-41, 50.

225. https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A5.pdf.

users' online data.[226] However, ESPs access far more than a "slice" of customer's data.

> The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem. Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. However, all pathways lead to essentially one Internet search company and one social network company. Privacy rules for ISPs are important and necessary, but it is obvious that the more substantial threats for consumers are not the ISPs.[227]

Additionally, refuting the FCC's assertion that ISPs rather than ESPs must be reined in because ESPs have access to significantly less data compared to their ISP counterparts, are several recent news reports indicating the significant capacity of particularly powerful ESPs regarding consumer protection. In his dissenting statement, then-Commissioner Pai highlighted the following news headlines: "Google quietly updates privacy policy to drop ban on personally identifiable web tracking,"[228] "Privacy Debate Flares With Report About Yahoo Scanning Emails,"[229] "Apple keeps track of all the phone numbers you contact using iMessage,"[230] "Twitter location data reveals users' homes, workplaces,"[231]and "Amnesty International rates Microsoft's Skype among worst in privacy."[232] Thus, contrary to the FCC's position in its Privacy Order, ESPs arguably have more insight into consumer data than ISPs.[233]

Since the FCC has not presented a compelling reason as to why ISPs should be subjected to more stringent standards than ESPs, aside from the "slice" argument, which is refuted by data, the FCC's regulation of ISPs appears to be corporate favoritism because it enables ESPs to transact business in a much less cumbersome and expensive way compared to their ISP counterparts who must follow the FCC's rules and regulations.[234] If both

---

226. Pai Dissenting Statement at 2.

227. *Privacy Order* at 210, citing EPIC Comments at 15.

228. https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A5.pdf; Anmol Sachdeva, *Google Quietly Updates Privacy Policy to Drop Ban on Personally Identifiable Web Tracking*, THE TECH PORTAL (Oct. 21, 2016), https://perma.cc/X6JN-3434.

229. Robert McMillan & Damian Paletta, *Privacy Debate Flares With Report About Yahoo Scanning Emails*, WSJ. (Oct. 5, 2016), https://perma.cc/F5T3-4KF4.

230. Oscar Raymundo, *Apple Keeps Track of All the Phone Numbers You Contact Using iMessage*, MACWORLD (Sept. 28, 2016), https://perma.cc/LVV5-HBNG.

231. Patrick Nelson, *Twitter Location Data Reveals Users' Homes, Workplaces*, NETWORKWORLD (May 18, 2016), https://perma.cc/G66N-HHH9.

232. Dennis Bednarz, *Amnesty International Rates Microsoft's Skype Among Worst in Privacy*, WINBETA (Oct. 23, 2016), https://perma.cc/4QQ8-WBGJ.

233. Pai dissent.

234. "Because the *Order* wants to treat ISPs differently from edge providers, it asserts that the latter only sees a "slice" of consumers' online data. This is not data-driven decision-making, but corporate favoritism." Pai Dissenting Statement at 2.

ISPs and ESPs have access to the same data about a consumer's Internet usage, why should the federal government give one company "greater leeway" to use it than the other?[235] Additionally, it does not make sense to require BIAS providers to follow more stringent rules because there are less BIAS providers than there are ESPs because consumers use multiple BIAS providers on a regular basis just like they use multiple ESPs on a regular basis. A customer may use different BIAS providers when she accesses the Internet on different devices on different Wi-Fi hotspots in different locations, such as home, work, or school.

The uneven regulations are especially unfair because for Internet businesses, access to consumer information creates a significant advantage. Not only does the FCC's argument fail to consider that ESPs have a significant interest in increasing the amount of data they collect on an individual, but the FCC also ignores the major and growing limitations on each ISP's visibility into consumer data, such as encryption of most web traffic and the tendency of consumers to switch continuously among different ISPs as they carry their devices from one network to the next.[236] One of the loudest critics of the FCC's position that ISP's should be punished for the comprehensive access they allegedly have to consumer's browsing history, is Peter Swire.[237] Swire was the Chief Counselor for Privacy, in the U.S. Office of Management and Budget under President Bill Clinton, and was Special Assistant to the President for Economic Policy under President Barack Obama.[238]

C. The FCC's Privacy Order is Not Helpful to Consumers

Prior to the FCC's entry into the online privacy enforcement space, the federal government, led by the FTC, has addressed online privacy by carefully balancing the costs of undue regulation against the need to protect consumers from a genuine privacy harm. The FTC's regime is a long-established flexible one that is effective and supported in large part by industry self-governance along with the FTC's statutory prohibitions against unfair or deceptive trade practices.[239] The FTC's system is beneficial to customers because, as was said in a 2012 White House Report, its approach relies on "multi-stakeholder processes to produce enforceable codes of conduct" that market participants

---

235. Ajit Pai, Chairman, FCC & Maureen Ohlhausen, Acting Chairman, FTC, *No, Republicans Didn't Just Strip Away Your Internet Privacy Rights*, Wash. Post (Apr. 4, 2017), https://perma.cc/TLM4-KZMK.

236. The FCC claims that even when web traffic is encrypted, an ISP can "infer" consumer information from unencrypted data such as top-level URLs and amount of data usage, but numerous industry leaders. *Compare Privacy Order* at para. 29, 186 *with* Swire Working Paper; CenturyLink Comments 5-12; Verizon Comments 17-24; AT&T Comments 13-30; CTIA Comments 114; T-Mobile Comments 5-7; Comcast Comments 26-29.

237. Swire Working Paper at 24-25.

238. *Id.*

239. *See* 15 U.S.C. § 45(b), (n) (2012)*; see also* Consumer Data Privacy in Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, J. of Privacy and Confidentiality 96, 98 (2012), http://repository.cmu.edu/cgi/viewcontent.cgi?article=1096&context=jpc.

can voluntarily incorporate into their privacy policies and thereby make subject to FTC enforcement.[240] However, if a business fails to adopt an industry standard policy as appropriate for their respective business, the FTC will judge any potential data breaches using a case-by-case standard.[241]

The FCC's increased regulations will have a negative impact on consumers because most consumers are not opposed to sharing information with Internet business in exchange for free or discounted services.[242] Former Obama FTC Chairman Jon Leibowitz disagreed with the FCC's proposal to prohibit ISPs from offering discounted services in exchange for customers opting-in to grant data collection and use.[243] Leibowitz believed the rules' prohibition of something that consumers don't find problematic will stifle the development of free online services, and other low cost resources, due to increased transactional costs.[244] Leibowitz suggested that instead the FCC could require a notice and choice regime, where, as "long as ISPs provide sufficient notice, users could have the choice of putting a value on their personal data."[245] This framework, according to Leibowitz, is consistent with the FTC's 2012 Privacy Report.[246] Furthermore, to the extent that a consumer is uncomfortable with providing data to Internet companies in exchange for potential benefits like targeted advertisements, many ESPs voluntarily allow consumers to opt-out of sharing such content.[247] Additionally, the FTC has taken enforcement actions against companies who did not act reasonably and consistent with industry best practices, given their particular circumstances,

---

240. WHITE HOUSE PRIVACY FRAMEWORK at 24 ("The United States relies primarily upon the FTC's case-by-case enforcement of general prohibitions on unfair or deceptive acts and practices. This approach helps develop evolving standards for handling personal data in the private sector.").

241. "The FTC's case-by-case application of these general principles has major advantages over a prescriptive rulemaking approach. The FTC's approach minimizes the regulator's knowledge problem, fosters incrementalism, and focuses limited resources on addressing consumer harm." *See* Maureen K. Ohlhausen, *The FCC's Knowledge Problem: How to Protect Consumers Online*, 67 FED. COMM. L.J. 203 (2015), https://perma.cc/Z9XM-U2MC.

242. "Indeed, one study found that, on average, Americans assigned a value of almost $1,200 per year to the package of free, ad-supported services and content currently available to them[.]" Thomas W. Hazlett & Joshua D. Wright, The Law and Economics of Network.

Neutrality, 45 IND. L. REV. 767, 770 (2012) (internal quotation marks omitted). In addition, "[m]ore than 85 percent of respondents said they preferred [that] ad-supported Internet model instead of paying for online content." *Zogby Poll: Americans Say Free, Ad-Supported Online Services Worth $1,200/Year; 85% Prefer Ad-Supported Internet to Paid*, DIGITAL ADVERTISING ALLIANCE (May 11, 2016), https://perma.cc/UJ7D-7MZ5.

243. John Eggerton, Former FTC Chair Has Issues with FCC's Opt-in CPNI Regime, Multichannel (Oct. 22, 2017, 5:48 PM EST) http://www.multichannel.com/news/fcc/former-ftc-chair-has-issues-fccs-opt-cpni-regime/404836.

244. *Id.*

245. *Id.*

246. *Id*.

247. The Network Advertising Initiative ("NAI") is the leading non-profit, self-regulatory body governing Internet advertising technology providers consisting of nearly 100 businesses as official members. The NAI's Code of Conduct provides that Internet companies should provide "a link to an Opt-Out Mechanism for Internet-Based Advertising." NAI Code of Conduct, NAI 6-7, https://perma.cc/PH3A-EJ8H (last accessed Apr. 11, 2017).

by not providing an opt-out mechanism.[248] However, Internet consumers are less likely to opt-in to sharing information when given the choice to do so.[249] Research conducted by *Wright Economic Analysis* found that "most consumers take the path of least resistance and click 'no' when presented with opt-in notices"; however, they do so not because they object to the use of their information, but because they don't want to take the time to understand the privacy notice.[250] There is also a benefit from the consumers' perspective to consenting to the use and/or sharing of their information because opting in enables a consumer to experience a more personalized Internet browsing experience, including access to discounts and other information that is consistent with her browsing history. [251]

Conversely, an opt-out method is preferable to an opt-in method because those who care greatly about their non-sensitive data can invest the time to understand the privacy options available to them and make an informed choice.[252] ESPs are currently not *per se* required by the FTC to offer an opt-out mechanism, unless otherwise required by law.[253] To accommodate the range of customer preferences concerning privacy, the FTC should require ESPs to make an opt-out mechanism available to consumers. Opt-out mechanisms allow those who care deeply about having enhanced privacy to choose how their data will be protected, while also not slowing down the transaction process or annoying what may be the majority of an ESP's consumers who do not want enhanced privacy.[254] Under the FCC's Privacy Order, those who are not concerned with the collection of their non-sensitive data will be bombarded with continuous opt-in messages.[255]

The Privacy Order's position is that distinguishing between "sensitive and non-sensitive categories [of data] is a fundamentally fraught exercise" that is not helpful to consumers.[256] The Privacy Order appears to administer regulations that do not distinguish between sensitive and non-sensitive information because doing so would be too difficult when, in actuality, ESPs distinguish between sensitive and non-sensitive data routinely. For instance,

---

248. ScanScout, Inc., C-4344 (Dec. 14, 2011) (consent order), https://perma.cc/8T2S-X7SC (requiring company to improve disclosure of its data collection practices and offer consumers a user-friendly opt out mechanism).

249. *Consumers Want Privacy, but Don't Take Advantage of Opt-Out Techs.*, HELP NET SECURITY (Feb. 26, 2014), https://perma.cc/RA7S-5SAM ("A majority of consumers worry about how marketers use their personal data, but 79 percent are more likely to provide personal information to what they consider a 'trusted brand,'… [W]hile consumers are not comfortable with being 'tracked' in a physical store, they tend to not read brands' privacy policies or take measures to opt-out of web tracking practices.").

250. Thomas W. Hazlett & Joshua D. Wright, *The Law and Economics of Network Neutrality*, 45 IND. L. REV. 767, 770 (2012).

251. See Lee Rainie & Maeve Duggan, Privacy and Information Sharing, PEW RESEARCH CENTER (Dec. 2015), https://perma.cc/9VDE-5XKF.

252. Privacy NPRM at 2.

253. See FTC Report at 16.

254. See Privacy NPRM at 2.

255. *Privacy Order* at para. 186-87 (Regardless of whether a user objects of her web browsing history from being used or shared, under the *Privacy Order* she must reply to opt-in messages provided by ISPs pursuant to the *Privacy Order).*

256. *Id.* at para. 187.

Google explains that, "[w]hen showing you personal ads, we will not associate an identifier from cookies or similar technologies with sensitive categories, such as those based on race, religion, sexual orientation, or health."[257] Online providers, like Google, rely on guidelines issued by industry self-regulatory organizations such as the Network Advertising Initiative for insight into which categories should remain "off-limits."

The FCC fails to properly establish that a harm is created if ISPs have access to non-sensitive data and, until the FCC is able to articulate such a harm, it is unfair to impose increased burdens on Internet businesses. Also, the FCC's Privacy Order is unnecessary because, as numerous "commenters pointed out, to the extent that web browsing and application usage data concerns sensitive information," like "health or financial records, it is already covered by the other categories" of the FTC Act.[258]

D. The FCC's Privacy Order is Significantly Costly to Businesses and Consumers

The Privacy Order responds to a perceived threat to privacy presented by BIAS with the argument that it is better to be over-inclusive with respect to what constitutes sensitive or non-sensitive data.[259] This cavalier implementation of regulation without regard for transactional costs is inappropriate. Moreover, until the FCC can demonstrate that consumers have experienced a harm that would have otherwise been avoided but for the FTC's inadequate framework, the FCC's Privacy Order is unnecessary.

Commissioner O'Rielly's dissenting statement to the Open Internet Order cautions that the reclassification of broadband will likely lead to the FCC regulating edge providers and applications.[260] O'Rielly maintains that "The Commission is intentionally setting itself on a collision course with the FTC's definition to up the burdens on edge providers and all technology companies, either here or at the FTC."[261]

Because consumer data is so helpful for industry, innovation, and competition, BIAS will find a way to obtain Internet users' data despite the FCC's ruling. Therefore, what the FCC's Privacy Order has done is create an extra step for a certain segment of industry. Instead of being able to easily access consumer's data, including their browsing activity, BIAS will need to "purchase and use the information they need from other Internet companies, including edge providers, because these companies" are covered by the FTC's

---

257. Google, *About Google Ads*, https://perma.cc/HH97-JMRP (last accessed Apr. 11, 2017); *see also* Letter from James J.R. Talbot, AT&T, to Marlene Dortch, FCC, 16-106, at 3 (Oct. 17, 2016).

258. *Privacy Order* at 215; Comment of Comcast at 43, *Privacy Order*; The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Modernization Act of 1999, is a federal law enacted to control the ways that financial institutions deal with the private information of individuals. *Gramm-Leach-Biley Act*, FTC, https://perma.cc/4XYJ-5FUK (last accessed on Apr. 11, 2017); The Health Insurance Portability and Accountability Act of 1996 (HIPAA), HHS, https://perma.cc/Z4YG-VS49 (last visited Apr. 11, 2017).

259. *Compare Privacy Order* at para. 9 *with* FTC Report at vii-viii; FTC REPORT at 15.

260. https://apps.fcc.gov/edocs_public/attachmatch/DOC-341937A6.pdf.

261. O'Rielly Dissenting Statement at 5-6.

rules, and "will continue to operate under the FTC's opt-out regime".[262] The FCC's Privacy Order limits BIAS providers "from using sensitive customer proprietary information without opt-in consent, but customer proprietary information is limited to information that the provider acquires in connection with its provision of telecommunications service."[263] Thus, data BIAS "obtain from an edge provider does not meet the definition," and is therefore permissible.[264] This is also another example of how the contradictory policies of the FCC and the FTC give ESPs an advantage over BIAS providers, as ESPs can provide substantial valuable content to interested BIAS providers that are unable to do so on their own due to FCC limitations.

Therefore, since non-sensitive consumer data is so valuable to BIAS providers, it is highly likely that BIAS providers will take the additional steps despite the Privacy Order to lawfully obtain consumer's non-sensitive information. The Privacy Order does not prohibit BIAS providers from purchasing consumer data lawfully collected from ESPs under the FTC. This is because when a user does not consent to ISP data use or sharing, the consumer's choice only applies to her data within the context of her relationship with the ISP and not the various ESPs she visits by way of the ISP. Thus, the Privacy Order has simply created needless extra transactional costs. These costs will be transferred to customers, making the service BIAS offer more expensive. The Privacy Order also creates a competitive edge for ESPs that would be in the position to sell data lawfully collected from its consumers to BIAS. Again, these increased hassles and transactional costs are unnecessary because the behavior the regulations are designed to prohibit is arguably not harmful to industry nor consumers.

E. Appropriate Changes to Existing Privacy Regulation Frameworks

The government's purpose with respect to Internet privacy is to ensure that customer's privacy is reasonably protected and that businesses clearly understand their duties to customers. In the spirit of simplifying Internet privacy laws, it is sensible for one agency to have complete jurisdiction over ISPs and ESPs. Now that the Privacy Order is reversed, Congress should pass legislation to limit the FCC's Internet privacy authority. The FCC's party-line vote in 2015 to remove ISPs from the FTC's jurisdiction was a mistake, and limiting the FCC's authority to enact Internet privacy rules and regulations will validate the FTC's role as a unilateral enforcer going forward. Congress should also pass legislation that preempts state laws on Internet data security. There are numerous conflicting state laws on Internet privacy matters, including but not limited to: children's online privacy, e-reader privacy, and privacy policies for websites and online services, privacy of PI held by ISPs,

262. *Privacy Order* at 216.

263. *Privacy Order* at 216-17; *Privacy Order*, *supra* note 15, at App. A § 64.2002(f).

264. *Privacy Order* at 216-17Even if the Commission "fixed" the definition, it would still be precluded by the statute from placing restrictions on a broadband provider's purchase or use of third-party data. *See, e.g.,* Comments of Comcast, *Privacy Order, supra note 15, at 75-76.*

and false and misleading statements in website privacy policies.[265] Federal preemption of state privacy laws will eliminate ambiguity concerning businesses' duties to consumers with respect to particular states. Differences between the HIPAA privacy rule and state physician-patient privilege laws have created substantial confusion in federal question cases.[266] This type of confusion will likely result from the duplicative and contradictory Internet privacy policies discussed in this Note.

On May 18, 2017, Republican Congresswoman Marsha Blackburn of Tennessee introduced the Balancing the Rights of Web Surfers Equally and Responsibly Act (BROWSER Act).[267] The bill would require ISPs and ESPs to "clearly and conspicuously" notify users of their privacy policies, and give users opt-in or opt-out approval rights with the respect to the "use of, disclosure of, and access to user information collected by such providers based on the level of sensitivity of such information, and for other purposes."[268] While the BROWSER Act would make the FTC the sole Internet privacy regulator, it would reinstate the FCC's higher bar for obtaining consumer consent to use certain data.[269] Moreover, the BROWSER Act would essentially have the FTC use the FCC's approach to consumer consent in the Privacy Order, and it would extend the rules beyond ISPs to also include ESPs.[270]

The BROWSER Act is unlikely to garner support in the Senate, and consequently unlikely to become law.[271] Predictably, numerous ESPs and their advocates have criticized Rep. Blackburn's bill because it would subject ESPs to a higher bar with respect to consumer privacy.[272] Additionally, the bill would eliminate the regulatory advantage ESPs had under the Privacy Order compared to their ISP competitors.[273] Since its introduction, few of Rep. Blackburn's conservative colleagues have voiced support of the bill. Significantly, the BROWSER Act is also very similar to the Privacy Order which was widely disliked by conservatives.[274] The BROWSER Act,

---

265. *State Laws Related to Internet Privacy*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 5, 2016), https://perma.cc/X53G-JADT/.

266. Jenna Phipps, *State of Confusion: The HIPAA Privacy Rule and State Physician-Patient Privilege Laws in Federal Question Cases*, 12 SUFFOLK J.TRIAL & APP. ADVOC. 159, 160 (2007).

267. H.R. 2520 115th Cong. (2017); Rep. Blackburn is Chairwoman of the House of Representatives Committee on Energy and Commerce Subcommittee on Communications and Technology.

268. H.R. 2520 115th Cong. (2017).

269. *Id.*

270. *Id.*

271. James Cooper, *The BROWSER Act: A Worthy Goal, But There's an Easier Fix to the Net Neutrality Privacy Mess*, FORBES (May 26, 2017, 5:06 PM), https://perma.cc/AFD3-R2M3.

272. Jenna Ebersole, GOP Plan Revives, Expands Part of Nixed FCC Privacy Rules, LAW 360 (June 1, 2017, 8:45 PM), https://perma.cc/V984-C8C8.

273. *Compare Privacy Order*, *with* H.R. 2520, 115th Cong. (2017).

274. H.R. 2520, 115th Cong. (2017) (Sensitive information includes not only information pertaining to children or social security numbers, but also web browsing history and app usage data, content that industry stakeholders and conservative policymakers have argued is overly broad).

ironically, would instate a very similar approach to Internet privacy as the Privacy Order except the BROWSER Act would have the FTC as the only cop on the beat and would give the FTC authority over both ESPs and ISPs.[275] Meanwhile, AT&T has praised the bill; however, AT&T is an ISP which would benefit from the regulatory crackdown on its ESP competitors that the bill would require.[276]

While there is value in leveling the playing field and applying a tech-neutral approach that does not preference ESPs nor ISPs, the opt-in and opt-out framework Blackburn supports is inappropriate. The bill and its burdensome opt-in and opt-out requirements has the potential to stifle innovation and also drastically decrease the free services available to consumers. Because the bill would require customers to opt-in to the sharing of a broad definition of sensitive information and most consumers are inclined to maintain default settings on their devices rather than opting-in due to a desire to minimize decision-making and increase the speed of their Internet use experience, the BROWSER Act would likely dramatically reduce the amount of data collected by ESPs.[277]

If ESPs collect less data from users, Internet consumers will see less relevant ads, and ESPs will earn considerably less revenue.[278] Furthermore, if ESPs cannot make enough money through advertisements, then they will need to start charging users for more services or go out of business.[279] Thus, the BROWSER Act's requirements would make the current business model of ESPs unsustainable and would push ESPs toward a pay model, ultimately harming consumers who cannot afford to pay for content and apps.[280] The BROWSER Act would be also harm industry and consumers because it would decrease competition and product quality.[281] Internet advertisements, especially of the targeted variety, create easy entry for startups and analytics performed on data collected from consumers help improve apps and personalize content.[282]

Chairwoman Blackburn's legislation also operates on the false premise that consumers would like to give up the free content and mobile apps they currently receive in exchange for enhanced privacy protections, despite

275. H.R. 2520, 115th Cong. (2017).

276. Jenna Ebersole, *GOP Plan Revives, Expands Part of Nixed FCC Privacy Rules*, LAW 360 (June 1, 2017, 8:45 PM), https://perma.cc/V984-C8C8.

277. James Cooper, *The BROWSER Act: A Worthy Goal, But There's an Easier Fi x to the Net Neutrality Privacy Mess*, FORBES (May 26, 2017, 5:06 PM), https://perma.cc/AFD3-R2M3 ("Today, almost no one reads privacy policies, and the BROWSER Act won't change that. It will dramatically reduce the amount of data collected—not because consumers will carefully consider the pros and cons of data sharing and decide to withhold consent, but rather because its not worth their time to make a decision.").

278. James Cooper, *The BROWSER Act: A Worthy Goal, But There's an Easier Fix to the Net Neutrality Privacy Mess*, FORBES (May 26, 2017, 5:06 PM).

279. *Id.*

280. *Id.*

281. *Id.*

282. *Id.*

numerous recent studies indicating otherwise.[283] For example, a recent George Mason University Antonin Scalia Law School working paper analyzed whether consumer autonomy is impacted by an increase in online surveillance by a commercial entity.[284] The study analyzed consumers' Internet browsing history and privacy choices as they relate to Google's privacy policies.[285]

Beginning in March 2012, Google combined user information across platforms, which meant that search queries would "be matched with YouTube views, Gmail or Maps activity, or Android use."[286] Google's new cross platform data collection policy prompted speculation and outcry from privacy advocates; however, direct harms caused by Google's actions are "unobservable."[287] Reduced anonymity may have deterred more privacy sensitive consumers from conducting searches on sensitive or potentially embarrassing topics on Google sites, but the overall effect was negligible and did not qualify as a direct harm for Google nor the majority of its users.[288]

A recent Pew Research Center survey also found that only about a quarter of adults believe their Internet browsing history is "very sensitive."[289] Thus, until objective evidence emerges that consumers want enhanced privacy instead of free content and mobile apps and increased competition among companies, the BROWSER Act is an inappropriate solution to a perceived but nonexistent harm.[290] While giving the FTC jurisdiction over both ISPs and ESPs is appropriate, Congress should reject the BROWSER Act or any similar proposal that attempts to replace the FTC's opt-out framework with opt-in requirements on the digital economy.

---

283. *See generally*, Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?* 45 J. LEG. STUD. S69 (2016) (when large, census-weighted samples of Americans read excerpts from Facebook's, Yahoo's, and Google's privacy policies, subjects generally stated agreement to either vague or explicit language authorizing companies to collect or use personal information seen though subjects regarded these corporate practices as intrusive); *see generally*, James C. Cooper, *Anonymity, Autonomy, and the Collection of Personal Data: Measuring the Privacy Impact of Google's 2012 Privacy Policy Change* (GEO. MASON U.L. & ECONS. RES. PAPER SERIES, Working Paper 17-06), https://perma.cc/5VT9-N4D8.

284. James C. Cooper, *Anonymity, Autonomy, and the Collection of Personal Data: Measuring the Privacy Impact of Google's 2012 Privacy Policy Change* (GEO. MASON U.L. & ECONS. RES. PAPER SERIES, Working Paper 17-06), https://perma.cc/5VT9-N4D8.

285. *Id.*

286. *Id.* at 3.

287. *Id.*

288. *Id.*

289. *The State of Privacy in Post-Snowden America*, PEW RESEARCH CENTER (Sept. 21, 2016), https://perma.cc/R5HR-Q6KC.

290. *See generally*, Lior Jacob Strahilevitz & Mathew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?* 45 J. LEG. STUD. (forthecoming 2017) (when large, census-weighted samples of Americans read excerpts from Facebook's, Yahoo's, and Google's privacy policies, subjects generally stated agreement to either vague or explicit language authorizing companies to collect or use personal information seen though subjects regarded these corporate practices as intrusive);, James C. Cooper, *Anonymity, Autonomy, and the Collection of Personal Data: Measuring the Privacy Impact of Google's 2012 Privacy Policy Change* (GEO. MASON U.L. & ECONS. RES. PAPER SERIES, Working Paper 17-06), https://perma.cc/5VT9-N4D8; *The State of Privacy in Post-Snowden America*, PEW RESEARCH CENTER (Sept. 21, 2016), https://perma.cc/R5HR-Q6KC.

Although both the current Chairman of the FCC and the Acting Chairman of the FTC support the Privacy Order's reversal and the FTC being the sole Internet privacy enforcer, these positions are not held exclusively by conservatives.[291] During the Obama Administration, the FTC concluded that "any privacy framework should be technology neutral" because "ISPs are just one type of large platform provider" and "operating systems and browsers may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles."[292] The Privacy Order, therefore, represented the FCC's divergence from the views of its Democratic colleagues at the FTC. The Obama FTC publicly expressed its criticism of the Privacy NPRM in a unanimous bipartisan comment, calling the FCC's framework "not optimal."[293] Additionally, Peter Swire, President Clinton's Chief Counselor for Privacy and President Obama's Special Assistant for Economic Policy has been one of the loudest critics of the FCC's Privacy Order.[294]

The argument that ISPs should be treated differently because consumers face a unique lack of choice and competition in the ISP marketplace is also flawed. For instance, according to a 2017 industry analysis, "Google dominates the world of search" with a global market share of 80.5% on desktop computers and 95.9% on mobile devices.[295] Meanwhile, Verizon, the largest BIAS, holds only an estimated 35% of its market.[296]

Federal Internet privacy laws are moving in the right direction, but more needs to be done to protect consumer's privacy, and to inform businesses on what they must do to protect themselves from privacy-related enforcement actions. While the FCC waits for Congressional legislation returning ISPs to the FTC's privacy jurisdiction, the FCC should align its rules with the FTC's approach. However, the FCC should act in accordance with the limitations imposed by the Congressional Review Act and other legal and regulatory provisions which may minimize the amount of privacy-related rules the FCC

---

291. Ajit Pai, Chairman, FCC & Maureen Ohlhausen, Acting Chairman, FTC, Opinion, *No, Republicans Didn't Just Strip Away Your Internet Privacy Rights*, WASH. POST (Apr. 4, 2017), https://perma.cc/TLM4-KZMK.

292. FTC Report at 56.

293. The Federal Trade Commission, Comment, Comment of FTC Staff of the Bureau of Consumer Protection of the Federal Trade Commission at 7-8, *Privacy NPRM*, https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf.

294. *See generally*, Swire Working Paper (discussing the functionality of ISPs therein challenging the fundamental premise of the FCC's privacy NPRM framework); *see also* Ajit Pai, Chairman, FCC & Maureen Ohlhausen, Acting Chairman, FTC, *No, Republicans Didn't Just Strip Away Your Internet Privacy Rights*, WASH. POST.: OPINION (Apr. 4, 2017), https://perma.cc/TLM4-KZMK.

295. Martin Armstrong, *Google, Googler, Googlest*, STATISTA (Mar. 31, 2017), https://perma.cc/4E5G-K7XW.

296. Market Share of Wireless Subscriptions Held by Carriers in the U.S. from 1st Quarter 2011 to 4th Quarter 2016, STATISTA,https://www.statista.com/statistics/199359/market-share-of-wireless-carriers-in-the-us-by-subscriptions/ (ast accessed Apr. 11, 2017).

can impose.[297] Then, once the necessary laws are enacted to preempt state regulations and limit the FCC's role in Internet data security, Congress should create a more clear and appropriate Internet security standard which the FTC will be responsible for enforcing. The updated FTC standards should be a pro-consumer, pro-industry approach considering the potential harms and benefits of data collection to consumers and businesses.

IV. CONCLUSION

Given the FTC's long history in consumer protection, it possesses significant privacy and data security expertise and it would behoove the FCC to consider the FTC's perspective. The Privacy Order places substantial, unjustified costs on businesses and consumers. Additionally, the Privacy Order facilitates superfluous corporate favoritism and does not protect consumers from any proven Internet privacy related harm. Therefore, Congress should take steps to strip the FCC of its authority to regulate online data security, and create a stronger uniform data security policy, which the FTC will be in charge of enforcing.

297. Jenna Ebersole, *FCC Faces Quandary If Obama-Era Privacy Rules Get Boot*, LAW360 (Mar. 24, 2017).

Sovereignty: The Race to Regulate, Putting Consumers First as Communications Technology Emerges

Symposium Authors (Multiple) *

TABLE OF CONTENTS

* This year's theme examines who would be better suited to regulate emerging technology and the related industries. For example, many states have recently passed laws regulating biometrics, driverless vehicles, and data breaches. Is Congress or the federal government better suited for this role? Conversely, should states and the federal government be left out so that the industry could develop its own standards?

Is There Freedom of Contract in the Age of Nationwide Communications Networks?

Justin Clark

When the First Responder Network Authority Board of Directors ("FirstNet") was established in 2012, Congress touted it as a way to encourage greater interconnectivity between multiple first responder agencies and facilitate communications in a time of crisis.[1] FirstNet is an independent authority within the Department of Commerce National Telecommunications and Information Administration responsible for constructing a nationwide public-safety broadband network.[2] In March 2017, FirstNet created a public-private partnership with AT&T to build out, operate, and maintain the Nationwide Public Safety Broadband Network.[3] Apart from issues of resource priority and insufficient network coverage in rural areas,[4] the very process of FirstNet's selection of a nationwide service provider has been criticized by some practitioners.[5] The chief concern with the partnership between FirstNet and AT&T is that the details of the service agreement were largely a mystery, specifically, how gaps in network coverage would be addressed by states and which types of dispute resolution mechanisms would be used between FirstNet and AT&T.[6] Although the governors of all 50 states have now accepted FirstNet's proposed partnership with AT&T,[7] the concerns around the contract negotiation process and the absence of state involvement in vetting, selection, and negotiation of service provider terms loom large

1. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-407, PUBLIC-SAFETY BROADBAND NETWORK: FIRSTNET SHOULD STRENGTHEN INTERNAL CONTROLS AND EVALUATE LESSONS LEARNED 1 (2015).

2. *See* Middle Class Tax Relief and Job Creation Act of 2012, Pub L. No. 112-96, §§ 6201-6202, 6204, 6207, 126 Stat. 156, 206, 208, 215 (2012).

3. The agreement provided that in exchange for AT&T's commitment to spend $40 billion on the project, the company would receive 20MHz of spectrum as well as payments from the government. Danny Crichton, *All 50 states vote yes on AT&T's $40 billion emergency response network FirstNet*, TECHCRUNCH (DEC. 29, 2017), https://techcrunch.com/2017/12/29/all-50-states-vote-yes-on-atts-40-billion-emergency-response-network-firstnet/.

4. *See* Stephen Klein, *Rural Response: The Need for an Effective Rural FirstNet Network*, 69 Fed. Comm. L.J. 53, 55 (2017).

5. *See* Al Catalano, *States Deserve A Complete Picture in Evaluating FirstNet/AT&T Coverage Plans, Beyond Digital Telecom Law Blog*, BEYOND TELECOM L. BLOG (June 29, 2017), https://www.beyondtelecomlawblog.com/states-deserve-complete-picture-evaluating-firstnetatt-coverage-plans/.

6. *Id.*

7. *Id.*

promising to plague future public-private partnerships in the area of spectrum development. These concerns are a further bi-product of the Federal Acquisition Regulation ("FAR"), and whether such a program should be used for other wide-scale communication projects moving forward.[8]

There are compelling arguments for why the decision on constructing a national first responder communications infrastructure should be handled through a framework like FirstNet.[9] However, the unique challenges of bringing together a myriad of law enforcement agencies at the local level, some of which have already developed their own localized system and do not have the opportunity to review the terms of the agreement, appears to create a need for a new procurement and development process.[10] The real culprit in all of this appears to be the strictures of FAR itself, a series of taxing rules governing the negotiation and administration of contracts between executive agencies and private third parties.[11] To open up negotiations and give state and local law enforcement authorities the opportunity to review the terms of a public-private partnership to develop a broad-reaching system, the FirstNet founding board might have considered using alternative means for soliciting bids and negotiating a contract. One such framework used by the Departments of Defense and Homeland Security in some of their fulfillment contracts is the "Other Transaction", an alternative instrument available for research and development efforts with certain agencies where traditional procurement laws and regulations are too burdensome.[12] Using such a regime may provide benefits in transactions involving multiple parties where cost-sharing and advancing dual-use technologies are key concerns.[13]

The creation, development, and administration of FirstNet could serve as a key lesson for other projects involving use and development of the spectrum, particularly as to how service providers are selected and how those providers negotiate contract terms with the numerous parties involved. Most importantly, Congress should consider the concerns of state and local governments and how these governments can be part of the contract negotiation and roll-out process.

---

8. *See* Al Catalano, *A Better Way Forward for FirstNet?*, BEYOND DIGITAL TELECOM L. BLOG (Mar. 8, 2017), https://www.beyondtelecomlawblog.com/better-way-forward-firstnet/.

9. "There are certainly some situations when interoperability is necessary, especially in major metropolitan areas, where first responders from multiple jurisdictions will swarm a dire emergency." *See* Steven Brill, *The $47 Billion Network That's Already Obsolete*, ATLANTIC (Sept. 2016), https://www.theatlantic.com/magazine/archive/2016/09/the-47-billion-network-thats-already-obsolete/492764/ [https://perma.cc/K8H9-2EH8].

10. Al Catalano, *States Deserve A Complete Picture in Evaluating FirstNet/AT&T Coverage Plans, Beyond Digital Telecom Law Blog*, BEYOND TELECOM L. BLOG (June 29, 2017), https://www.beyondtelecomlawblog.com/states-deserve-complete-picture-evaluating-firstnetatt-coverage-plans/.

11. Al Catalano, *A Better Way Forward for FirstNet?*, BEYOND DIGITAL TELECOM L. BLOG (Mar. 8, 2017), https://www.beyondtelecomlawblog.com/better-way-forward-firstnet/.

12. *See* Nancy O. Dix, et al., *Fear and Loathing of Federal Contracting: Are Commercial Companies Really Afraid to Do Business With the Federal Government? Should They Be?*, 33 Pub. Cont. L.J. 5, 23-7 (2003).

13. *Id.* at 26.

The How and Where of Regulating Communication Technology?

Sean Davis Jr.

In today's era, communication technology is emerging as a pillar in American society and economy. From artificial intelligence to social media platforms, tech focused companies are growing in social relevance and market space. For example, Facebook and Google, two of Silicon Valley's titans are expected to take half of the internet advertising revenue worldwide and over sixty percent in the U.S.[1] Further, with the recent rollback of open internet protections, many in congress have made net neutrality a campaign issue,[2] subsequently placing telecomm issues at the forefront of the American conscious. Other issues, such as the repeal of broadband privacy[3] begs a pertinent question: who is best suited to regulate communication technology and relevant innovations? Touching on a myriad of anti-trust and civil rights issues, technology such as social media algorithms or driverless cars creates complex legal issues that are heavily debated.

The answer to these questions although complex, are not far off. First, it is critical that regulatory bodies such as the Federal Communications Commission, the Federal Trade Commission, and the House Subcommittee on Communications and Technology acknowledge that there is a spectrum of communications technology that requires varying degrees of regulation. For example, Silicon Valley Titans such as Facebook and Google have monopolized the online advertising market[4], while subsequently being questioned for their mishandling of extremist content on their platforms[5]. Given their relevance in both American society and economy, placing sensible regulations on Facebook and Google's online advertising power and screening of user content is pertinent. On the other end, communications technology associated with artificial intelligence is in a developing stage, which would easily be stifled by too much regulation. However, there are steps that can be taken to address such tech without stifling innovation. One

1. Reuters, *Why Google and Facebook Prove the Digital Ad Market Is a Duopoly?*, FORTUNE (July 28, 2017), http://fortune.com/2017/07/28/google-facebook-digital-advertising/.

2. Klint Finley, *Why Net Neutrality will be a campaign Issue in 2018*, WIRED (Dec. 21, 2017), https://www.wired.com/story/why-net-neutrality-will-be-a-campaign-issue-in-2018/.

3. Devin Coldewey, *Broadband Privacy Rules (Update: Passed)*, TECHCRUNCH (Mar. 22, 2017), https://techcrunch.com/2017/03/22/senate-debates-legislative-rollback-of-fccs-broadband-privacy-rules/.

4. Reuters, *Why Google and Facebook Prove the Digital Ad Market Is a Duopoly?*, FORTUNE (July 28, 2017), http://fortune.com/2017/07/28/google-facebook-digital-advertising/.

5. Alex Wagner & Tony Romm, *Facebook, Google and Twitter testified before congress again*. RECODE (NOV. 21, 2017), https://www.recode.net/2017/11/1/16588374/live-updates-facebook-google-twitter-testify-senate-congress-russia-president-election.

such example is the Future of Artificial Intelligence Act of 2017. Sponsored by Senator Maria Cantwell, the Act would name the Department of Commerce responsible for creating a committee to provide recommendations on how businesses and government can come together to: (1) create reasonable legislation on artificial intelligence (AI); (2) support developmental AI ventures and protect the rights of consumers as AI continues to grow.[6] Legislation such as this shows forward thinking and recognition that communications technology is a multifaceted market that has the ability to usher the U.S. into a new economic revolution.

6. *Young Introduces bill to promote and understand the Future of Artificial Intelligence Technology.* SENATOR TODD YOUNG (Dec. 12, 2017), https://www.young.senate.gov/newsroom/press-releases/young-introduces-bill-to-promote-and-understand-the-future-of-artificial-intelligence-technology.

The Federal Trade Commission Protects Consumers as Communications Technology Evolves

Morgan Rucker Kennedy [1]

Communications technology has greatly expanded the scope of connectivity in everyday life. Consumers are no longer just connecting to the Internet through a desktop computer or home modem.[2] Instead, consumers are connecting through, among other things, mobile phones, wearables, refrigerators, thermostats, televisions, and vehicles.[3] While these technological innovations have provided revolutionary benefits to the way consumers live and interact with the people and things around them, it also means companies are collecting an immense amount of data from consumers.[4] Fitness trackers can log when you went for a walk, where you walked, your stride length, and your heart rate.[5] Modern vehicles permit you to sync your smart phone to the car's infotainment system, permitting the storage of address book, call, and text message information.[6] The amount of data collected by a potential multitude of actors means it is crucial for consumers to have transparency about companies' data use and collection practices, and confidence that their information will be kept secure.

As the leading privacy and data security agency in the United States, the Federal Trade Commission ("FTC" or "Commission") is uniquely situated to protect consumers as technology evolves. The FTC is a bipartisan independent agency with law enforcement jurisdiction over a broad swath of

1. Ms. Kennedy is an attorney in the FTC's Office of the General Counsel. The views expressed herein are the author's own and do not necessarily represent the views of the Commission or any individual Commissioner.

2. *Share of devices used to access the internet at home, in the United States, from 2010 to 2015*, STATISTA https://www.statista.com/statistics/199055/devices-used-to-access-the-internet-at-home-in-the-united-states/ (last visited Apr. 18, 2018).

3. Krissy Rushing, *5 Benefits of Internet Appliances*, http://www.hgtv.com/remodel/mechanical-systems/5-benefits-of-internet-appliance.s

4. *Connected Devices and Your Privacy*, CONSUMER REPS. (Apr. 30, 2015), https://www.consumerreports.org/cro/magazine/2015/06/connected-devices-and-your-privacy/index.htm.

5. James Stables, *Best fitness tracker guide 2018: The top activity bands you can buy now*, WAREABLE (Apr. 17, 2018), https://www.wareable.com/fitness-trackers/the-best-fitness-tracker.

6. Ronald Montoya, *Car Technology and Privacy: Top 5 Things Your Car Knows About You*, EDMUNDS (Feb. 12, 2013), https://www.edmunds.com/car-technology/car-technology-and-privacy.html.

the American economy.[7] When the FTC was founded over a century ago, Congress could not have imagined the types of technology that are commonplace in modern society. However, the FTC Act, which broadly authorizes the FTC to prevent "unfair methods of competition" and "unfair or deceptive acts or practices,"[8] gives the Commission flexibility to protect consumers as new technologies emerge.

The FTC has brought a substantial number of cases protecting the privacy and security of consumers' information, many of which have involved new or emerging technology.[9] For example, in 2013, the FTC issued a complaint against TRENDnet, Inc. ("TRENDnet"), which sold Internet-connected cameras for monitoring a user's home or business.[10] The FTC alleged that the company advertised its cameras as secure, but engaged in a number of practices that made the cameras' live feeds susceptible to unauthorized access by strangers.[11] In settling the complaint, TRENDnet was required by order to, among other things, establish and maintain a comprehensive security program designed to address security risks that could result in unauthorized access to or use of the company's devices and protect the security, confidentiality, and integrity of information collected, input into, stored on, captured with, accessed, or transmitted through the company's devices.[12] Four years later, the FTC and the Office of the New Jersey Attorney General filed a complaint alleging that VIZIO, Inc. ("VIZIO"), a manufacturer and seller of Internet-connected "smart" televisions, and an affiliated software company installed software on VIZIO televisions to collect second-by-second viewing data on millions of consumers without their

---

7. The Federal Trade Commission Act ("FTC Act") contains some limitations on the FTC's jurisdiction. The FTC Act exempts from the FTC's jurisdiction "common carriers subject to the Acts to regulate commerce," which bars the agency from reaching certain conduct by telecommunications companies. 15 U.S.C. § 45(a)(2). For well over a decade, the Commission, on a bipartisan basis, has advocated that Congress repeal this common carrier exemption. *See, e.g., Prepared Statement of The Fed. Trade Commission Before the Subcomm. on Commerce, Trade, and Consumer Protection of the Comm. on Energy and Commerce* (June 11, 2003), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-reauthorization/030611reauthhr.pdf. [https://perma.cc/8TZ3-TG9S].

8. 15 U.S.C. § 45.

9. *Enforcing Privacy Promises*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited Apr. 18, 2018).

10. Complaint at 2, In the Matter of TRENDnet, Inc., a Corp., No. C-4426 (FTC Sept. 3, 2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/09/130903trendnetcmpt.pdf. [https://perma.cc/SXA8-PLAT].

11. Complaint at 3,6, In the Matter of TRENDnet, Inc., a Corp., No. C-4426 (FTC Sept. 3, 2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/09/130903trendnetcmpt.pdf. [https://perma.cc/SXA8-PLAT].

12. Decision and Order, *In the Matter of TRENDnet, Inc., a Corp.*, No. C-4426 (FTC Jan. 16, 2014), https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf.

knowledge or consent.[13] VIZIO and its affiliate agreed to pay $2.2 million to settle these charges, and the stipulated federal court order requires the companies to disclose and obtain affirmative express consent for their viewing data collection and sharing practices, and prohibits misrepresentations about the privacy, confidentiality, or security of consumer information collected.[14]

To pursue such matters and to police the marketplace effectively, the FTC has to remain informed about new technologies and their effects on consumers. To do so, the Agency routinely hosts workshops to engage with industry, academics, government agencies, and consumer advocates.[15] Recent workshops have examined the connected car ecosystem[16] and injury to consumers resulting from the misuse of personal information in products and services.[17] The FTC also encompasses the Office of Technology Research and Investigation ("OTech") to facilitate technical expertise internally.[18] OTech technologists conduct independent studies and assist FTC investigators and attorneys by providing technical expertise, investigative assistance, and training.[19] Finally, the FTC hears directly from the public — consumers file complaints directly with the Agency.[20] Although the FTC does not adjudicate individual complaints, it uses them to understand what practices cause significant harm to consumers and focus its investigations.[21]

For all of the above reasons, the FTC has the expertise and capability to take targeted law enforcement action to address unlawful conduct without impeding innovation.

---

13. Complaint for Permanent Injunction and Other Equitable and Monetary Relief, *FTC v. VIZIO, Inc.*, No. 17-cv-00758 (D. N.J. Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf.

14. Stipulated Order for Permanent Injunction and Monetary Judgment, *FTC v. VIZIO, Inc.*, No. 17-cv-00758 (D. N.J. Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf.

15. *All Events*, FTC, https://www.ftc.gov/news-events/events-calendar/all (last visited Apr. 18, 2018).

16. *Connected Cars Workshop, Staff Perspective*, FTC (Jan. 2018), https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf?utm_source=govdelivery.

17. *Informational Injury Workshop*, FTC, https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop (last visited Jan. 16, 2018).

18. *Office of Technology Research and Investigation*, FTC, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/office-technology-research-investigation (last visited Apr. 18, 2018).

19. *Office of Technology Research and Investigation*, FTC, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/office-technology-research-investigation (last visited Apr. 18, 2018).

20. *Filing A Complaint*, FTC, https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/filing-complaint (last visited Apr. 18, 2018).

21. *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FTC, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last visited Apr. 18, 2018).

Federal, State, and Self-Regulation Strategies for Data Collection & Use

Grant Nelson [1]

> "It is the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet, . . . unfettered by Federal or State regulation; . . . ."[2]

Regulation of the collection and use of online information requires balancing the interests of encouraging technological innovation, maintaining a free and open internet, and protecting consumers' online privacy. Federal legislation, state action, and self-regulation all offer benefits and risks, and different contexts require different approaches. Ultimately, given the fast pace of technology advancement in the online information industry, a flexible approach like self-regulation may prove the most effective.

I. FEDERAL LEGISLATION

Federal legislation offers consistency across states, but not across countries, nor does it offer state-level decision-making and experimentation. Federal legislation consistency may come at the expense of the flexibility that rapidly changing technology may require. The federal legislative process takes time—so much time, in fact, that by the time a law is enacted —it may already be outdated, or is quickly made irrelevant or ambiguous by advances in technology. For example, the Computer Fraud and Abuse Act,[3] enacted in 1986 (years before home internet use—much less mobile internet use), has been called obsolete due to its dated and over-broad language.[4] Similarly, the 1986 Electronic Communications Privacy Act[5] which regulates the circumstances under which law enforcement may access electronic

1. Counsel, Compliance & Technology for the Network Advertising Initiative (NAI).
2. *See* Communications Decency Act, 47 U.S.C. § 230(b) (2016) (providing the policy reasons for protecting internet platforms and providers from being held liable as a publisher or speaker of information).
3. 18 U.S.C. § 1030 (2016).
4. *See, e.g.*, Tiffany Curtiss, *Computer Fraud and Abuse Act Enforcement: Cruel, Unusual, and Due for Reform*, 91 WASH. L. REV. 1813, 1813 (2016); Tor Ekeland, *How to Reform the Outdated Federal Anti-hacking Law*, CHRISTIAN SCI. MONITOR (Mar. 24, 2017), https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0324/How-to-reform-the-outdated-federal-anti-hacking-law.
5. 18 U.S.C. § 2510 (2016).

communications without a warrant, has been criticized for using standards from "a bygone era" based on outdated technology.[6]

Amending federal statutes to account for new technology is also challenging. The Video Privacy Protection Act of 1989[7] was not amended until 2012, and even its amended form has been described by one court as "an attempt to place a square peg (modern electronic technology) into a round hole (a statute written in 1988)."[8]

Perhaps more important is the argument that legislation often has the effect of stifling innovation, a point made by many in all sectors; not just technology.[9] Regulation drives up operating costs and reduces the incentive for entrepreneurs to enter the market, thus stifling the very innovative spirit responsible for the internet as we know it today.

II. STATE LEGISLATION

State legislation creates a patchwork of regulation across the country, allowing states to "experiment" with the regulation of an industry. However, because internet companies invariably do business in all (or close to all) states, they often elect to abide by the strictest of the state laws, a practice that curtails the "experimentation" theory and often results in the same innovation-stifling effects of federal regulation. However, different states electing to take different positions with respect to technologies may encourage competition among states to attract innovative technologies.

III. INDUSTRY SELF-REGULATION

Unlike state and federal regulations, self-regulatory organizations have the ability to respond to—and even stay ahead of—advances in technology, which is a significant advantage when regulating a constantly evolving industry.[10] Perhaps more importantly, members of such associations are

---

6. Veronique de Rugy, *Federal Agencies Fight for Warrantless Access to Emails*, MERCATUS CENTER, (Aug. 13, 2015), https://www.mercatus.org/expert_commentary/federal-agencies-fight-warrantless-access-emails.

7. 18 U.S.C. § 2710 (2016).

8. Yershov v. Gannett Satellite Information Network, Inc., 104 F. Supp. 3d 135, 140 (D. Mass. 2015).

9. *See, e.g.*, Tim Day, *When It Comes to Tech, It's Regulation vs. Innovation*, U.S. CHAMBER OF COMM.: ABOVE FOLD.; https://www.uschamber.com/series/above-the-fold/when-it-comes-tech-it-s-regulation-vs-innovation (last visited Feb. 12, 2018); Andrea O'Sullivan, *Don't Let Regulators Ruin AI*, MIT TECH. REV. (Oct. 24, 2017) https://www.technologyreview.com/s/609132/dont-let-regulators-ruin-ai/; Henry I. Miller, *Bad Times Ahead for Pharmaceutical Innovation*, FORBES: OPINION (Aug. 4, 2010, 3:17PM), https://www.forbes.com/2010/08/04/fda-regulation-pharmaceuticals-opinions-columnists-henry-i-miller.html#7fb3f1306928.

10. *See generally* Robert W. Cook, *Why do we need self-regulatory organizations? - Cook*, INVESTMENT NEWS (Apr. 2, 2017), http://www.investmentnews.com/article/20170402/FREE/170409997/why-do-we-need-self-regulatory-organizations-cook.

invested in the industry's reputation, meaning their businesses benefit from both the protection of consumer privacy (thereby demonstrating to consumers that they are both professional and trustworthy), and the preservation of a free and innovative internet ecosystem.[11] As such, self-regulatory organizations craft regulations that provide meaningful consumer privacy protections, while also educating consumers and government regulators about responsible industry practices.[12] Self-regulation creates a dynamic regulatory environment in which consumers' privacy is protected, and technological innovation is encouraged.

11. *Id.*
12. *Id.*

Sovereignty Disrupted

Travis LeBlanc [1]

Sovereignty has been disrupted. Emerging technologies have repeatedly broken the molds of regulated industries such as taxicabs, hotels, telephone companies, and cable providers. At the same time as new technologies disrupt regulated industries, these same technologies are also disrupting the very regulatory processes that we have traditionally relied upon to protect the public good. The fundamental problem is the velocity of innovation has outpaced the inertia of the regulatory process. Sovereignty is at a crossroads—our system of government must quickly adapt to this new technological landscape or it will be forced to concede the "race to regulate," leaving the technology as the only contestant standing.

I. THE PROBLEM

Emerging technologies, including communications technologies, are evolving at exponential speeds and are permeating every facet of life. By 2020, it is expected that there will be between 30 and 50 billion devices connected to the internet, or about 7 for each person on the planet. Unlike the recent past where a phone was a phone, a camera was a camera, and refrigerator was a refrigerator, a phone is now a camera, a refrigerator is a television, and the coolest appliance in the house streams, listens, and talks with you. But these technologies are not simply limited to new platforms for "chatting" or "talking"; even the simplest devices that used to be "offline" products are now becoming "smart," technology-based communicators. These technologies include a long list of devices radically changing society—from smartphones to autonomous vehicles to new-fangled medical devices—whose communicative elements are essential to their nature and desirability. And many more innovations are coming down the road that we cannot yet imagine. No aspect of life or regulation will remain untouched.

Governments thus far have been unable to keep up with these technological advances, and there is no prospect of our sovereigns catching up to these rapid changes anytime soon. Our sovereigns have been unable to regulate emerging technologies effectively and timely-in part due to the velocity of innovation, the cumbersome legislative and regulatory structure

1. Travis LeBlanc is an Affiliate with the Berkman Klein Center for Internet and Society at Harvard University, an Affiliated Scholar with the Institute for Innovation Law at UC Hastings College of the Law, and a Partner at Boies Schiller Flexner LLP. Previously, Mr. LeBlanc served as the Chief of Enforcement at the Federal Communications Commission. This article has been written in Mr. LeBlanc's personal capacity. The opinions expressed in this article are his own and do not reflect the views of the Federal Communications Commission, any commissioner thereof, the federal government, or Boies Schiller Flexner.

developed in and for an offline world, the diffusion of authority across multiple government actors without a final decision maker, the lack of technological sophistication among policymakers across governments, and the comprehensiveness of the challenge in a world where everything is connected to the internet. And then there is partisan gridlock.

To be fair, states have been far better than the federal government at keeping up with technological change—they are smaller, more nimble, less gridlocked—but even they have been unable to keep up with the growth of emerging technologies. Indeed, many of these new technologies are solving problems that we traditionally relied upon the government to handle. They are providing first-class learning to students in resource-strapped schools. Ride sharing companies are solving public transportation gaps. Doctors are providing care to patients in remote areas of the country. On the media side, consumers are able to view media content anytime anywhere and to create their own high-quality content, distribute it across multiple platforms, and generate considerable revenue. As we embrace these innovations, we accept that technology can solve inefficiencies; we become more reliant upon these technologies; and we become more willing to place our trust and confidence in them as decision-making authorities.

II. THE FUTURE IS HERE

Technological innovations are not only solving public policy problems, they are also showing that they can perform existing government tasks more quickly, effectively, and at less cost-whether that is identifying perpetrators of hate crimes, evaluating which foreigners should be admitted to the country, or determining where police resources should be targeted. It is indeed beyond apparent that emerging technologies are supplanting the traditional functions of the sovereign. The advent of email largely obviated the need for a government-operated postal service. Cryptocurrencies such as bitcoin are vying to replace government-backed currencies. And elections are being influenced by social media. Fundamentally, the government is *losing* to technologists, data scientists, and machine algorithms in the race to regulate. We do not have a defined legal regime for cloud services; there are almost no laws that govern the internet of things; and digital rights are essentially non-existent or minimally enforceable. In this environment, consumers are necessarily dependent upon technologists, data scientists, and machine algorithms to protect their welfare and safety.

Yet, unlike our sovereigns, emerging technologies are not required to honor constitutional freedoms of speech, religion, and the press. Nor must they provide any kind of due process before terminating a user account, ceasing to support legacy software, or taking down user content. Nor are they bound to protect the rights to life, liberty, and the pursuit of happiness. I am by no means suggesting that technologists, data scientists, and algorithms are intending to trample on these cherished freedoms, but a lack of timely regulatory action is necessarily transforming technologists, data scientists, and algorithms into policymakers. If government does not act, we will be left

to the regulatory authority of technologists, data scientists, and algorithms—a worrisome prospect no matter how altruistic such companies may be and no matter how much these companies promise to police themselves.

Accordingly, faced with both competition from ubiquitous technology and the associated threats carried by those technologies, it is imperative we reboot our notion of sovereignty. The fundamental impact of emerging technologies on government is as tectonic as it has been in all industries. The business of regulating is no different. Just as taxi companies are reinventing themselves in the face of competition from ride sharing companies, so must the government reconsider how it regulates in the 21st Century.

The current processes of legislating and regulating are too slow and cumbersome, the legacy of a bygone offline era. As our Founding Fathers did in 1776, we must reexamine sovereignty, this time for digital life in the 21st Century. We need to hack our democracy and the regulatory process with the goal of designing a regulatory structure for a digital world. We must devise ways for governments of all levels—from state and local governments to national and international bodies—to quickly promulgate rules that are flexible and adaptable. We need our sovereigns to have the ability to regulate the problems of tomorrow rather than relegating themselves to solving the problems of yesteryear. We need our sovereigns to address a world that is constantly connected and mobile, where information and currency are not bounded by geography, and where cyberattacks may become the exception rather than rule. These are problems that the Founders of our country, even with their clairvoyant wisdom, could not have even begun to imagine. To properly address them, iterative case-by-case reforms are not enough or effective. The challenges that emerging technologies pose to sovereignty are fundamental. We must now revisit the structure of government for life in the 21st Century, the connected world we now inhabit. Sovereignty has been disrupted by emerging technologies. We cannot afford to wait. The future is already here, and it eagerly awaits governmental resolution to protect our fundamental rights.