EDITOR'S NOTE

Welcome to the third issue of Volume 69 of the Federal Communications Law Journal ("FCLJ"), the official journal of the Federal Communications Bar Association ("FCBA"). Over the summer, the FCLJ welcomed 50 new talented individuals to our membership. Our team has worked tirelessly to create a satiating Annual Review issue that encompasses a range of topics, including data security regulation, media ownership rules, Open Data Initiatives ("ODIs"), and international cybersecurity regimes.

In the first Note, Alex Bossone addresses the lack of federal consumer data security regulation in an age where consumers suffer from identity thefts and cyber-attacks. Mr. Bossone suggests an augmentation of the FTC's existing data security powers and an emulation of the FCC Enforcement Bureau's approach to mandate an effective legal framework. In the second Note, Bryan Schatz explores the shortcomings of the current media ownership rules. Mr. Schatz proposes solutions that can free up the Quadrennial Review and help the FCC promulgate and enforce new media ownership rules. In the third Note, Monica Savukinas examines how the Obama administration encouraged federal agencies to use ODIs for innovation. Ms. Savukinas suggests that the FCC use ODIs through prize contests, hackathons, and open dialogue with developers, as part of its innovation policy.

This issue also features an interesting article on international cybersecurity, penned by Zahra Dsouza, who is currently a Law Clerk at Kohn Swift & Graf P.C. and an LL.M. graduate of Temple University Law School. Noting the growing problem of malicious cybersecurity incidents, Ms. Dsouza assesses the futility of Cybersecurity Incident Response Teams ("CSIRTs") as a response to such incidents, as they have been without a clear mandate. Ms. Dsouza proposes structural recommendations that may enable CSIRTs to respond to cybersecurity incidents at a global level. Finally, the FCLJ proudly presents a series of case briefs to provide an overview of the significant legal movements in the communications law field in the past year.

The editorial board is grateful for the support of the FCBA and The George Washington University Law School this year, as we have enjoyed the addition of new FCLJ Committee members, adjunct professors, and faculty advisor. For this issue, the FCLJ sends a special thanks to the lawyers who shared their insights at the FCC's Year-in-Review CLE Seminar, as the event has provided the editorial board with guidance on structuring the case briefs.

We welcome your feedback or questions to fclj@law.gwu.edu, and 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 69 FED. COMM. L.J. ___ (2018).

FEDERAL COMMUNICATIONS LAW JOURNAL

GW LAW

VOLUME 69 ISSUE 3

JANUARY 2018

FCBA FEDERAL COMMUNICATIONS BAR ASSOCIATION

ARTICLE

Are Cyber Security Incident Response Teams (CSIRTs) Redundant or Can They Be Relevant to International Cyber Security?

The magnitude of cyber security incidents is growing due to the sophistication of tools and techniques employed by adversaries and increased interdependency. International cooperation is vital to prevent and respond to trans-border cyberattacks. A key response to cybersecurity incidents has been Cybersecurity Incident Response Teams ("CSIRTs"). However, CSIRTs face legal and practical challenges to their continuing existence. The role and relationships of CSIRTs within the state and with international actors is unclear, which manifests in a trust deficit and a lack of cooperation in incident response.

This paper examines the constitutive statutes of the International Red Cross and Red Crescent Movement ("Movement") and proposes that the role of actors in the cybersecurity landscape and CSIRTs be re-conceptualized by adopting functions of components of the Movement and features of the relationships between them. This paper provides background on the cyber security incident landscape and the global CSIRT network, discusses the legal and practical obstacles that limit information sharing, and explores emergency response mechanisms to humanitarian crises. The paper suggests that: (1) Forum for Incident Response and Security Teams ("FIRST") serve as an umbrella organization responsible for providing information, support, and coordination between CSIRTs; (2) that States support National CSIRTs ("NCSIRTs") by enacting legislation that clearly defines the mandate of CSIRTs and allocate resources for CSIRTs; and (3) that NCSIRTs assist victims and contribute to the community by assisting in the development of other CSIRTs. This will enable CSIRTs to coordinate the response to cyber security incidents at a global level.

NOTES

The Battle Against Breaches: A Call for Modernizing Federal Consumer Data Security Regulation

In a global economy where consumer data is an increasingly valuable asset, businesses are facing an ever-increasing threat of data breaches. While countries in the European Union all have established independent Data Protection Agencies (DPAs) to regulate the data security practices of companies, the United States has opted to allow the Federal Trade Commission (FTC) to function as its own "de-facto" DPA pursuant to its preexisting consumer protection authority.

The FTC has developed substantial expertise in the area of data security, but it remains constrained to a vague "reasonableness" standard when determining whether businesses that suffer data breaches have undertaken adequate security measures. This standard has faced resistance from companies that argue the FTC has not provided clear requirements for what security practices are required to avoid penalization.

The Federal Communications Commission (FCC), which regulates data security practices in the telecommunications industry, proposed a promising alternative enforcement model that imposed more specific standards on the target company in a recent data breach action. Not only did the FCC seek to eliminate the cause of that breach, but it also imposed clearly-defined security measures aimed at preventing future breaches from other foreseeable sources.

Congress needs to modernize U.S. data legislation by affirmatively granting the FTC explicit authority over the data security practices of businesses. A new model under the FTC should take the FCC's approach as an example upon which to build, and create a more stringent, efficient data security framework that ensures companies constantly adapt to the latest technological innovations. The ultimate goal should be to keep personal data in the rightful control of consumers, many of whom do not yet realize the true value that it holds.

The Quadrennial Review: The Federal Communications Commission's Latent Superpower & What Can Be Done to Free It

It's a bird! It's a plane! It's faster than a speeding bullet! It's... changing media consumption avenues!

As more Americans begin to consume their media over the Internet, it becomes increasingly apparent that the standing media ownership rules – the rules governing who can own what TV station, radio station, or newspaper in a given market and nationally – are outdated as the shift towards Internet media has already begun. While these rules exist to protect Americans from a concentration of viewpoints, these rules must be updated regularly to

guarantee that viewpoints are not lost, especially as the Internet becomes the dominant source of news.

The Federal Communications Commission (the "FCC") currently enforces media ownership rules, guaranteeing diversity, localism, and competition. But, the current media ownership rules need to be able to adapt to the changing times. The FCC has that precise superpower in its Quadrennial Review authority. Every four years, the FCC is empowered to review its media ownership rules in order to maintain, modify, or repeal the rules to best serve the public interest. But, this superpower is currently locked up and reduced from its full potential due to constant legal challenges and intense scrutiny from the courts.

This Note explains how the FCC has attempted – and failed – to modify its media ownership rules through the use of the Quadrennial Review and suggests potential solutions to help free this regulatory tool from its current stagnancy. Section II will explore the legislative, legal and procedural history of the Quadrennial Review and highlight the current media ownership rules. Section III will analyze the potential solutions that Congress, the courts, and the FCC can employ to help the FCC realize the power underlying the Quadrennial Review and let the FCC guide the way into the new media consumption era and protect consumers.

A New Dog With the Same Old Tricks: The Government's Open Data Initiatives

The Internet connects us all in ways the law has yet to fully understand. In recent years, Google has developed into a powerful search engine that effectively functions as a monopoly on indexing Internet content. We have also created an entirely new industry around social media where individual users freely share information, both trivial and profound, about every aspect of their lives. And then we have developed an online memory, with cached data and viral sharing, such that almost nothing on the Internet can ever be truly deleted.

Personal identity has become a twofold construct: an offline identity, which an individual displays in his or her interpersonal interactions; and an online identity, which an individual displays on the Internet in various forms, for friends, family, acquaintances and strangers alike. With new technology has also come new ways to harm others, and because our twofold identities are not always easy to separate, online harms can creep into offline harms in ways the law has yet to anticipate. A federal statute is necessary to update and enforce our cultural understanding of identity and the human rights to which we are entitled under the federal Constitution.

COMMUNICATIONS LAW: ANNUAL REVIEW

Are Cyber Security Incident Response Teams (CSIRTs) Redundant or Can They Be Relevant to International Cyber Security?

Zahra Dsouza *

TABLE OF CONTENTS

* Zahra Dsouza is a Law Clerk at Kohn Swift & Graf P.C. and a graduate of Temple University Law School's LL.M. Program. The author wishes to acknowledge that this paper was based on the concept of "A Red Cross for Cyberspace" by Duncan Hollis and Tim Maurer originally published in New America's digital magazine, The Weekly Wonk and extend particular thanks to Duncan Hollis, Associate Dean and Professor at Temple Law School for his assistance in the preparation of this article.

I. INTRODUCTION

Cyber security incidents can have severe consequences for individuals, businesses and states. The scope of the problem is expanding as adversaries develop increasingly sophisticated cyber tools and techniques.[1] Moreover, the scale of the problem is growing with increased interdependency.[2] Given the cross-border nature of cyberattacks, international cooperation is critical to prevent and respond to incidents.[3] A key response to cybersecurity incidents has been Cybersecurity Incident Response Teams ("CSIRTs"). A CSIRT is "a service organization that is responsible for receiving, reviewing and responding to computer security incident reports and activity."[4] CSIRTs traditionally served as intermediaries "between benign identifiers, who reported vulnerabilities, and software users" and disseminated vulnerability information.[5] However, CSIRTs face legal and practical challenges to their continuing existence. CSIRTs do not have a clear mandate: their role and relationship with the state, other CSIRTs operating within the state, and international actors are unclear and national laws impede the ability of CSIRTs to share data.[6] Moreover, the information collected and shared may be inaccurate due to under reporting and inconsistencies. Trust and cooperation are also impeded by the commodification of vulnerabilities, state perceptions of cyberspace as

1. *Worldwide Threat Assessment of the US Intelligence Committee: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. (2017), https://www.intelligence.senate.gov/sites/default/files/documents/os-coats-051117.pdf [https://perma.cc/S9ZL-CAC7] (statement of Richard R. Coats, Director of National Intelligence).

2. Wyatt Hoffman and Ariel Levite, *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?*, CARNEGIE ENDOWMENT FOR INT'L PEACE (June 14, 2017), http://carnegieendowment.org/2017/06/14/private-sector-cyber-defense-can-active-measures-help-stabilize-cyberspace-pub-71236 [https://perma.cc/N2NZ-MFRV].

3. *Id.*

4. *See* Isabel Skierka, Robert Morgus, Mirko Hohmann & Tim Maurer, *CSIRT Basics for Policy Makers: The History, Types & Culture of Computer Security Incident Response Teams* 8 (New Am. & Global Pub. Pol'y Inst., Working Paper No. 1, 2015), https://static.newamerica.org/attachments/2943-csirt-basics-for-policy-makers/CSIRT%20Basics%20for%20Policy-Makers%20May%202015%20WEB%2009-15.16efa7bcc9e54fe299ba3447a5b7d41e.pdf [https://perma.cc/68RH-75PC]

5. *See* Karthik Kannan & Rahul Telang, *Market for Software Vulnerabilities? Think Again*, 52 MGMT. SCI. 726 (2005) (examining whether a market-based mechanism for vulnerability disclosure outperforms CERTs).

6. Skierka et al., *supra* note 4.

a new threat domain, the expansion of the CSIRT community, and advent of a "cyber regime complex."[7]

This paper examines the constitutive statutes of the International Red Cross and Red Crescent Movement ("Movement") and proposes that the role of actors in cybersecurity and CSIRT landscapes and CSIRTs be re-conceptualized by adopting Movement functions and components. The first section of this paper will provide background on the cyber security incident landscape, explaining the nature and scope of the problem. The second section will provide background information on the global CSIRT network by describing the historical and current roles and responsibilities a CSIRT assumes and exploring current cooperation, collaboration, and information-sharing efforts. The third section will focus on the legal and practical obstacles that limit information sharing. The fourth section explores emergency response mechanisms to humanitarian crises and considers whether CSIRTs can be re-conceptualized. The paper concludes with the following recommendations: (1) that the Forum for Incident Response and Security Teams ("FIRST") serve as an umbrella organization responsible for providing information, support, and coordination between CSIRTs; (2) that States support National CSIRTs ("NCSIRTs") by enacting legislation that clearly defines the mandate of CSIRTs and their relationship with other actors and allocate resources for CSIRTs; and (3) that NCSIRTs assist victims and contribute to the community by assisting in the development of other CSIRTs. This will enable CSIRTs to coordinate the response to cyber security incidents at a global level.

II. THE CYBER SECURITY INCIDENT LANDSCAPE

Cybersecurity incidents can have severe consequences for individuals, businesses, and States. Individuals may suffer financial loss through phishing or devastating psychological effects as occurred in the suicides associated with the leak of Ashley Madison customer details.[8] Businesses may suffer direct financial loss as a result of data theft and corporate espionage (e.g., cyberattacks on Target, Anthem, Home Depot, and J.P. Morgan) or physical damage to operating equipment, such as servers.[9] It is

7. Samantha Bradshaw, *Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity* 6 (Cent. for Int'l Governance Innovation, Working Paper No. 23, 2015), https://www.cigionline.org/sites/default/files/gcig_no23web_0.pdf [https://perma.cc/8G3G-J5HB] (examines the role of CSIRTs in the emerging cyber regime complex and considers what factors contribute to the lack of trust and information sharing within the community).

8. Chris Baraniuk, *Ashley Madison: 'Suicides' Over Website Hack*, BBC NEWS, (May 15, 2016, 5:40 PM), http://www.bbc.com/news/technology-34044506 [https://perma.cc/XKT4-J984].

9. Peter Elkind, *Sony Pictures: Inside the Hack of the Century,* FORTUNE (June 25, 2015, 6:00 AM), http://fortune.com/sony-hack-part-1/ [https://perma.cc/F9Q2-DXT4].

estimated that computer crime is costing the United States $10 billion,[10] and that computer fraud is now costing businesses in the U.K. 5 billion pounds a year.[11] Businesses also face indirect costs including liability and loss of reputation, customer confidence, and productivity.[12] Threat actors also target government agencies and their contractors, "potentially resulting in the disclosure, alteration, or loss of sensitive information, including personally identifiable information (PII); theft of intellectual property; destruction or disruption of critical systems; and damage to economic and national security."[13] For example, the data compromised in the hack of the Office of Personnel Management involved sensitive information of current, former, and prospective federal employees, including forms which contain details about the employees' personal life, family members, other contacts, interviews, record checks, fingerprint data (limited), polygraph data,[14] social security numbers, addresses, employment history, and financial records of approximately 21.5 million people.[15] States may also be concerned with attacks that threaten their values as evidenced by the cyberattack against Sony Pictures Entertainment.[16] The attack was in response to the release of a film depicting the assassination of the North Korean head of state and was viewed as an attack on freedom of expression.[17]

The reach and impact of cyberattacks exceeds that of traditional crimes. Perpetrators of cybercrimes do not require physical proximity to their victims and are not impeded by national borders.[18] Cyberattacks can be carried out at high speeds and directed at multiple victims simultaneously,

---

10. Sasha Romanosky, *Examining the Costs and Causes of Cyber Incidents* 2 (Jan 14, 2016) (unpublished draft) (on file with FTC), https://www.ftc.gov/system/files/documents/public_comments/2015/10/00027-97671.pdf [https://perma.cc/TQ52-S8D8].

11. Scott Charney & Kent Alexander, *Computer Crime*, 45 Emory L.J. 931, 937 (1996).

12. Ahmad, Atif, Justin Hadgkiss & A.B. Ruighaver, *Incident Response Teams - Challenges in Supporting the Organisational Security Function*, 31 COMPUTERS & SECURITY 643, 644 (2012).

13. *Is the OPM Data Breach the Tip of the Iceberg? Joint Hearing Before the H. Subcomm. on Oversight & H. Subcomm. on Research & Tech. of the Comm. on Science, Space & Tech.*, 114th Cong. 52 (2015) [hereinafter *Wilshusen*] (written statement of Gregory C. Wilshusen, Director, Information Security Issues, U.S. Gov't Accountability Office).

14. Michael Adams, *Why the OPM Hack Is Far Worse Than You Imagine*, LAWFARE BLOG (March 11, 2016, 10:00 AM), https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine [https://perma.cc/5AK3-867E].

15. Marina Koren, *About Those Fingerprints Stolen in the OPM Hack*, ATLANTIC (May 14, 2016, 5:56 PM), http://www.theatlantic.com/technology/archive/2015/09/opm-hack-fingerprints/406900/ [https://perma.cc/ANZ9-98UE].

16. Elkind, *supra* note 9.

17. *Id.*

18. Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Product Liability and Other Issues*, 5 PITT. J. TECH. L. & POL'Y 1 (2004), https://tlp.law.pitt.edu/ojs/index.php/tlp/article/viewFile/16/16. [https://perma.cc/9DVQ-MX9M]

and attackers more easily can remain anonymous.[19] The adversaries in cyberspace include bot net operators, criminal enterprises, hackers, insiders, state-sponsored groups or states themselves, and terrorists.[20] The scope of the problem is also expanding as adversaries develop increasingly more sophisticated cyber tools and techniques.[21] Moreover, the scale of the problem is growing with increased interdependency. Information security incidents reported by federal agencies over the last several years have risen from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014.[22]

Due to the cross-border nature of cybercrime, no State can deal with the problem independently.[23] For example, if a Pakistani national is suspected of illegally accessing a computer system located in the United States, Pakistan's Federal Investigation Agency may require information that is only available in the United States in order to investigate and prosecute the offense.[24] Therefore, international cooperation is critical to preventing and responding to cybersecurity incidents.

International cooperation is impeded by difficult legal questions. Cybersecurity incidents often go unreported,[25] and even when they are reported, law enforcement prosecutors face significant challenges including technological and evidentiary, and jurisdictional hurdles.[26] For example, a number of developing countries do not have legislation that specifically addresses cybercrime.[27] Existing legislation enacted for the protection of

19. *Id.*

20. *Wilshusen*, *supra* note 13.

21. *Cyber Threat Source Descriptions*, ICS-CERT, https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions [https://perma.cc/W8F6-4NLS] (last visited: Aug. 1, 2017).

22. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-194T, INFORMATION SECURITY: FEDERAL AGENCIES NEED TO BETTER PROTECT SENSITIVE DATA (2015), http://www.gao.gov/assets/680/673678.pdf [https://perma.cc/YGL4-BCP7].

23. Roderic Broadhurst, *Developments in the Global Law Enforcement of Cyber-Crime*, 29 POLICING: AN INT'L J. POLICE STRATEGIES & MGMT. 408 (2006), https://pdfs.semanticscholar.org/a3f6/5eb8980eb6fee577aa55d12f061e590e9b7a.pdf [https://perma.cc/4A45-YC7G].

24. COMPREHENSIVE STUDY ON CYBERCRIME: DRAFT, at 5, U.N. OFFICE ON DRUGS & CRIME (2013), https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [https://perma.cc/52SH-7Y7J].

25. *Id.*

26. *Assistant Attorney General Leslie R. Caldwell Delivers Remarks at "Cybersecurity + Law Enforcement: The Cutting Edge" Symposium*, U.S. DEP'T JUSTICE (Oct. 16, 2015), https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-cybersecurity-law [https://perma.cc/97F2-XYEJ].

27. Philip Garson, *Cybercriminals Find Wonderland in Developing Countries*, OPENDEMOCRACY: OPENSECURITY (Dec. 10, 2013), https://www.opendemocracy.net/opensecurity/philippa-garson/cybercriminals-find-wonderland-in-developing-countries [https://perma.cc/HY8Q-KH78].

physical property is not equipped to deal with cybercrimes.[28] For example, traditional search and seizure procedures cannot be applied to computer data.[29]

Where legislation does exist, insufficient harmonization of cybercrime offences, investigative powers, and admissibility of electronic evidence across national legal frameworks impede the investigation and prosecution of cybercrimes.[30] For example, signatories of the Convention on Cybercrime ("Convention")[31] that have implemented legislation akin to the Convention may be reluctant to share data with states that are not parties to the Convention for fear that, in the absence of agreement on what constitutes cybercrimes, the receiving state may use the data to prosecute conduct that is not recognized as an offence, such as blasphemy online. Conversely, signatory states may be reluctant to receive data collected from states that have failed to implement civil liberties and due process safeguards, such as independent oversight and limits on the scope and duration of powers. Further, trans-border searches pose jurisdictional problems and have international ramifications.[32]

III. HISTORICAL BACKGROUND AND THE EMERGENCE OF CSIRTS

The purpose of the CSIRT mandate is to develop and promote best management practices and technology applications to "resist attacks on networked systems, to limit damage, and to ensure continuity of critical services."[33] CSIRTs provide a range of services including proactive and reactive services, as well as security quality management functions.[34] With

28. Oona A. Hathaway & Rebecca Crootof, *The Law of Cyber-Attack* (Yale Law School Legal Scholarship Repository, Paper No. 3852, 2012), http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4844&context=fss_papers [https://perma.cc/H48C-UZVN].

29. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 557 (2005).

30. Zahid Jamil, Cybercrime Model Laws 5 (Dec. 2014) (discussion paper) (on file with the Cybercrime Convention Committee of the Council of Europe), https://rm.coe.int/1680303ee1 [https://perma.cc/H7DX-9S7B] (summarizing the content and analysing the strengths and weaknesses cybercrime model laws as well as their consistency and compatibility with the Budapest Convention).

31. Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.

32. P. Sean Morris, *"War Crimes" Against Privacy—The Jurisdiction of Data and International Law*, 17 J. High Tech. L. 1 (2016), https://sites.suffolk.edu/jhtl/wp-content/uploads/2016/12/War-Crimes-Against-Privacy.pdf.

33. Stuart Madnick, Xitong Li & Nazli Choucri, *Experiences and Challenges with using CERT Data to Analyse International Cyber Security* 3 (MIT Sloan School of Management, Working Paper No. 4759-09, 2009), http://ssrn.com/abstract=1478206.

34. *CSIRT Services*, SOFTWARE ENGINEERING INST.:CERT, http://www.cert.org/incident-management/services.cfm? (last visited Oct. 31, 2017, 6:00 PM).

its reactive services, a team acts to mitigate incidents when notified.[35] Proactive services and security quality management, on the other hand, seek to prevent future incidents.[36] Victims are more likely to report intrusions to Computer Emergency Response Teams (CERTs) to obtain immediate technical assistance and when CERTs identify patterns, they can alert potential victims and seek assistance from other experts working to address the same problem.[37]

Tracing the historical emergence of CSIRTs provides insight into the original conception of the purpose CSIRTs would serve. The first CERT was formed by the United States Department of Defense and Carnegie Mellon University in response to the Morris worm incident in 1988.[38] The CERT was created to improve communication, avoid redundant analysis, and ensure timely defensive and corrective measures to limit the damage done by cyber incidents.[39] In the 1990s, the United States' CERT lead the way for other countries to develop their own CERTs.[40] The United States' CERT adopted CERT Coordination Center (CERT/CC) as its official name, as many other response teams have chosen the name CERT (where others have chosen CSIRT).[41]

CERT/CC coordinates actions for all global CERTs and sets the bar for best practices:

> CERT/CC works in the following fields, which provide a guideline for the work of other national CERTs and CSIRTs around the world:
> • *Software Awareness*: Searches for, receives, analyses, and reports major software security vulnerabilities and malicious code. Publishes advice on responses to vulnerabilities and threats, and helps create software more secure to attack.
> • *Secure Systems*: Engineering [] networks that have high situational awareness and high response speed to deal with coordinated attacks. Goal is to create networks that can survive attack and continue functioning.

35. Georgia Killcrece, *Incident Management*, U.S. COMPUTER EMERGENCY READINESS TEAM (Dec. 19, 2005), https://www.us-cert.gov/bsi/articles/best-practices/incident-management/incident-management [https://perma.cc/D3U2-4XHN].

36. *CSIRT Services*, *supra* note 34.

37. Charney & Alexander, *supra* note 11, at 938.

38. *Id.* at 933–935 ("Robert Morris, a Cornell University student, developed a program in 1988 designed to attack computers throughout the Internet. After the worm penetrated the target computer, it would consume the computer's available memory, resulting in the shutdown of the computer. Before the worm could be neutralized, it had crippled approximately 6,200 computers and caused over 98 million dollars in damage. If Stoll's experience taught us that our information was vulnerable, the Morris worm proved that our hardware was equally at risk.").

39. Bradshaw, *supra* note 7, at 5.

40. Madnick et al., *supra* note 33.

41. *Id.*

> • *Organizational Security*: Encourages and helps develop implementation of proper security management and software in individual organizations, and advocates government policy that increases security of national, corporate, and private systems.
> • *Coordinated Response*: Helps create and train response teams for different organizations, governments, and companies, including the Department of Homeland Security (US-CERT), and the National Computer Security Incident Response Team (CSIRT) of Qatar.
> • *Education and Training*: Provides public training seminars, certification training/testing, as well as collegiate degrees at CMU.[42]

CERT/CC currently partners with government, industry, law enforcement, and academia to develop advanced methods and technologies to counter large-scale, sophisticated cyber threats.[43] Activities of CERT/CC include working with the Department of Defense to protect critical data, providing operational support and training to law enforcement for digital intelligence and investigation, providing organization security, identifying vulnerabilities and insider threats, conducting training though traditional classroom based courses and a virtual training environment, and developing curriculum in software assurance survivability and information assurance.[44] CERT/CC is also involved with the Software Engineering Institute's Smart Grid effort, a "project that focuses on improving the efficiency of the power grid while reducing the impact to the environment."[45] "Although the statistics available with CERT/CC are not as detailed as nation-level CERTs, they are highly aggregated and serve as a useful indicator of global CERT effectiveness."[46] This suggests that CERT/CC has evolved from providing incident response to undertaking research and development.

The roles and responsibilities of various CSIRTs with respect to cooperation, collaboration and information-sharing differ based on factors such as their constituency, skill set, and funding levels.[47] A New America paper entitled "CSIRT Basics for Policy-Makers" categorizes different CSIRTs by the constituency they serve, since most incident response teams continue to underscore the importance of an approach in which the top priority is to stop an incident and save the victim.[48] Today, CSIRTs serve a diverse group of organizations and institutions including governments, private sector organizations, and technical organizations.

---

42. Madnick et al., *supra* note 33, at 3.
43. Bradshaw, *supra* note 7, at 9.
44. *About Us*, SOFTWARE ENGINEERING INST.:CERT (May 15, 2016, 07:55 AM), http://www.cert.org/about [https://perma.cc/5WJ5-JB7U].
45. *Id.*
46. Madnick et al., *supra* note 33, at 2.
47. Bradshaw, *supra* note 7, at 9.
48. Skierka et al., *supra* note 4, at 11–13

National CSIRTs (NCSIRTs) serve as the point of contact for both domestic incident response stakeholders and other NCSIRTs.[49] In the national context, NCSIRTS receive, analyze and synthesize information on vulnerability issues in their countries via surveys that ask organizations to disclose attack types, defenses, and shortcomings within the organization.[50] Some CSIRTs have the capability and means in their national networks to collect data via passive probes.[51] Aggregated data can be compiled by CSIRTs to report national trends.[52] The centralized reporting function of CSIRTs facilitates determination of the scope of computer misuse.[53] NCSIRTs may serve as the response team of last resort and assist other organizations lacking an incident response capability with securing their networks.[54]

Advanced NCSIRTs may be part of a larger national security operations center whereas less developed NCSIRTs operate within a particular government department such as law enforcement and more than one NCSIRT may exist.[55] NCSIRTs may be exclusively responsible for critical infrastructure incident response coordination or may be responsible for executing a state's cyber defense policy typically by issuing various alerts and warnings, handling aspects of cyber incidents, or providing training and education to government constituents.[56] NCSIRTs that coordinate incident response typically share information with other actors, including other CSIRTs and provide secure communication channels, like phone call or in person meetings, for CSIRTs to exchange information and cooperate in incident handling and response.[57]

In addition to incident response, advanced NCSIRTs proactively develop security tools, perform risk analysis, test products for vulnerabilities, provide education to employees on security matters, and operate information security bulletins to share important information pertaining to vulnerabilities and software patches.[58] As an illustration, the Australian Computer Emergency Response Team (AusCERT) publishes advisories and alerts in bulletins describing the flaws in operating systems

49. *Id.* at 11.
50. Madnick, *supra* note 33, at 4.
51. *Id.*
52. *Id.* at 2.
53. *See generally* Isabel Skierka, Robert Morgus, Mirko Hohmann & Tim Maurer, *National CSIRTs and Their Role in Computer Security Incident Response* (New Am. & Global Pub. Pol'y Inst., Working Paper No. 2, 2015), http://www.digitaldebates.org/fileadmin/media/cyber/National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response__November_2015_--_Morgus__Skierka__Hohmann__Maurer.pdf.
53. SOFTWARE ENGINEERING INST.:CERT, *supra* note 44.
54. *Id.*
55. Bradshaw, *supra* note 7 at 9.
56. SOFTWARE ENGINEERING INST.:CERT, *supra* note 44.
57. Skierka et al., *supra* note 4.
58. *Id.* at 12.

applications or hardware and its impact recommended solutions and workarounds.[59] Hence, many NCSIRTs today principally engage in proactive activities. CSIRTs that operate without a legal or government mandate to do so, but are recognized as national points of contact by other NCSIRTs and stakeholders, are de facto NCSIRTs.[60] A list of NCSIRTs is available at CERT/CC.[61]

In contrast to Advanced NCSIRTs, governmental NCSIRTs serving as the national point of contact are responsible for protecting and responding to incidents on the national government network.[62] US-CERT is the 24-hour operational arm of the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC).[63] US-CERT is charged with providing response support and defense against cyberattacks for the Federal Civil Executive Branch and information sharing and collaboration with the state and local government, industry, and international partners.[64] US-CERT accepts, triages, and collaboratively responds to incidents, provides technical assistance to information system operators, and disseminates timely notifications regarding current and potential security threats and vulnerabilities.[65] Additionally, "US-CERT leverages the Protected Critical Infrastructure Information (PCII) Program to prevent inappropriate disclosure of proprietary information or other sensitive data."[66] Established in response to the Critical Infrastructure Information Act of 2002 (CII Act), the PCII Program enables members of the private sector to voluntarily submit confidential information regarding the nation's critical infrastructure to DHS with the assurance that the information will be protected from public disclosure.[67] Through its National Cyber Awareness System (NCAS), US-CERT is a valuable source of information about cyber threats and software vulnerability and an appropriate place to report breaches and other related matters.[68]

A brief description of other categories of CSIRTs is as follows:

---

59. *See* Richard Peters & Rober Sikorski, *Email Trojan Horses*, 281 SCI. NEW SERIES 1822, (1998).

60. Skierka et al., *supra* note 4, at 11.

61. SOFTWARE ENGINEERING INST.:CERT, *supra* note 44.

62. Skierka et al., *supra* note 4, at 11.

63. *National Cybersecurity and Communications Integration Center*, DEP'T HOMELAND SECURITY (May 15, 2016, 05:30 PM), https://www.dhs.gov/national-cybersecurity-and-communications-integration-center [https://perma.cc/2R5X-VZ2E].

64. SOFTWARE ENGINEERING INST.:CERT, *supra* note 44.

65. *Id.*

66. *OSINT – U.S. CERT (Computer Emergency Readiness Team)*, CCCC PROJECT (Dec. 21, 2014), https://cccounterterrorismcenter.wordpress.com/tag/cyberdefense/ [https://perma.cc/T8AL-VGD9].

67. *Protected Critical Infrastructure Information (PCII) Program*, DEP'T HOMELAND SECURITY, (May 15, 2016, 05:30 PM), https://www.dhs.gov/protected-critical-infrastructure-information-pcii-program [https://perma.cc/TEU2-9MH8].

68. *National Cyber Awareness System*, U.S. COMPUTER EMERGENCY READINESS TEAM, https://www.us-cert.gov/ncas [https://perma.cc/V7BH-NWL7] (last visited May 15, 2016, 05:24 PM).

> Sectoral CSIRTs serve a specific sector of society or the economy, and may conduct technical incident response operations.[69]
>
> Organizational CSIRTs monitor and respond to incidents on internal networks and may serve private companies, international organizations, and academic institutions.[70]
>
> Vendor CSIRTs are typically teams within vendors that produce IT used by individuals and companies that provide operational support for commonly used products like commercial operating systems to the public.[71]
>
> Commercial CSIRTs provide incident-handling services as a product to other organizations.[72]
>
> Non-profit commercial CSIRTs are funded by fees, donations, and corporate partners, while for-profit commercial CSIRTs sell incident response services.[73]
>
> Regional coordinating bodies connect national CSIRTs across borders at a regional level, and they serve to enhance cooperation between national CSIRTs and facilitate information sharing between CSIRTs in the region.[74]

CSIRTs do not handle attacks on national defense and intelligence networks, so data concerning these types of incidents are not available for analysis. Vulnerability reports prepared by CSIRTs as a result of carefully analyzing different computer system weaknesses reported daily by organizations and individuals in the U.S. are the best indicator we have regarding the types of potential cyberattacks launched on the Internet. While such reports do not represent the behavior of cyberattacks, they convey information about the types of cyberattacks that occur along with recommendations to minimize the probability of attacks against such weaknesses.[75] The reports classify and organize security weaknesses by vulnerability type and make recommendations to protect against possible

69. Skierka et al., *supra* note 4, at 11.
70. *Id.* at 12.
71. *Id*.
72. *Id*.
73. *Id*.
74. *Id*.
75. Alexander McLeod, Carlos Alberto Dorantes & Glenn Dietrich, Modeling Security Vulnerabilities Using Chaos Theory: Discovering Order, Structure, and Patterns from Chaotic Behavior in Complex Systems (June 2, 2008), *in* PROCEEDINGS OF THE 7TH ANNUAL SECURITY CONFERENCE, JUNE 2–4, 2008 (2008), https://ssrn.com/abstract=2515047.

attacks.[76] "Therefore, it is assumed that vulnerabilities are signals of the persistency of security incidents such as virus, worms, intrusions, and other types of cyberattacks."[77]

The growth in the number and categories of CSIRTs worldwide demonstrates the potential for the development of a sophisticated and coordinated global cybersecurity response network. Ideally, information sharing between NCSIRTs under the supervision of an umbrella organization would increase prevention and monitoring capability and in turn lead to a coordinated response to cyberattacks.

FIRST is the global forum for CSIRTs worldwide.[78] Founded in the U.S. in 1990, it is comprised of various CSIRTs.[79] FIRST aims to foster cooperation and coordination in incident prevention, to encourage rapid reaction to incidents and to promote information sharing among members and the community on a global level.[80] FIRST promotes best practices and standards for cyber security and develops curricula to build and strengthen CSIRT capacity and maturity.[81] In order to become a member of FIRST, two existing full members must nominate the CSIRT, then the Steering Committee must approve membership by a two-thirds vote, and lastly, the CSIRT must undergo a site visit.[82] FIRST expects members to actively improve the security of their constituents' information technology resources and to raise awareness of computer-security issues among its constituency and within the community.[83] Membership may be revoked if a member fails to contribute to these goals or to cooperate with other members.[84] Membership in FIRST facilitates access to incident information shared among members, exchanges of best practices or to training sessions.[85]

In addition to FIRST, other regional mechanisms, for example the European Network and Information Security Agency (ENISA) and Asia Pacific Computer Emergency Response Team (APCERT), also help CSIRTs share knowledge, strengthen capacity and cooperate.[86] APCERT's mission is to "promote regional and international cooperation on information security" by "developing measures to respond to large-scale or regional

76. *Id.*
77. *Id.*
78. *See FIRST Vision and Mission Statement*, FIRST, https://www.first.org/about/mission [https://perma.cc/5C6D-98LJ] (last visited Oct. 31, 2017, 10:00PM).
79. *See FIRST History*, FIRST, https://www.first.org/about/history [https://perma.cc/HM5J-C5CC] (last visited Nov. 1, 2017, 9:30 PM).
80. *See* FIRST, *supra* note 78.
81. *Id.*
82. *See Membership Process at a glance*, FIRST, https://www.first.org/membership/ [https://perma.cc/2CN8-P9HR] (last visited Nov. 1, 2017, 9:30 PM).
83. *Id.*
84. *See Bylaws of FIRST.Org, Inc.*, FIRST, https://www.first.org/about/policies/bylaws [https://perma.cc/7C9R-23QE] (last visited Nov. 1, 2017, 9:30 PM).
85. *See* FIRST, *supra* note 78.
86. Skierka et al., *supra* note 4.

network security incidents"; facilitating information sharing among its members; "promoting collaborative research and development"; assisting other teams in the region with emergency response; and providing inputs on "legal issues related to information security and emergency response across regional boundaries."[87] APCERT membership has two categories: operational and supporting members.[88] Operational membership is open to operational, national, not for profit CSIRTs in the Asia Pacific region that provide the required information and submit an application form, obtain a sponsor from among current APCERT Operational Members to provide a report and serve as a mentor, and be approved by the APCERT Steering Committee.[89] Supporting membership is open to CSIRTs that are able to participate in information sharing, training and provide other assistance.[90] Supporting membership applicants must submit an application sponsored by three existing APCERT Operational Members and obtain Steering Committee approval.[91]

While some programs require members to be from a particular region, other platforms enable anyone to share information. Building on the experience and knowledge acquired by other CSIRTs, CSIRTs can identify and avert damage from cyber threats more quickly. Further, by sharing threat information with law enforcement agencies and governments, CSIRTs can help dismantle criminal networks. While the utility of sharing information may be limited in instances where an individual is used as the conduit for attack or a novel technique is employed, sharing threat data still remains critical for the overall resilience of the network. For example, following the hack on Sony,[92] US CERT published US Cert Alert (TA14-353A) on Targeted Destructive Malware,[93] and Security Tip (ST13-003) on Handling Destructive Malware,[94] and the Federal Bureau of Investigation

87. *Mission Statement*, ASIA PACIFIC COMPUT. EMERGENCY RESPONSE TEAM (May 15, 2016, 8:02 AM), http://www.apcert.org/about/mission/index.html [*hereinafter Mission Statement*].

88. *See Member Teams,* ASIA PACIFIC COMPUT. EMERGENCY RESPONSE TEAM, https://www.apcert.org/about/mission/index.html [https://perma.cc/G7KP-JPBV] (last visited Nov. 1, 2017, 9:30 PM).

89. *See How to Join APCERT*, ASIA PACIFIC COMPUT. EMERGENCY RESPONSE TEAM (May 15, 2016, 08:02 AM), http://www.apcert.org/application/index.html [https://perma.cc/3X8E-6PUF].

90. *Id.*

91. *Id.*

92. NOVETTA, OPERATION BLOCKBUSTER: UNRAVELLING THE LONG THREAD OF THE SONY ATTACK (2016), https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf.

93. *Alert (TA14-353A)*, U.S. COMPUTER EMERGENCY READINESS TEAM (May 15, 2016, 8:02 AM), https://www.us-cert.gov/ncas/alerts/TA14-353A [https://perma.cc/TB8R-WCT8].

94. *Security Tip (ST13-003)*, U.S. COMPUTER EMERGENCY READINESS TEAM (May 15, 2016, 8:05 AM), https://www.us-cert.gov/ncas/tips/ST13-003 [https://perma.cc/V4PG-AB33].

camped out at Sony's lot and conducted multiple hour-long "clinics" on identity theft and computer security on a sound stage for Sony employees.[95]

Cooperation could be strengthened through the enhanced and timely exchange of cyber threat information. CSIRTs should continue to play a critical role in global cybersecurity as CSIRTs have the technical skills necessary to prevent and respond to cyber incidents through incident analysis and response, information sharing and dissemination, and skills training. However, CSIRTs have been unable to solve the cyber security problem due to legal and practical obstacles. If CSIRTs are not able to adapt to respond to increasingly sophisticated incidents on a larger scale, global cybersecurity will become less stable. Nevertheless, drawing on lessons from other emergency response endeavors, CSIRTs can adapt to remain relevant to International Cyber Security.

IV. LEGAL AND PRACTICAL OBSTACLES THAT LIMIT INFORMATION SHARING

Cooperation is impeded by difficult legal questions and "a lack of trust among community members."[96] CSIRTs face both external and internal challenges because national laws on data localization exchange and jurisdiction may bar information sharing. For example:

> [Russia's] 242-FZ law, which went into effect September 1, 2015, adds a specific data localization requirement that "personal data operators" collect, store, and process any data about Russian users in databases inside the country and inform Russian authorities of the location of their data centers. In addition, the law provides authorities easier access to information and imposes harsh penalties on non-compliant companies. Finally, it restricts Russian users' access to any website that violates the nation's data protection laws.[97]

Further, sharing information may expose CSIRTs to liability or civil fines in certain cases. Requirements to make certain agency records public may also dissuade CSIRTs from sharing threat data. These laws are especially troublesome for private sector CSIRTs where threat intelligence

95. *See* Tami Abdollah, *Sony CEO breaks down hack response, Google role in 'The Interview' release,* MERCURY NEWS (May 15, 2016, 8:05 AM), http://www.mercurynews.com/business/ci_27290586/sony-ceo-breaks-down-hack-response-google-role [https://perma.cc/C9XL-A9F4].

96. Bradshaw, *supra* note 7, at 6.

97. ALBRIGHT STONEBRIDGE GRP., *Data Localization: A Challenge to Global Commerce*, (2016), http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf [https://perma.cc/3JCC-V5XN].

might contain proprietary information.[98] For example, by voluntarily providing data, which often contains proprietary information, with a third party, companies in the United States risk losing any intellectual property rights protection afforded under the Uniform Trade Secrets Act.[99] In addition, privacy laws will determine when and how CSIRTs may use and disclose data that could constitute personal information, such as IP addresses or emails, to prevent or respond to incidents.[100] Sanitizing cyber threat data of any proprietary or personal information would enable disclosure, but this process can be time-consuming and the information may have become obsolete by the time all identifiers are removed. Sanitization requires significant resources and does not guarantee privacy as studies suggest that data is easily de-anonymized and individuals can be identified.[101]

CSIRTs, especially private sector CSIRTs, must have confidence that information shared will be carefully controlled, especially given the high costs associated with a security breach. However trust and cooperation are impeded by "the commercialization of cyberspace and the commodification of vulnerabilities; geopolitical power and cyberspace as a new threat domain, and the growth of the CSIRT community and the emergence of a cyber regime complex."[102] First, commercial CSIRTs that profit from stopping cyber threats view threat data as a valuable commodity and are reluctant to share it.[103] Competition usually facilitates choice however, in a scenario where vulnerability data is not equally accessible, it creates insecurity between entities trying to secure the network and is counterproductive.[104]

Second, states view the Internet "as a new domain in which to exert control."[105] States guard their knowledge of vulnerabilities and threat information in order to use it to develop malware and deliver exploits for various national security or surveillance purposes. However, developing new exploits or leaving old vulnerabilities unaddressed creates risk in the system.[106] The objective of obtaining a strategic military advantage over another state's cyber defenses is at odds with the state's responsibility to secure cyberspace.[107] The uncertainty over CSIRT involvement in pervasive surveillance activities by state actors has discouraged cooperation with

98. *See* Bradshaw, *supra* note 7, at 12.

99. *See* NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS, UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS (1985), http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.

100. *See* Bradshaw, *supra* note 7, at 5.

101. *See generally* Yves-Alexandre de Montjoye et al., *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata,* 347 SCIENCE 536, 536–39 (2015).

102. *See* Bradshaw, *supra* note 7, at 13.

103. *Id.*

104. *Id.*

105. *Id.*

106. *Id.* at 14.

107. *Id.*

CSIRTs and organizations involved in national cyber security and law enforcement efforts.[108]

Third, new "CSIRTs are entering the CSIRT community, and the CSIRT community is itself entering the emerging cyber regime complex. CSIRTs must determine how they will work with institutions and organizations that have their own unique and at times incompatible laws, interests and norms.[109] Together, these processes create a number of challenges for international cooperation.

Data collection presents its own problems. Many countries do not have national CSIRTs. Data collected by CSIRTs may fail to represent the complete breadth of the problem since victims may not be aware that they have been victims of cyberattacks. Alternatively, victims may decide to handle incidents internally due to reporting costs, reputational costs or fears of additional attacks in response to the exposure of vulnerabilities,[110] or regulatory scrutiny.[111] Many CSIRTs have only started to record data within the last three or four years, limiting the possibility for historical trend analysis.[112] Information collected across CSIRTs is inconsistent and impedes comparisons. Surveys used by CSIRTs to collect data vary greatly. CSIRTs define terms inconsistently, do not share categorization methods for threats and vulnerabilities, track different categories of attacks and vulnerabilities, and lack a consistent data presentation method. Finally, national CSIRTs that are not mandated by federal governments respond to only a fraction of the total number of national incidents.[113] Thus, information provided by CSIRTs may not be indicative of the true volume of national domestic attacks.

Given the transnational nature of cyber-attacks and the current threat landscape, CSIRTs have formed an informal network to cooperate in preventing and responding to such attacks. CSIRTs play an active role in protecting the privacy and security of data for their constituents, and in helping to respond to such incidents.

---

108. *Id.*

109. *Id.* at 6.

110. *See* Charney & Alexander, *supra* note 11, at 938.

111. *See*, *e.g.*, *FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy*, FED. TRADE COMMISSION (Aug. 29, 2013), https://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers [https://perma.cc/RT6M-2FMR] (describing FTC complaint against medical testing laboratory alleging that the company, in two separate incidents, "exposed the personal information of approximately 10,000 consumers"); *FTC Files Complaint Against Wyndham Hotels For Failure to Protect Consumers' Personal Information*, FED. TRADE COMMISSION (Jun. 26, 2012), https://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect [https://perma.cc/7GR4-PTXV] (describing FTC suit against Wyndham Worldwide Corporation for alleged data security failures that "led to fraudulent charges on consumers' accounts, millions of dollars in fraud loss," and the export of consumer payment information to a domain name registered in Russia).

112. Madnick et al., *supra* note 33, at 13.

113. *Id.*

The question follows: Is there an alternative to CSIRTs? Private internet security companies, such as FireEye,[114] may not be considered CSIRTs, "but Commercial CSIRTs are largely a new phenomenon, and while many of these teams do not self-identify as CSIRTs, there is an active debate within the CSIRT community about their role and how they complement traditional CSIRTs."[115] CSIRTs serve vulnerability disclosure better than market based private corporations or even regulated market based mechanism because private corporations serve a limited market, i.e. their subscribers.[116] Therefore. non-subscribers may be susceptible to attacks especially if vulnerability information is leaked to the public in unregulated market.[117] This may also have the adverse effect of creating an increase in the supply of vulnerabilities and socially detrimental forces may force users to pay a premium for protection and other services.[118] Therefore, CSIRTs offer the best solution and must evolve to remain relevant to international cybersecurity.

V. RE-CONCEPTUALIZATION OF CSIRTS: EMERGENCY RESPONSE

The inability of CSIRTs to cooperate effectively suggests that either CSIRTs are a waste of resources or this approach to securing networks ought to be abandoned or re-conceptualized. One way to re-conceptualize CERTs is to classify them as international humanitarian organizations. To illustrate this potential, a comparison of the primary international humanitarian regime, i.e. the Red Cross and Red Crescent Movement, may prove useful. The actors in the Cybersecurity incident response space must restructure their roles and responsibilities, as well as their relationships with each other. In particular, CSIRTs must adapt their functional and operational behavior to be able to assist victims and to contribute to the community by assisting in the development of other CSIRTs.

A. History of the International Red Cross and Red Crescent Movement (Movement) and Its Components

Upon witnessing firsthand the bloodshed in the battle of Solferino, a citizen of Geneva, named Henry Dunant, was moved to establish an impartial corps of civilian volunteers, unattached to the armed forces of any state, to tend to individuals wounded in battle.[119] This corps formed in 1863

114. *See Incident Response Services*, FIREEYE, https://www.fireeye.com/services/mandiant-incident-response.html [https://perma.cc/Y48L-H7L6] (last visited October 31, 2017, 10:00 PM).

115. Skierka et al., *supra* note 4, at 12.

116. *See* Kannan & Telang, *supra* note 5, at 727.

117. *Id.*

118. *Id*.

119. *See* Michael Ignatieff, *Unarmed Warriors*, NEW YORKER, Mar. 24, 1997, at 54.

was the predecessor of the Red Cross Movement.[120] Dunant viewed war as inevitable and hence his mission was not to end war, but rather to ensure that the art of war was conducted in a civilized manner.[121] The Geneva Convention, adopted in 1864,[122] is an international recognition of the principle that enemy soldiers deserved the same medical treatment as troops of the state. Under the Convention, states agreed to neutralize hospitals, ambulances and medical staff.[123] The Convention did not include any mechanisms for penalizing non-compliance or enforcement with its provisions but rather, set a standard that combatants had to meet to be considered civilized.[124]

While the concept of civilized war has gained international recognition today, it was not accepted immediately. When Prussia invaded France in 1870, Dunant proposed that Paris be declared a safe haven however his proposal was ignored.[125] Paris came under attack and the Red Cross emblems flying above Parisian hospitals were fired upon.[126] The Movement has come a long way. "Today in Syria, the International Red Cross and Red Crescent Movement supports millions of people with food and shelter, health and first aid services, provision of safe water and livelihood projects."[127] The Movement is currently composed of three components operating under the convention and statutes[128]: the International Committee of the Red Cross (ICRC), which prioritizes "armed conflict;" the International Federation of Red Cross and Red Crescent Societies (IFRC),[129] which coordinates the international activities of National Societies and represents them in the international field;[130] and the National Red Cross Societies (Red Crescent societies in Islamic countries), which focus on responding to domestic emergencies.[131] Moreover, numerous conventions on civilizing war, for example, the 1868 Declarations of St.

120. *Id.*

121. *Id.*

122. *See* Convention for the Amelioration of the Condition of the Wounded in Armies in the Field, Aug. 22, 1864, 22 Stat. 940, T.S. No. 377.

123. *Id.* at 9.

124. *See* Ignatieff, *supra* note 119.

125. *Id.*

126. *Id.*

127. *Syria: Red Crescent and Red Cross is everywhere and for everyone*, INT'L COMMITTEE RED CROSS (May 08, 2016), https://www.icrc.org/en/document/syria-red-crescent-and-red-cross-everywhere-and-everyone [https://perma.cc/4X2U-VDPZ].

128. *Id.*

129. *Id.* at 6.

130. *See* INT'L FED'N OF RED CROSS & RED CRESCENT SOC'YS, CONSTITUTION OF THE INTERNATIONAL FEDERATION OF RED CROSS AND RED CRESCENT SOCIETIES 6 (1987) [hereinafter IFRC CONSTITUTION].

131. *The International Red Cross and Red Crescent Movement*, INT'L COMMITTEE RED CROSS, https://www.icrc.org/en/who-we-are/movement [https://perma.cc/5WTU-MCVG] (last visited October 31, 2017).

Petersburg,[132] and the Hague Convention of 1907,[133] have been drafted and ratified. However, the authority of international conventions and the ability of the law to govern war is uncertain, especially in the environment of armed conflict where judges and policemen are not available to enforce the law on the battlefield. Rather, conventions draw upon moral codes, which exist across cultures and are common to all people. As an example, there is now a fundamental principle distinguishing between combatants and non-combatants during armed conflict.[134]

Analysis of the key features in the relationship of the IFRC, National Societies, and state parties to the Conventions provides some useful lessons for CSIRTs. The IFRC is comprised of the National Red Cross and Red Crescent Societies,[135] and aims to "inspire, encourage, facilitate and promote their humanitarian activities."[136] The IFRC was formed "with the objective of (i) ensuring coordination of international activities, (ii) development and implementation of common standards and polices, (iii) organizational development, capacity building, effective international disaster management and of having an international presence and recognition as a global partner in humanitarian assistance."[137] Broadly, it "coordinates and directs international assistance following natural and man-made disasters" and combines relief operations with development work.[138] Its functions include, inter alia:

> Act as permanent body of liaison, coordination and study between the National Societies and to give them any assistance they might request; to encourage and promote in every country the establishment and development of an independent and duly recognized National Society; to assist the National Societies in their disaster relief preparedness, in the organization of their relief actions and in the relief operations themselves; to encourage and coordinate the participation of the National Societies in activities for safeguarding public health and the promotion of social welfare in cooperation with their

132. *See* Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Dec. 11, 1868, *reprinted in* 1 AM. J. INT'L L. 95, 95–96 (1907) (Supplement: Official Documents).

133. *See* Convention (IV) Respecting the Laws and Customs of War on Land., preamble, Oct. 18, 1907, 36 Stat. 2277.

134. *See* Ignatieff, *supra* note 119, at 54.

134. *See* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, T.I.A.S. 3362.

135. INT'L FED'N OF RED CROSS & RED CRESCENT SOC'YS, STATUTES OF THE INTERNATIONAL RED CROSS AND RED CRESCENT MOVEMENT 11 (1986) [hereinafter IFRC STATUTES].

136. *Id*.

137. IFRC CONSTITUTION, *supra* note 130.

138. INT'L FED'N OF RED CROSS & RED CRESCENT SOC'YS, AT A GLANCE (2007), http://www.ifrc.org/Global/Publications/general/at_a_glance-en.pdf.

> appropriate national authorities; to encourage and coordinate between National Societies the exchange of ideas . . . .[139]

National Societies have the right to receive services and information which the IFRC has the ability to provide, and support from other National Societies.[140] The IFRC is independent and has no governmental, political, racial, or sectarian nexus in order to preserve impartiality.[141] The IFRC acts through or in agreement with the National Society and state laws.[142]

The guidelines suggest that the IFRC should take steps to assist National Societies in facilitating the coordination of NGO efforts in disaster relief or to assist other appropriate national NGOs by providing:

> Pre-disaster preparedness assistance to National Societies to aid them in preparing for a possible coordination role, including the provision of training and communications equipment where appropriate; assistance to National Societies in times of disaster to carry out timely needs assessments and formulate effective relief action plans; the provision of specifically allocated and suitably equipped international personnel, in times of disaster, to assist National Societies in the critical work of gathering, analysing and sharing information pertinent to the disaster, within the responding NGO community, with a view to providing a common basis of understanding from which cooperation and coordination can grow; assistance to National Societies, in times of disaster, to develop the potential to act as a facilitator between the NGO community and the host government, if so requested.[143]

A National Society will be recognized if it fulfils the conditions for recognition[144]: namely if it has its own statute and autonomous status,[145] complies with the fundamental principles of the Movement, and cooperates with components of the movement.[146] National Societies must be directed and represented by a central body in dealings with other components of the Movement.[147] The relationship between States and National Societies is one of mutual support[148]: National Societies cooperate with public authorities

139. IFRC CONSTITUTION, *supra* note 130.
140. *Id.* at 5.
141. *Id.* at 11.
142. *Id.* at 12.
143. INT'L FED'N OF RED CROSS & RED CRESCENT SOC'YS, HANDBOOK OF THE INTERNATIONAL RED CROSS AND RED CRESCENT MOVEMENT (2011) [hereinafter IFRC HANDBOOK], https://www.icrc.org/eng/assets/files/publications/icrc-002-0962.pdf.
144. IFRC STATUTES, *supra* note 135, at 10.
145. *Id.* at 9.
146. *Id.*
147. *Id.*
148. *Id.* at 7.

and establish programs for education, health and social welfare, organize emergency relief operations for victims of armed conflict and disasters, and disseminate international humanitarian law. National Societies also provide assistance for victims of armed conflict, natural disasters and other emergencies in the form of services and personnel, material, financial and moral support through national societies, the IC or the IFRC.[149] They also contribute to development of other National Societies.[150]

The section on Relief Activities in Disaster Situations urges governments to prepare and pass legislation enabling immediate and adequate action to be taken to meet natural disasters as per a pre-established plan.[151] Although National Societies provide relief, the primary responsibility remains with the state. Hence states need to make preparations in advance, including planning for mobilization of resources, training personnel and gathering data.[152]

Actions between relief organizations must be coordinated to ensure prompt action and effective allocation of resources and to avoid duplication of effort.[153] This requires improved awareness, clarification, application and development of laws, rules and principles applicable to international disaster response. The roles and responsibilities for National Societies and international systems of disaster response in national disaster preparedness plans, including representation on appropriate national policy and coordination bodies, must be clearly defined. The guidelines also provide for the establishment and compliance with "minimum quality and accountability standards and mechanisms for disaster relief and recovery assistance."[154] Humanitarian relief must retain an apolitical character and avoid prejudicing state sovereignty and other legal rights to create confidence in the role of National Societies and preserve the impartiality of relief organizations. The Movement's four fundamental principles namely: "impartiality, political, religious and economic independence, the universality of the Red Cross and the equality of its members" included by the ICRC when revising its own statutes after the First World War, are the foundation of its legitimacy.[155] The Movement endeavors to relieve the suffering of individuals prioritized by need and does not discriminate based

149. INT'L COMM. OF THE RED CROSS, THE ICRC: ITS MISSION AND WORK (2009) [hereinafter ICRC MISSION], https://www.icrc.org/eng/assets/files/other/icrc_002_0963.pdf.

150. *Id.* at 7–8.

151. IFRC HANDBOOK, *supra* note 143, at 1206.

152. IFRC HANDBOOK, s*upra* note 143 at 1207

153. *Id.* at 1209.

154. *See* INT'L COMM. OF THE RED CROSS AND THE INT'L FED. OF RED CROSS AND RED CRESCENT SOC'YS, REPORT OF THE 30TH INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT 49 (2007) [hereinafter RESOLUTION 4], https://www.icrc.org/eng/assets/files/2011/bluebook-2007-english.pdf (Resolution 4: Adoption of the Guidelines for the Domestic Facilitation and Regulation of International Disaster Relief and Initial Recovery Assistance).

155. Statuts du Comité international de la Croix-Rouge, 10 mars 1921, Article 3, RICR , No. 28, April 1921, pp. 379-380.

on nationality, race, religious beliefs, class or political opinions. The Movement does not take sides in hostilities or engage in political, racial, religious or ideological controversies.[156] National Societies are independent from state governments. Universality touches on the responsibilities and duties the components of the Movement to help one another.[157]

The Guidelines define the relationship between states and National Societies as one where the state retains responsibility and sovereignty over disaster relief and the latter serves an auxiliary function. Hence States are competent to seek international and regional assistance.[158] National Societies are responsible for abiding by the laws of the affected State and applicable international law and coordinating with domestic authorities. Other principles of response include neutrality and impartiality. Disaster relief must be transparent and consistent with international standards, coordinated and implemented with domestic actors and those affected by disasters, provided by adequately trained personnel and commensurate with organizational capacity, with the aim to strengthen domestic disaster risk reduction relief and recovery capabilities and minimize adverse effects.[159]

The Guidelines also include language on the role of states. States should have legal policy and institutional frameworks in place which account for the role of National Societies and other stakeholders and allocate resources to ensure their effectiveness.[160] Specifically, these frameworks should address the procedures for initiation, facilitation, transit and regulation of international disaster relief and allow for effective coordination of international disaster relief and initial recovery assistance and the role of organizations which perform this function.[161] It is recommended that states designate one national relief authority to coordinate all domestic relief activities in connection with appropriate government departments and domestic and international relief agencies.[162] The Guidelines suggest that states should have procedures in place to facilitate the expeditious sharing of information about disasters with other states and organizations engaged in providing humanitarian relief.[163] Expedited cooperation may require reducing formalities or simplifying requirements for communication and information sharing.[164]

The Guidelines call for the international community to support developing states and National Societies and help with capacity building to enable them to adequately implement legal, policy, and institutional

156. ICRC MISSION, *supra* note 149.
157. IFRC STATUTES, *supra* note 135, at 519–520.
158. IFRC HANDBOOK, *supra* note 143, at 1215.
159. *Id*.
160. IFRC HANDBOOK, *supra* note 143.
161. *Id.* at 1217.
162. *Id.*
163. *Id.*
164. *Id.*

frameworks to facilitate international relief.[165] However, state sovereignty must be respected and therefore disaster relief and initial recovery should only be initiated upon obtaining consent of the affected State. Requests must be specific and States should provide information about relevant laws and regulations which govern the operation of disaster relief.[166]

The guidelines also note the importance of mobilization of adequately trained, skilled and knowledgeable professionals having the necessary experience to analyze needs; for the planning, coordination, conduct and appraisal of emergency medical actions; and recommend the preparation of instructional materials and programs for training purposes.[167]

B. Lessons for CSIRTs

The objectives of, and relationships between, components of the Movement have lessons for CSIRTs. The Movement and the first CERT were conceived in response to emergencies. Just as the ICRC principles of civilized war did not gain immediate acceptance,[168] CSIRTs face significant obstacles in terms of legal obstacles and mistrust. However, the universal acceptance of these principles today suggests that there is hope that CSIRTs can agree on principles and norms of organization and cooperation.[169]

The IFRC's objectives and the relationship between the IFRC and National Societies are instructive. CSIRTs must prioritize coordination, development, and implementation of common standards and polices, and organizational development. It may be useful to have an umbrella organization to coordinate the functions of national CSIRTs. Such an organization may merge the functions of the IFRC, Conference and Council to serve in a supervisory and guiding role. FIRST could play a role analogous to the IFRC where it could serve as a permanent liaison between CSIRTs, to promote the establishment of national CSIRTs and provide them with information and support. Similarly, FIRST could assist national CSIRTs with facilitating the various CSIRTs operating within the state similar to the role of the IFRC in assisting National Societies with facilitating NGOs. FIRST could fulfill this role by providing assistance (1) with emergency preparedness in the form of training and equipment where appropriate; (2) during incidents including the provision of specifically allocated and suitably equipped personnel to assist national CSIRTs in gathering, analysing, and sharing information pertinent to the incident; (3) within the responding CSIRT community; (4) with a view toward providing a common basis of understanding from which cooperation and coordination can grow; and (5) assistance to national CSIRTs during incidents to develop

165. *Id.* at 1217–18.
166. IFRC HANDBOOK, *supra* note 143, at 1218.
167. *Id.* at 1229.
168. *See* Ignatieff, *supra* note 119, at 54.
169. *See* Ignatieff, *supra* note 119, at 54.

the potential to act as a facilitator between the CSIRT community and the state government.

States may model their relationship with CSIRTs on their relationships with National Societies. States must support CSIRTs and CSIRTs, in turn, must cooperate with public authorities in effective incident response and capacity building. States must therefore enact legislation clearly defining the roles and responsibilities of the state, national CSIRTs, and other CSIRTs operating within the state in national incident preparedness and response plans, including representation on appropriate national policy and coordination bodies. States must also allocate resources for mobilization of resources, training personnel, and gathering data. States should also consider procedures for seeking international assistance, for example from FIRST or other national CSIRTs and the form and content of, as well as the information that the state must provide. States may also consider adopting simplified procedures to facilitate expedited cooperation in incident response. Assistance must be coordinated and implemented with domestic actors and victims of incidents, provided by adequately trained personnel and commensurate with organizational capacity, with the aim to strengthen domestic preparedness, incident risk reduction and response.

However, it is vital that CSIRTs retain their impartiality and neutrality in order to preserve the relationship of trust with other CSIRTs. Some CSIRTs publish their policies and procedures, services offered and scope of operations. However, these mechanisms do not define the intricacies of handling sensitive information and do not entirely dispel distrust. Accreditation may also provide a mechanism of engendering greater trust through demonstrating compliance with standards. Improving standards and making them transparent and obligatory would reduce uncertainty around incident response. Membership within a community with shared values and best practices, as well as with a certain degree of trust among its members is likely the best way to dispel distrust however members are quickly isolated if they do not contribute to the shared norms. CSIRTs have already begun this process, by attempting to develop norms for strengthening trust between each other as well as among their constituents.

Just as National Societies provide support to victims through national societies, or the IFRC, NCSIRTs must provide assistance to victims of incidents in the form of services and personnel, material and financial assistance, and contribute to the community by assisting in the development of other NCSIRTs.[170] The recognition that assistance may take different forms is useful in the context of CSIRTs where new CSIRTs may need technical and other forms of assistance beyond merely sharing information. Principles regarding use of resources may also be helpful in the context of CSIRTs. For example, the principle that "states should use funds and relief goods donated to them, and which they have accepted in relation to a disaster, in a manner consistent with the expressed intent with which they were given" could serve a guiding principle for how CSIRTs use

170. IFRC STATUTES, *supra* note 135, at 8.

information.[171] Similarly, the principle of limiting facilities "subject to the interests of national security, public order, public and environmental health, and public morals of the concerned affected, originating and transit States" may be instructive as to the circumstances under which information may be withheld by CSIRTs.[172]

VI. CONCLUSION

The number, gravity and complexity of threats have increased significantly over the last decade, and so have the targets. Cyberattacks have been employed to harm states' critical infrastructures or financial systems, which has further elevated the issue to the level of national and international security.[173] As the article indicates, cyber incidents are perpetrated by different kinds of adversaries using sophisticated and creative means. While CSIRTs have provided a useful solution to aggregation of information, cyber incident response and preparedness, CSIRTs must adapt in order to keep pace with adversaries.

It is recommended that actors in the cyber security incident re-structure their relationships and CSIRTs be re-conceptualized by adopting functions of components of the Movement and features of the relationships between them. First, it is suggested that an umbrella organization should be responsible for promoting the establishment of NCSIRTs, providing them with information and support, coordinating the functions of NCSIRTs and assisting NCSIRTs in facilitating the various CSIRTs operating within the state. Further, membership within a community with shared values and the development of norms will engender trust between NCSIRTs as well as among their constituents. Second, states must support NCSIRTs by enacting legislation that clearly defines the roles and responsibilities of the state, NCSIRTs and other CSIRTs in national incident preparedness and response. NCSIRTs in turn must cooperate with public authorities in effective incident response and capacity building, akin to the relationship between National Societies and states. Third, just as National Societies provide support to victims through national societies, the IC or the International Federation of Red Cross and Red Crescent Societies (IFRC), NCSIRTs must provide assistance to victims of incidents in the form of services and personnel, material and financial assistance and contribute to the community by assisting in the development of other NCSIRTs.[174]

171. IFRC HANDBOOK, *supra* note 143
172. *Id.* at 1220.
173. Skierka et al., *supra* note 4, at 22.
174. IFRC STATUTES, *supra* note 135, at 8.

In conclusion, the functions CSIRTs serve and the way they operate is not adequate to meet current cybersecurity challenges. Moreover, private entities do not provide a viable alternative. Thus, is it necessary to re-evaluate the functions and the way CSIRTs operate and adopt lessons where applicable in order to further their evolution and continuing relevance. Nevertheless, the key functions of components of the Movement and relationships provide viable lessons, provided that CSIRTs and other actors within this space are able to draw on them and adapt accordingly.

The Battle Against Breaches: A Call for Modernizing Federal Consumer Data Security Regulation

Alex Bossone *

TABLE OF CONTENTS

* J.D., The George Washington University Law School, May 2017. Senior Notes Editor, *Federal Communications Law Journal*, 2016–17.

I. INTRODUCTION

In the United States, the years 2013 and 2014 were marked by a series of high-profile data breaches that resulted in the theft of consumer payment information from various retailers' data systems. By May 2015, data breaches were on pace to cost roughly $70 billion annually[1] in the United States.[2] While not every consumer who had their personal information stolen incurred harm due to fraudulent charges or identity theft, many consumers have become wary of which companies they choose to do business with, and some have chosen to avoid using electronic payment methods that have been compromised by hacks.[3] Companies have also suffered losses as cyber-attacks have become increasingly frequent and costly.[4] The average data breach in 2015 cost $3.79 million for the victim company, eight percent more than the year prior, as negative publicity and expensive security measures take their toll on the bottom line.[5]

Consumers who are affected by breaches have turned to the courts for recourse, but federal circuit courts are split over when an individual may recover for a data breach claim. In *Remijas v. Neiman Marcus Group, LLC*, the United States Court of Appeals for the Seventh Circuit held that customers have Article III standing to seek relief against a company from which the customers' data was stolen, even where the data has not yet been harmfully used (for example, via fraudulent credit card charges).[6] In contrast, the Third Circuit held in *Reilly v. Ceridian Corporation* that data breach plaintiffs in a separate incident lacked Article III standing to recover where the alleged harm of an increased risk of identity theft from exposure of the data was deemed to be too hypothetical and incapable of being quantified.[7]

The circuit split highlights the inadequacy of available remedies for consumers in the event of a data breach, and the lack of a regulatory scheme that sufficiently reflects the increasing value of personal data. In contrast to many other countries that have specialized data privacy agencies (DPA) to administer a national regulatory framework for data privacy, the United States has designated the Federal Trade Commission (FTC) as its "de facto federal

1. This approximate number was reached by multiplying the per capita cost ($217) of domestic data breaches as of May, 2015 by the United States population as of January, 2015 (320 million). 2015 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 2, PONEMON INSTITUTE (2015), https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF.

2. Bill Hardekopf, *The Big Data Breaches of 2014*, FORBES, (Jan. 13, 2015, 7:16 PM), http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/#52151e823a48.

3. Brett Conradt, *Think Shoppers Forget Retail Data Breaches? Nope*, CNBC (June 22, 2015), http://www.cnbc.com/2015/06/22/think-shoppers-forget-retail-data-breaches-nope-commentary.html [https://perma.cc/EK5Y-Z2BX].

4. The average cost from lost business due to a breach was $1.57 million in 2015—up from $1.33 million the year prior. PONEMON INSTITUTE, *supra* note 1, at 2.

5. *Id.* at 1.

6. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693–95 (7th Cir. 2015).

7. Reilly v. Ceridian Corp., 664 F.3d 38 (3rd Cir. 2011).

DPA."[8] The FTC bases its data privacy authority on Section 5 of the FTC Act,[9] which establishes its power to guard against unfair or deceptive business practices. Other federal agencies claim narrower authority over the data practices of companies within their respective industries, with the Federal Communications Commission (FCC) pursuing enforcement actions over telecommunications and cable providers that suffer breaches.[10]

This Note will argue that Congress should augment the FTC's existing data security powers to preclude any challenges to the Commission's authority in that area, and to mandate a more effective framework by emulating the FCC Enforcement Bureau's approach. The Enforcement Bureau laid out its enforcement model in a 2015 data breach action that, for the first time, imposed specific technological requirements on a FCC licensee, in contrast to the FTC's approach of holding companies to a general "reasonableness" standard regarding data security practices.[11] The framework proposed in this Note would provide more specific guidelines to companies on how to keep their security practices up to date, and would provide incentives for businesses to follow the guidelines. The new regulations would also provide consumers with recourse in the event of a breach. As personal data becomes an increasingly valuable commodity, consumers face an unprecedented need for a reliable means of asserting their rights against the companies who profit from the use of data yet negligently handle it. As technology improves, data security systems will only become more complex, and hackers will only become more sophisticated. A new regulatory scheme addressing consumer data security requires specific solutions for businesses to ensure that data practices effectively keep pace with rapid technological developments and further integration of the Internet into individuals' daily lives. In addition, enforcement actions need to provide consumers with adequate remedies for the exposure of personal data, and should give businesses notice of the level of responsibility to which they will be held for failing to protect consumer data.

Accordingly, Part II of this Note will examine the circuit split over consumers' right of action in response to a breach, and will explore the FTC and FCC's roles in regulating the data security practices of U.S. businesses. Part III will discuss why the current regulatory framework for data security is insufficient to protect consumers from data breaches, and will outline what a new FTC regime of regulatory oversight based on the FCC's "specific

8. LEE A. BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 177 (1st ed. 2014).

9. 15 U.S.C. § 45(a) (2015).

10. *See, e.g.*, Cox Commc'ns, Inc., 30 FCC Rcd 12302 (2015); Terracom, Inc., & Yourtel Am., Inc., 30 FCC Rcd 7075 (2015).

11. *See* Cox Commc'ns Inc., 30 FCC Rcd 12302, 12310 (2015); *see also FCC Expands Its Claim of Data Security Authority with Recent Enforcement Action Against Cox Communications*, ROPES & GRAY (Nov. 12, 2015), https://www.ropesgray.com/newsroom/alerts/2015/November/FCC-Expands-its-Claim-of-Data-Security-Authority-with-Recent-Enforcement-Action.aspx [https://perma.cc/WW8Y-753F]; *Cox Commc'ns*, 2015 WL 6779864.

requirements" enforcement method might look like. Finally, Part IV will offer conclusions and a brief summary of the proposed legislation.

II. THE CURRENT LEGAL FRAMEWORK FOR DATA SECURITY IS NEBULOUS – BUT THE THREAT OF BREACH IS VERY REAL

The prevailing U.S. policy approach regarding consumer data security at both the federal and state levels can largely be described as "hands-off," especially when compared with the protectionist approaches of countries in the European Union (EU).[12] Until 2003, when California passed the first state law requiring entities to notify individuals whose personal data have been compromised by a breach,[13] no government entity in the U.S. had undertaken broad legislative measures to protect data owners from third-party theft.[14] As for the establishment of a comprehensive regulatory scheme that covers both data privacy and protection, the EU has proved to be perhaps the most aggressive legislative body through its creation of the Data Protection Directive (DPD) in 1995.[15] The DPD, which is binding on all EU member states, establishes personal data protection as a "fundamental [human] right," and requires each EU member to create its own independent Data Protection Agency (DPA) to oversee and enforce domestic data security regulations.[16]

In contrast, the U.S. has designated the FTC as its own "de facto federal DPA," pursuant to the FTC's enforcement powers under Section 5 of the FTC Act regarding "unfair or deceptive business practices."[17] The FTC has also utilized a number of federal statutes related to the protection of very specific kinds of personal data.[18] Despite the FTC's recently expanded role in regulating data security practices, "its field of competence is more restricted than is typical for European DPAs."[19] One explanation for this divergence in policy approaches may be that U.S. corporations like Google and Facebook have lobbied for data legislation in the U.S. that EU authorities have viewed as insufficient to satisfy their own fundamentally held principle of data protection as a human right.[20] As the current data security paradigm stands in the U.S., the FTC has not been able to provide recourse for individual consumers who have had personal data stolen via increasingly costly retail

12. LOTHAR DETERMANN, DETERMANN'S FIELD GUIDE TO INTERNATIONAL DATA PRIVACY LAW COMPLIANCE xv (2012).

13. California's first attempt was contained in Cal. S.B. 1386, an amendment to Cal. Civ. Code § 1798.29.

14. *See* DETERMANN, *supra* note 12, at xiv ("[M]ost U.S. states and many countries [followed California's example]."); *see also* Getting it Right on Data Security and Breach Notification Legislation in the 114th Congress, (Hearing), 33 (2015).

15. DANIEL J. SOLOVE, INFORMATION PRIVACY LAW 53–54 (5th ed. 2015).

16. *Id.* at 59–60, 170.

17. *Id.* at 177–78.

18. *Id.* at 177–78; *see also* Fair Credit Reporting Act, 15 U.S.C. § 1641 (1970); Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998); Financial Services Modernization Act, Pub. L. 106–102 (1999).

19. SOLOVE, *supra* note 15, at 177.

20. *Id.* at 107.

data breaches, leaving them to fend for themselves in the courts – with varying measures of success.[21]

This section will first explore how courts have struggled to fully appreciate the harm that a data breach causes the affected consumers, especially in cases where the victims do not suffer immediate financial costs. Next, this section will discuss the FTC's vague "reasonableness" standard for commercial data security practices and will argue that the standard fails to adequately promote best practices among companies that handle consumer data. Finally, an examination of the FCC's more focused regulatory approach will follow, before moving on to a discussion of the proposed legislation.

A. U.S. Federal Circuits Are Divided on an Individual Right of Action in the Event of a Breach

The U.S. judicial system is ill suited to address the pressing need for a federal legal standard on consumer data security, as it lacks expertise and clear statutory guidance in that area. The split between the Third and Seventh Circuits is an example that some courts do not yet understand the increasingly high value of personal data and the harmful impact of breaches. [22] While many U.S. consumers have been left without a remedy for stolen personal data, the Seventh Circuit in *Remijas* recognized the cognizable harm that a retail data breach poses to the affected consumers, even where the precise level of financial harm cannot be calculated.[23] In 2014, a number of customers at Neiman Marcus brought a consolidated action against the retailer for a data breach that exposed approximately 350,000 credit card numbers, 9,200 of which were subsequently used to make fraudulent purchases.[24] Though the plaintiffs conceded that they were reimbursed by Neiman Marcus for the fraudulent charges, they argued successfully that they had incurred redressable harm in the form of: (1) mitigation expenses (the time and money lost resolving the stolen data issue and protecting themselves from future fraudulent charges or identity theft) and (2) future harm (the threat of potentially harmful uses of the stolen data at an unknown future time).[25]

In attempting to downplay the adverse impact of the breach on consumers, Neiman Marcus argued the Supreme Court's decision in *Clapper v. Amnesty International USA*[26] was controlling. The retailer contended that the plaintiffs did not have Article III standing to bring the future harm or mitigation cost claims because *Clapper* required that allegations of future harm be "'certainly impending' [to be deemed an injury-in-fact, while mere] 'allegations of possible future injury are not sufficient.'"[27] However, the

21. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015*);* Reilly v. Ceridian Corp., 664 F.3d 38 (3rd Cir. 2011).

22. *Compare*, Clapper v. Amnesty International USA et al., 133 S. Ct. 1138 (2013), *with* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015), *and Reilly*, 664 F.3d 38.

23. *Remijas*, 794 F.3d at 693.

24. *Id.* at 690.

25. *Id.* at 692.

26. *See generally Clapper*, 133 S. Ct. 1138.

27. *Remijas*, 794 F.3d at 692 (citing *Clapper*, 133 S. Ct. at 1147).

Seventh Circuit found *Clapper* to be distinguishable from the case at hand because *Clapper* involved the *alleged* or *speculative* interception of communications data instead of the *actual*, *undisputed* theft of individual consumer data that occurred in *Remijas*.[28] Further, the court drew from *Clapper* a test for whether plaintiffs have standing to recover for future harm. In other words, there must be a "'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm."[29] Ultimately, the Seventh Circuit determined that the plaintiffs *did* face a "substantial risk" that some future harm would occur from the breach and therefore found that the plaintiffs had Article III standing.[30]

The *Remijas* holding represents a step in the right direction for the adjudication of data breaches, but there the Seventh Circuit did not quite demonstrate a full understanding of the concrete economic value that personal data holds. The Court correctly recognized that the harm caused by a breach does not only manifest itself in the actual, illicit use of the stolen data; instead, any breach or exposure of such data instantaneously results in a reasonably imminent loss of value for the individual victim.[31] As the court put it: "[w]hy else would hackers break into a store's database and steal consumers' private information" if that data did not hold any value to them?[32] However, the court narrowly interpreted that notion of personal data having an inherent value when the it declined to allow recovery for the breach as a "concrete injury" on the same level as theft of physical property.[33] Essentially, and somewhat paradoxically, the court seemed to reason that even though personal data can be used to financially benefit hackers at the victim's expense, that data does not grant the original owner any positive economic value that can be lost if the data is stolen.[34] Finally, the court reasoned that if potential data breach plaintiffs are forced to wait until fraudulent charges are made on their card or until their identity is stolen before bringing a claim, then the interim period of time would only leave more room (perhaps unjustifiably) for the defendant to argue that the plaintiff incurred harm due to a reason other than the breach.[35]

In its petition for *en banc* review to the Seventh Circuit, Neiman Marcus argued that there was a circuit split with regard to Article III standing, as evidenced by the Third Circuit's decision in *Reilly v. Ceridian Corporation*.[36] In Reilly, the court "held that an increased risk of identity theft from a payroll database breach doesn't satisfy Article III's injury-in-fact

28. *Id.* at 693 (emphasis added).
29. *Id.* (citing *Clapper*, 133 S. Ct. at 1150 n.5).
30. *See id.* at 693–4.
31. *See id.* at 694 ("[O]nce stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years." (quoting U.S. Gov't Accountability Office, GAO-07-737, report to Congressional Requesters: Personal Information 29 (2007))).
32. *Id.*at 693.
33. *Id.*at 695 ("Plaintiffs refer us to no authority that would support such a finding. We thus refrain from supporting standing on such an abstract injury, particularly since the complaint does not suggest that the plaintiffs could sell their personal information for value.").
34. *See id.* at 696.
35. *Id.*at 693; *see also* Adobe Sys., 66 F. Supp. 3d 1197, 2014 WL 4379916, at *8 n.5.
36. Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011).

requirements."[37] The Third Circuit then denied the appellants Article III standing on the following grounds:

> Appellants' contentions rely on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names. Unless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm.[38]

Though the facts in *Reilly* are different from in *Remijas* – *Reilly* involves purely speculative harm that might result from the breach while *Remijas* saw *some* actual harmful use of the exposed data (fraudulent charges on some of the cards) – the contrasting holdings reflect that the Seventh and Third Circuits disagree on one key point. As the Seventh Circuit pointed out in *Remijas*, the hackers would not have expended the effort to illegally access Neiman Marcus' data systems if not to derive some benefit or value from the personal data contained therein; thus, the potential for easily inflicted harm by the hacker(s) against the affected consumers was enough of an imminent threat to confer standing.[39] The Third Circuit in *Reilly* did not require a showing that the appellants' exposed data had been harmfully used to determine whether personal data has an inherent value; instead, the Court took a firm stance that there must be clear evidence the hacker physically looked at the exposed personal data (rather than merely accessing the system) for the harm to be sufficiently imminent.[40] The circuit split is evidence that courts, consumers, and data-collecting entities (retailers or otherwise) are all in need of some clarity regarding how the harm from a personal data breach should be legally assessed. Given the border-blurring nature of the Internet and the fact that hackers operate across state and national lines, an inconsistent approach among federal circuit courts on the issue of data breaches and the remedies provided to the individuals affected is no longer tolerable nor feasible.

B. The FTC's Vague Role as the Unofficial U.S. Data Protection Agency

The FTC holds the primary data security regulation and enforcement authority over U.S. companies, pursuant to its stated goal to prevent "deceptive" or "unfair" practices that are "in or affecting commerce" under

37. *See* Remijas v. Neiman Marcus Grp., 794 F.3d 688 (2015); *see also* Joey Godoy, *7th Circ. Won't Revisit Neiman Marcus Data Breach Ruling*, LAW360 (Sep. 17, 2015), http://www.law360.com/articles/704243/7th-circ-won-t-revisit-neiman-marcus-data-breach-ruling.

38. *Reilly*, 664 F.3d at 42.

39. *See Remijas*, 794 F.3d at 693.

40. *See Reilly*, 664 F.3d at 42.

Section 5 of the FTC Act.[41] Since 2002, the Commission "has brought more than 50 enforcement actions against companies that have engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk"– seven of those actions came in 2014 alone.[42] Some of these actions under the "deceptive" prong were taken against companies that were found to have misrepresented to consumers how the company plans to use their personal data,[43] while others were taken against companies that were found to have misrepresented the level of security of their data systems.[44] Some within the FTC claim that Section 5 is poorly suited for data security regulation, arguing that the "deceptive" acts authority unduly narrows the FTC's jurisdiction to instances where companies violate their own stated data security policies rather than where they violate a general legal standard.[45]

However, since the turn of the twenty-first century, the FTC has pursued a number of enforcement actions under its "unfair" acts authority under Section 5 that have supported a stronger – but still debated – claim to regulate the data security practices of companies generally.[46] For the data security actions that are broader in scope than those brought strictly under the "deceptive" prong of Section 5, a company's act is deemed "unfair" under a three-part test[47] if it "[(1)] causes or is likely to cause substantial injury to consumers [(2)] which is not reasonably avoidable by consumers themselves and [(3)] not outweighed by countervailing benefits to consumers or competition."[48] In addition to the FTC Act, more recent federal statutes such as the Fair Credit Reporting Act (FCRA), the Children's Online Privacy Protection Act (COPPA), and the Gramm-Leach-Bliley Act (GLBA) all grant the FTC affirmative data security authority in very specific areas – but this still means that in most industries, data security practices are only covered under Section 5's "deceptive" or "unfair" acts provisions.[49]

As far as the specific data security practices that companies are obligated to follow, the FTC has a flexible standard that requires businesses to undertake "reasonable" measures to keep consumer data secure.[50] This

41. 15 U.S.C. § 45(b) (2015).

42. FED. TRADE COMM'N, *2014 Privacy and Data Security Update* 5 (2014).

43. *See* FED. TRADE COMM'N, OFFICE OF PUB. AFF., *FTC Approves Final Order Setting Charges Against Snapchat* (Dec. 31, 2014).

44. *See FTC 2014 Privacy and Data Security Update* at 5.

45. Jeffrey Benner, *FTC Powerless to Protect Privacy*, WIRED (May 31, 2001), http://archive.wired.com/politics/security/news/2001/05/44173 (quoting Lee Peeler, former Associate Director of Advertising Practices at the FTC).

46. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 614–15 (D.N.J. 2014).

47. The Third Circuit was uncertain whether all three factors *must* be met to constitute an "unfair" act, or if they are instead merely sufficient conditions. *See* FTC v. Wyndham Worldwide Corp,, 799 F.3d 236, 244, 259 (3rd Cir. 2015).

48. 15 U.S.C. § 45(n) (2015).

49. Fair Credit Reporting Act, 15 U.S.C. § 1641 (1970) (regulating the use of consumer data by consumer reporting institutions); Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998) (regulating the use of data belonging to children under age thirteen); Gramm-Leach-Bliley Act, 15 U.S.C. § 6801(b) (regulating the use of consumer data in the hands of financial institutions); 15 U.S.C. § 45.

50. *See* Jessica Rich, Data Security: Why It's Important, What the FTC is Doing About It, FTC, 4 (Mar. 24, 2014), https://www.ftc.gov/system/files/documents/public_statements/295751/140324nclremarks.pdf, [https://perma.cc/KRE3-GSEQ].

"reasonableness" standard is grounded in the idea that "security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurs does not mean that a company has violated the law."[51] Factors that the FTC takes into account when making a reasonableness determination include "the sensitivity and volume of consumer information [the company] holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[52] Although the FTC does provide some guidance on what constitutes reasonable data security practices, a bright-line rule that explicitly defines the "reasonableness" standard for companies to meet in order to avoid liability remains elusive.[53]

The FTC's interpretation of Section 5 as granting authority to regulate data security in commerce has not gone unchallenged.[54] In a recent data breach action against the Wyndham Worldwide hotel chain, the Third Circuit, on appeal from the United States District Court for the District of New Jersey, upheld the FTC's Section 5 authority over "unfair" data security practices after Wyndham claimed that such authority was an overextension of the FTC's congressionally granted powers.[55] *Wyndham* can be cited as a particularly egregious instance of a businesses' failure to take reasonable data security measures, as the company allowed hackers to steal hundreds of thousands of customers' personal and financial information over three separate instances, resulting in more than $10.6 million in fraudulent charges.[56] The FTC based its action on the ground that Wyndham did not take basic steps to protect its customers' data, and did not take preventative measures after the first breach, even though hackers used similar methods in the subsequent attacks.[57] When the FTC initially sued Wyndham in District Court, that court found Wyndham had committed a Section 5 "deceptive" acts violation by overstating its cybersecurity in a policy statement online.[58]

On appeal to the Third Circuit, Wyndham conceded the "deceptive" acts issue, but challenged the FTC's authority to bring a separate "unfairness" claim relating to the substance of the hotel chain's data security practices that led to the breaches.[59] Wyndham argued that Congress did not intend for Section 5 "unfair" act powers to grant the FTC any jurisdiction over data security, taking the position that the specific grants of data security jurisdiction under the FCRA, COPPA, and GLB would have been futile if the

51. *Id.*

52. *Commission Statement Marking the FTC's 50th Data Security Settlement*, FTC, 1 (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf, [https://perma.cc/P9NS-P6Y3].

53. *See generally Start with Security: Lessons Learned From FTC Cases*, FTC (Jun. 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business, [https://perma.cc/LF7T-DT2N].

54. *See* generally FTC v. Wyndham Worldwide Corp*.,* 799 F.3d 236 (3d. Cir. 2015).

55. *Id. See generally Start with Security: Lessons Learned From FTC Cases*

56. *See Id.* at 241-42.

57. *See Id.* at 241.

58. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d. 602, 626-28 (D.N.J. 2014).

59. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d. 602, 614 (D.N.J. 2014).

FTC had universal data security authority to begin with.[60] The Third Circuit rejected that argument on the ground that the newer acts *required*, rather than merely authorized, the FTC to regulate data security in their respective areas.[61] Furthermore, the statutes reduced some of the jurisdictional hurdles for the FTC to declare information security practices "unfair" in the covered industries, meaning that the newer statutes expanded, rather than proscribed, the FTC's existing data security authority under Section 5.[62]

The Third Circuit ultimately held that the FTC currently *does* have Section 5 authority over "unfair" data practices at least to some degree, but the ad hoc manner in which the Court interpreted the statutory application of "unfair" in regard to Wyndham's conduct provides little instructive value for future breach cases where businesses are not so plainly negligent.[63] The *Wyndham* holding thus illustrates a troublesome picture – both for the FTC, which lacks a solid legislative footing to define the legitimate scope of its data security jurisdiction, and for businesses that are left with hazy guidelines on how to grapple with cybersecurity.[64] There remains uncertainty as to how the three-part "unfair" acts test defines what data security measures are necessary in practice for a company to avoid an FTC action.[65] This ambiguity is especially apparent in more borderline breach cases where companies are not so plainly negligent, and cases where there has not been a "deceptive" misrepresentation by the company.[66]

In attempting to apply the three-part test, the Third Circuit problematically left open the possibility that the FTC's "unfair" acts authority is in fact entirely superfluous in the context of breaches. This suggests that the exceptionally narrow "deceptive" acts authority granted by Section 5 may provide the FTC's only vessel, however inoperable, for pioneering the uncharted jurisdictional void that data security presents.[67] The opinion did not conclude whether Section 5 required all three conditions to be met in order to declare an act "unfair," and the case was decided on the ground that Wyndham's conduct could not be shown to fall outside the ordinary meaning of "unfair."[68] The Court easily concluded that the breach exposed Wyndham's customers to the likelihood of substantial injury, as the first part of the Section 5 test requires.[69] For the second prong, which asks whether the injury was "reasonably avoidable by [the] consumers," the Court reasoned that Wyndham's misleading security policy plausibly could have prevented customers from avoiding the breach, and no alternative means of satisfying that inquiry were considered.[70] This is highly problematic as it suggests that a "deceptive" act may be *required* in order to meet the "unfair" act test for

60. *Id.* at 612–13.
61. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 248 (3d Cir. 2015).
62. *Id.* at 248.
63. *See id.* at 258–59.
64. *See id.*
65. *See id.* at 258–59.
66. *See id.* at 245, 259 ("The three requirements in § 45(n) [(for unfair acts)] may be necessary rather than sufficient conditions of an unfair practice").
67. *See id.* at 245–46.
68. *See id.*
69. *Id.* at 245.
70. *Id.* at 245–46.

breaches, meaning the FTC's ostensibly broader "unfair" acts jurisdiction may be inseparable from the deception prong in consumer data breach cases. Unless there is conduct other than a company's *misrepresentation* that may satisfy the "reasonably avoidable" injury test, the FTC may be unable to use its "unfair" acts authority to pursue a data breach action outside the restrictive confines of its "deceptive" acts authority.[71]

While the second prong of the "unfair" acts test threatens to potentially narrow the scope of the FTC's jurisdiction, the third and final part further muddies the waters on a data security regulatory standard. The Court interpreted the third inquiry of whether the potential injury is "outweighed by countervailing benefits to consumers or to competition," as requiring a cost-benefit analysis between the heightened costs of various security measures as passed on to consumers and the risk of harm from breach.[72] This cost-benefit analysis was applied to examine Wyndham's security procedures in order to decide the merits of the hotel's separate claim that the FTC violated due process.[73] Wyndham contended that the FTC did not provide adequate notice as to what specific security measures are required to meet the "reasonableness" standard.[74] The Court, however, pointed to numerous FTC guidelines, publications and previous enforcement actions as providing a general idea of what data security measures a company can reasonably take, none of which Wyndham attempted to follow.[75] Though the Court found that Wyndham clearly failed to satisfy this third inquiry, it acknowledged that "there will be borderline cases where it is unclear if a particular company's conduct falls below the legal threshold," implying that companies may not have a precise means of determining what conduct the Third Circuit's cost-benefit analysis requires.[76] Essentially, the Court deferred to the FTC's "reasonableness" standard for company data practices, but it declined to explore the issue of whether or where a line for "reasonableness" can truly be drawn. Because the FTC has been left with the unwieldy Section 5 as its only statutory tool to craft a necessarily-sophisticated data security legal framework for all industries, concrete clarification of the "reasonableness" standard in *Wyndham* was forcibly set aside by the preliminary question of whether the FTC has data security authority in the first place. *Wyndham*, at a minimum, established that the FTC has jurisdiction over at least *some* companies that suffer breaches, but the holding should not give consumers much confidence that the FTC is currently in the position to elucidate and administer a regulatory regime that effectively safeguards personal data.

71. *See id.*
72. *Id.* at 255.
73. *Id.*
74. *Id.*
75. *Id.* at 256–57.
76. *Id.* at 256.

The FTC's heavy dependence on its decades-old authority to regulate "deceptive" or "unfair" practices as a jurisdictional hook[77] in data breach actions indicates that data security is thus far a legislative afterthought in the U.S., despite the reality that data security is a modern concern of paramount importance in all areas of commerce.[78] *Wyndham* demonstrates that although the FTC can assert a facially broad claim to regulate "unfair" data security practices, the one-size-fits-all nature of Section 5 may mean that for breaches, a "deceptive" act is required to satisfy the "unfair" act test.[79] This is problematic when compared with the Seventh Circuit's holding in *Remijas*, which arguably suggests that there is (or should be) an *implied* understanding that a company is undertaking adequate steps to protect consumer data in the course of business.[80] Thus, any *express* claims made by the company as to its proficiency in data security should be irrelevant. The FTC, in lacking an explicit grant of jurisdiction from Congress over data security, could be needlessly restricted only to pursuing companies that suffer data breaches *and* have explicitly misrepresented the security of their data systems.[81] Based on the somewhat contradictory opinions federal courts have handed down, it is evident that companies are in need of clearer guidance on how to properly secure their data systems, and that consumers could benefit from a more developed statutory framework.

C. The FCC is Expanding its Role in Data Security Regulation, and is Taking a More Focused Approach Than the FTC

Historically, the FCC has regulated the data security practices of telecommunications providers under interpretations of Sections 201(b), 222(a) and (c) of the Communications Act of 1934, in a manner that is similar to the FTC's "reasonable" practices standard.[82] Specifically, in a 2014 action against TerraCom and YourTel, two telecommunications companies who failed to protect the personal information of more than 300,000 customers, the FCC Enforcement Bureau reasoned that the language of Section 201(b), referring to "reasonable" practices, created an enforceable duty to protect

77. *See, e.g.*, Credit Karma, Inc., No. C-4480 (F.T.C. Aug. 13, 2014) (consent order), available at https://perma.cc/G5RM-M2UMhttp://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc; Fandango, LLC, No. C-4481 (F.T.C. Aug. 13, 2014) (consent order), available at https://perma.cc/W65Y-BVPRhttp://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc; TRENDnet, Inc., No. C-4426 (F.T.C. Jan. 16, 2014) (consent order), available at https://perma.cc/F4RL-Q4GUhttp://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.

78. *Discussion Draft of H.R.__, Data Security and Breach Notification Act of 2015: Hearing Before the H. Comm. on Energy & Commerce, Subcomm. On Commerce, Mfg., & Trade*, 114th Cong. 1–2 (2014) (statement of Jessica Rich, Dir. Bureau of Consumer Prot. at the FTC).

79. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 245–46 (3d Cir. 2015).

80. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).

81. 15 U.S.C. § 41 (2012).

82. 47 U.S.C. §§ 201(b), 222(a), (c) (2012); *see also* Terracom, Inc., & Yourtel Am., Inc., *order*, 30 FCC Rcd 7075 (2015).

such personal data from unauthorized access or use.[83] Section 222(a) affirmatively imposes a duty on telecommunications providers "to protect the confidentiality of proprietary information [(PI)] of, and relating to … customers,"[84] while Section 222(c) limits the use of customer proprietary network information (CPNI) collected incidentally during the provision of telecommunications services to reasonable uses.[85] All enforcement actions taken by the FCC, pursuant to Sections 201(b) and 222(a) and (c), against telecommunications providers have involved incidents where customers' information was either accessed unlawfully by company personnel or was placed in a publicly accessible folder on the Internet.[86]

In 2015, the FCC sought to expand its data security regulatory authority to cable providers by pursuing a data breach action against Cox Communications.[87] The FCC Enforcement Bureau utilized Section 631 of the Communications Act, which regulates cable providers, to issue an order and consent decree after Cox lost its customers' personal information in a breach.[88] The relevant portion of Section 631(c) provides that a cable operator:

> [S]hall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator.[89]

Since Cox is a provider of broadband and telecommunications services, in addition to cable, the Enforcement Bureau additionally determined that Sections 201 and 222 of the Communications Act also should apply.[90]

The primary focus of the Enforcement Bureau's order was to prevent further security lapses of the specific type that Cox suffered in the present instance.[91] The breach involved a hacker pretending to be a Cox employee, who then convinced a legitimate employee of the telecommunications provider to enter her internal account ID and password into a fake website controlled by the hacker, an activity known as "phishing," who then was able to access Cox's data systems.[92] According to the Enforcement Bureau, "at the time of the breach, Cox employed multi-factor authentication for some

83. 47 U.S.C. § 201(b) (2012) ("[a]ll charges, practices, classifications, and regulations for and in connection with [[interstate or foreign] communication service [by wire or radio], shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful").
84. 47 U.S.C. § 222(a) (2012).
85. 47 U.S.C. § 222(c) (2012).
86. *See, e.g.,* Terracom, Inc., & Yourtel Am., Inc., *order*, 30 FCC Rcd 7075, 7081 (2015).
87. *See* Cox Commc'ns, Inc., *order*, 30 FCC Rcd 12302 (2015).
88. *See id.* at 12307; *see also* ROPES & GRAY, *supra* note 11.
89. 47 U.S.C.A. § 551(c)(1) (2012).
90. Cox, 30 FCC Rcd at 12307–08.
91. *Id*. at 12304.
92. *Id.* at 12308.

employees and third party contractors with access to Cox electronic data systems, but not for the compromised employee or contractor."[93] As a result, one of the specific requirements that the Enforcement Bureau imposed on Cox was to implement a standard system whereby the company takes targeted steps to ensure the security and authenticity of communications among Cox employees and third parties contractors.[94]

The FCC's pursuit of a breach action against a cable provider was a novel practice for the agency, but the biggest departure from its previous actions was the uniquely tailored remedy the agency sought to enforce on Cox. In lieu of ordering Cox to comply with the general "reasonable" practices standard, the Enforcement Bureau proposed a number of specific requirements as part of an overall "compliance plan."[95] Included in the compliance plan was a risk assessment program that is consistent with the National Institute of Standards and Technology's (NIST) Cybersecurity Framework,[96] designed to evaluate internal and external security threats and requiring a biennial report of its findings to the FCC.[97] Also included was a comprehensive information security program that documents who is given access to customers' propriety network information (CPNI), establishes safeguards to prevent unauthorized access or use of that data, and outlines sanctions for parties who disregard the guidelines set out in the program.[98] Additionally, the consent decree requires annual audits and periodic penetration testing of Cox's security systems, as well as the use of a site-to-site virtual private network (VPN) for use by third-party vendors who must access customer data in the course of business with Cox, among other procedures.[99] Cox also would be required to designate a compliance officer with senior management authority in its corporate structure, with the role of ensuring that Cox follows through with the compliance plan and consent decree.[100]

Following the enforcement approach of the *Cox* order, on October 27, 2016, the FCC adopted an order that granted the agency authority to regulate the data security practices of broadband and other telecommunications service providers.[101] The Privacy Order affirmed the need for clearer data privacy laws, and established a focus on transparency in data collection, consumer choice, and the maintenance of secure data systems as three crucial

93. *Id.* at 12309.

94. *Id.* at 12311.

95. *Id*. at 12310–16.

96. NAT'L INST. OF STANDARDS & TECH., *Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. OF STANDARDS & TECH. (Feb. 12, 2014), available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, [https://perma.cc/6VKA-64ZJ].

97. Cox, 30 FCC Rcd at 12310.

98. *Id.*

99. NAT'L INST. OF STANDARDS & TECH., *supra* note 96. Cox, 30 FCC Rcd at 12310 (pg. 8)

100. Cox, 30 FCC Rcd*Id.* at 12310.

101. In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Report and Order*, FCC-16-148, para. 5 (2016), https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1_Rcd.pdf [https://perma.cc/W27E-WGLF], [hereinafter *Privacy Order*].

components of a viable legal framework.[102] The issues relating to transparency and choice, specifically regarding what types of data may be collected and what options consumers should have in permitting or refusing collection of their personal data, deal more with privacy than security. Policymaking over data privacy has generated its own debate that is separate from data security, despite the issues being intertwined.[103] Privacy concerns are thus related to the data collection process, while security concerns arise once a company is in possession of consumer data.

In addressing data security, the Privacy Order took a step back from the type of specific requirements imposed by the Enforcement Bureau in the 2015 order against Cox, and instead adopted a more general "reasonableness" approach similar to that of the FTC.[104] The lack of rigidity in the Privacy Order's security proposal stems from a concern that overly-detailed and inflexible guidelines could prove unsuited for keeping pace with technological advances, may unfairly burden smaller companies, or could reduce incentives for innovation and competition in developing security techniques.[105] It remains contentious whether or not a one-size-fits-all procedural standard could prove to be obstructive for companies with fewer resources to put toward new security measures.[106] The concern was that a comprehensive set of specific guidelines may be well-suited for larger carriers, but could present unnecessary costs for smaller providers.[107] Finally, the Privacy Order contemplated, but explicitly stopped short of implementing, safe harbors for companies that follow a predetermined set of "best practices" in data security and nonetheless suffer a breach. The rationale for refusing to implement safe harbors was that rigid adherence to an inflexible list of "best practices" would restrict the "reasonableness" standard from keeping pace with technological developments.[108] Though the Privacy Order was later overturned on April 3, 2017[109], it appears that legislators are reluctant to move away from the FTC's imprecise "reasonableness" standard for data security regulation.

102. *See id.* at para. 3; *see also* Margaret Harding McGill, *FCC, FTC Zero in on Data Security, Privacy*, LAW360 (Jan. 6, 2016, 8:27 PM EST), http://www.law360.com/articles/743314/fcc-ftc-chiefs-zero-in-on-data-security-privacy, at 2.

103. *See* Natasha Lomas, *FCC Urged to Rein in Broadband Providers on Privacy Grounds*, TECHCRUNCH, (Jan. 19, 2016), http://techcrunch.com/2016/01/19/fcc-urged-to-rein-in-broadband-providers-on-privacy-grounds/./, [https://perma.cc/CH8Z-W43S], at 1.

104. *See Privacy Order* at para. 236.

105. *See id.* at para. 235.

106. *See id.* at para. 241-42.

107. *See id.*

108. *See id.* at para. 249.

109. S.J. Res. 34, 115th Cong. (2017).

III. THE FTC SHOULD MOVE FORWARD WITH A SPECIFIC REQUIREMENTS ENFORCEMENT MODEL SIMILAR TO THE FCC'S APPROACH DEMONSTRATED IN *COX*

A legislative overhaul is sorely needed to fully address the modern importance of consumer data – not only as a preventative measure to abate the economic harms caused by breaches, but also to more effectively protect consumers who are directly affected by the exposure of their personal information. Currently, the FTC has rooted its data security enforcement authority (for industries not covered by the FCRA, COPPA, and GLBA) in Section 5 of the FTC Act, which makes no specific mention of consumer data.[110] The FTC has undertaken thorough efforts to provide businesses and consumers with up-to-date information on how to maintain effective data security practices.[111] However, given that the FTC's statutorily granted authority has left the agency with the vague "reasonableness" standard for investigating data breach cases, companies are left guessing at how a court will rule if their data practices are brought under judicial scrutiny. Indeed, the FTC itself has recognized the need for new legislation in this area. For example, the FTC has proposed to Congress "a data security bill to establish broadly applicable data security standards for companies and [to] require them, in certain circumstances, to notify consumers in the event of a breach."[112] It is true that rapid notification to consumers in the event of a breach is imperative so measures can be taken to mitigate any harm after personal information has been exposed.[113] But the goal should be to create a legal framework that places an emphasis on preventing breaches in the first place.

A. The FTC Needs to Provide Businesses with More Clarity on What Data Security Practices to Adopt, and When a Breach Should be Actionable

The *Wyndham Worldwide* case demonstrated that, while the FTC is certainly willing and able to enforce its authority to regulate the data security practices of companies, businesses are currently left to sift through the body of data breach enforcement actions in order to figure out what the FTC's "reasonableness" standard truly requires. The mere fact that the Third Circuit in *Wyndham* recognized the potential for unresolvable "borderline cases" illustrates the need for a concrete code of conduct.[114] If companies are uncertain as to what constitutes "reasonable" data security practices, then it is possible they could overlook certain crucial security measures as not being

110. 15 U.S.C. § 45 (2012)..

111. *Discussion Draft of H.R.__, Data Security and Breach Notification Act of 2015: Hearing Before the H. Comm. on Energy & Commerce, Subcomm. On Commerce, Mfg., & Trade*, 114th Cong. 7–9 (2014) (statement of Jessica Rich, DirectorDir. of the Bureau of Consumer ProtectionProt. at the FTC).

112. *Id*. at 9.

113. *Id*. at 10.

114. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 256 (3d3rd Cir. 2015).

conclusively "required", thereby opening themselves up to breaches that could have been prevented had there been universally applied standards. Why leave open the possibility for these borderline cases to be picked apart by courts in *response* to harmful breaches when a viable alternative is to lay out a specific set of technical and procedural requirements that represents the cutting edge in protective measures?

Up until the FCC's Privacy Order, the Enforcement Bureau's specific-requirements approach[115] had provided companies under the FCC's purview with perhaps the clearest and most specific model for an up-to-date data security program.The requirements that the Enforcement Bureau imposed on Cox "[did] not appear to be limited to remediating the particular alleged deficiencies that the FCC contended led to the data security breach."[116] Instead, the consent decree outlined what the Enforcement Bureau determined was the most effective set of security measures that a company can take to prevent *any* form of data breach – not just the type that Cox suffered.[117] This forward-looking approach at the time provided a sustainable data security solution not only for Cox, but for *any* business that wished "to avoid running afoul of the Enforcement Bureau."[118]

It is important to note that the Enforcement Bureau did not go so far as to dictate every detail of the new security regime for Cox to follow. Instead, it left room for flexibility, as long as Cox met the specific goals outlined in the decree and documented its security procedures.[119] This provided a relatively non-intrusive middle ground between the imprecise "reasonableness" standard currently promulgated by the FTC and one that is so painstakingly specific and restrictive that it would restrain Cox from conducting business effectively. Finally, the requirement that Cox integrate a compliance officer into the company's senior management structure, with the role of overseeing execution of the consent decree, is significant because it incorporates data security implementation into the core operations of the company.[120] Hiring a compliance officer at a high-level position also provides flexibility for the company, as it leaves the day-to-day execution of the consent decree, and further matters of data security, in the hands of Cox's leadership instead of imposing an onerous system of FCC oversight.[121] The mandatory designation of this officer, along with the narrower technical requirements addressed toward curing the cause of the breach, makes the

115. *See* Patrick H. Haggerty, F. Paul Pittman, *FCC's Growing Privacy and Data Security Enforcement, Data Privacy Monitor* (Dec. 8, 2015), http://www.dataprivacymonitor.com/enforcement/fccs-growing-privacy-and-data-security-enforcement/, [https://perma.cc/TYA3-NCL9].

116. ROPES & GRAY, *supra* note 11; *see also* Cox Commc'ns, Inc., 30 FCC Rcd 12302, 12310 (2015) (the designation of a compliance officer was a more general security requirement imposed by the FCC that was not specifically related to the phishing scheme that caused Cox to suffer the data breach).

117. *See generally* Cox, 30 FCC Rcd at 12302.

118. Haggerty, *supra* note 115.

119. *See* Cox, 30 FCC Rcd at 12311.

120. *See id.* at 12310.

121. *See id.*

order a more lasting and effective enforcement model than a general requirement of "reasonable" data security practices.

A statutory solution for the FTC, modeled after the Enforcement Bureau's approach in *Cox*, would be to enact a statute granting the FTC affirmative authority to regulate the data security practices of businesses in the U.S. generally, and granting the same to specialized agencies like the FCC. The new statute would (1) establish the FTC as the official U.S. DPA (while granting other agencies like the FCC affirmative data protection authority in their respective industries); (2) require the FTC to publish an annual list of guidelines that represent the most up-to-date security measures; (3) mandate the implementation of a safe harbor from breach actions for companies that follow the FTC's annual data security guidelines; (4) provide for a six-month grace period for companies to adapt to newly-published guidelines while remaining inside the safe harbor; and (5) form a system for adequately compensating consumers who fall victim to data breaches, either by requiring companies to pay victims directly, or by establishing a victims' fund that can be paid out of the U.S. Treasury in an instance where the company falls within the safe harbor.

This new legal framework would help to eliminate the issue of notice criticized in *Wyndham* by allowing the FTC to establish a legitimate foundation as the undisputed authority in the realm of data security, rather than forcing the FTC to overextend its rudimentary Section 5 "deceptive" and "unfair" acts powers to fill a regulatory void. The proposed statute would not necessarily mandate specific data security measures for companies to follow, but would instead give legal effect to the FTC's determination of what constitutes the current best practices in data security. The FTC would be required to periodically update a core list of data security practices that represent the most innovative and current means of protecting consumers' personal information – much in the way that the agency already does of its own volition.[122] For industries that are regulated by a specialized agency, like telecommunications for example, the relevant agency would be allowed to add to or clarify the FTC's list of requirements, but could not waive any of the FTC's specifications absent a showing that a certain requirement that places an undue burden for that industry.

The goal would be for the FTC to effectively assume the role of a standard-setting body in consumer data security, as businesses would presumably want to earn the statute's legal benefits by keeping their data systems up to date with the FTC's guidance. A potential advantage of having at least a semi-standardized set of data security measures across all U.S. businesses would be that systemic flaws could be identified rapidly. If one company suffers a breach or encounters problems due to an issue with the prevailing data security paradigm, then every other business that has adopted the same security measures would be able to pool their intellectual resources into fixing the issue and strengthening the overall system. To account for the evolution of technology and increasing sophistication of hackers, the FTC

122. *See Start with Security: A Guide for Businesses*, FTC (June, 2015) https://perma.cc/P7YY-GQYKwww.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

would be required to update its data security guidance on a yearly basis, much like how the Enforcement Bureau sought to require Cox to submit risk assessment reports on its security measures at least every two years.[123] Any concern that a standard set of security guidelines would reduce competition and innovation[124] is without merit; the rising cost of breaches and persistent threat of hackers will naturally continue to provide a market-based incentive for companies to stay ahead of the curve in protecting consumer data.[125] Additionally, to avoid the issue of constantly requiring companies that had met the FTC data security certification benchmark in previous years to overhaul their systems, the statute would provide for a grace period of six months to a year during which businesses could have extra time to adopt any new standards before losing its certification. This period could be shortened if there is so drastic a change in the FTC's guidelines, due to a flaw, innovation, or otherwise, that the previous year's security paradigm has already become obsolete. The statute would give the FTC discretion over when this would be the case.

The central goals of this proposal are to improve data security in U.S. commerce generally, to prevent data breaches, and to protect the individual consumer. The time is ripe for a genuine and focused legislative effort that aims to put the U.S. ahead of the curve on data security, particularly in a time when consumers are taking data privacy concerns into serious consideration when deciding the companies with which to do business.[126]

B. Data Breach Remedies Should Include Recourse for Consumers Commensurate with the Modern Value of Personal Data

Even with a more robust data security framework in place for businesses, a further component is required to ensure that consumers can seek adequate remedies in the event of breach. The Seventh Circuit in *Remijas* recognized that assessing the harm caused to individual consumers who are affected by a data breach is difficult, especially when the personal information has not yet been used to their detriment.[127] While the plaintiffs in *Remijas* were able to recover against Neiman Marcus, both for damages incurred in trying to mitigate the harm caused by the breach as well as the for the risk of future harm,[128] the Court held that there could be no recovery for an injury in the abstract, "particularly since the complaint did not suggest that the plaintiffs could sell their personal information for value."[129] This seems to conflict with the Court's own statement when, in response to Neiman Marcus' assertion that a data breach did not constitute a substantial risk of future harm

123. *See* Cox Commc'ns, Inc., 30 FCC Rcd 12302, 12310 (2015).
124. *See Data Privacy NPRM* at para. 179.
125. *See 2015 Cost of Data Breach Study: Global Analysis*, Ponemon Institute, May 2015, at 2.
126. *See* Conradt, *supra* note 3, at 1.
127. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693–94 (7th Cir. 2015).
128. *Id.* at 693-95.
129. *Id.* at 695.

for those affected, it posed the rhetorical question: "[w]hy else would hackers break into a store's database and steal consumers' private information?"[130]

What the court failed to recognize in concluding that a data breach could not cause a harm to consumers other than through mitigation damages or future potential harm, is that personal data *does* carry an inherent value that the individual can monetize.[131] Consumers are already able to independently sell their personal information to companies that act as a middle-man for selling to data-collecting and processing entities and it is likely that these opportunities for consumers to "operate their own digital enterprises" will only become more numerous as awareness increases.[132] Thus, the loss of personal data can correspondingly constitute an economic loss if the original owner is no longer in control of it.[133] However, thus far, only a small number of people realize what monetary value their personal data holds.[134] Though Neiman Marcus, in its petition for *en banc* review, raised the issue of a potential split between the Seventh and Third Circuits,[135] the latter's holding in *Wyndham* indicates that the court agrees a data breach should be actionable even where no harmful use of the data has manifested.[136] Further, there is evidence that hackers will often wait before using any stolen data to commit fraud in order to avoid detection.[137] This suggests that even absent immediate harm caused to consumers affected by a breach, there is still a very substantial threat that some harm will manifest at some unknown point in the future.

Should the FTC develop a sustainable regulatory framework to handle the data security practices of companies across the U.S., it must, in an effort to protect the interests of consumers who suffer the effects of a data breach, integrate remedies into the framework that fully reflect the loss of economic value caused by a breach. Given that consumers are becoming more aware of personal data's inherent value and the increasing means by which personal data can be put to use for the individual,[138] a set of private remedies that the FTC could choose to update over time would conceivably work well to empower consumers with more control over their information in the marketplace. While these remedies could remain flexible under the discretion

---

130. *Id.* at 693.

131. *See* Tim Cooper & Ryan LaSalle, Guarding and Growing Personal Data Value, Accenture (2016) at 14.

132. *See id.* at 14 ("As individuals become more aware of the potential to monetize their data—and as channels for doing so become more accessible—they will be able to operate as their own digital enterprises, treating their data as a business would manage its intellectual property. For example, intermediaries … enable users to sell their data by connecting their social media and debit and credit card accounts to businesses that want to gather quality data about their target customers").

133. *See id.* at 14.

134. *See id.* at 14.

135. Joey Godoy, *7th Circ. Won't Revisit Neiman Marcus Data Breach Ruling*, LAW360 (Sept.Sep 17, 2015, 5:29 PM EDT), http://www.law360.com/articles/704243/7th-circ-won-t-revisit-neiman-marcus-data-breach-ruling.

136. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 246 (3d Cir. 2015).

137. Matthew Goldstein & Nicole Perlroth, *Authorities Closing in on Hackers Who Stole from JPMorgan Chase*, N.Y. TIMES (Mar. 15, 2015), http://www.nytimes.com/2015/03/16/business/dealbook/authorities-closing-in-on-hackers-who-stole-data-from-jpmorgan-chase.html?_r=0, [https://perma.cc/BP5B-QE86].

138. *See* Cooper & LaSalle, *supra* note 131, at 14.

of the FTC, there are several possible options that could also work from the outset.

The best method of compensating consumers whose personal data has been breached would be to pay out monetary damages for the immediate harm, and to provide services that mitigate potential future harm from illicit use of the data. An effective solution to calculate the monetary damages would be to fine companies at a rate corresponding to the volume and value of data lost, paid into a fund to be distributed among the affected consumers. For example, if a retailer suffers a breach, the compensation would be greater for financial and personally identifiable information, like credit card numbers, names, and addresses, than it would be for data that cannot directly be used to commit identity theft, like shopping history. Exact valuation may be difficult to calculate, though the existing market for consumer data bought and sold among companies could serve as a viable reference point.[139] A more punitive method would be to fine the liable company in the same way as previously discussed, except by calculating the damages as a percentage of profit that was realized by the company. The rationale behind this would be that the company charged its customers a premium for its goods and services yet chose not utilize those funds towards providing adequate data security measures (a rationale for damages raised and ultimately rejected by the court in *Remijas*).[140] Applying this method to the above example, the retailer would pay a percentage of the total profits made from its transactions with the specific customers who fell victim to the breach. The method that fines companies according to the value of data lost is the preferable choice, as it directly corresponds with the actual damages. The profit-based method, on the other hand, may produce unfair results if one company dealing in luxury goods has to pay a much greater fine than a company dealing in less expensive goods, even though the two suffer a breach of the same severity from the customers' standpoint.

In addition to applying monetary damages to account for the calculable losses from a breach, further redress should include equitable relief to compensate for the increased vulnerability of data theft victims. To address the threat of future harm faced by a consumer who has lost personal data, the company should pay for an identity protection or credit monitoring service. Neiman Marcus recognized the need to mitigate such future harm as it provided credit monitoring services to its customers after the breach, and before the class action suit went to trial.[141] This form of amends would ideally maintain or restore consumer confidence in the security of the market moving forward, in addition to purely rectifying the immediate economic harms caused by a given breach.

---

139. *See id.* at 8 (42% of the businesses currently gather personal data through commercial or data-sharing agreement with other organizations; 33% of the businesses currently purchase personal data from third-party data suppliers).

140. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 695-96 (7th Cir. 2015) ("[W]e refrain from deciding whether the overpayment for Neiman Marcus products and the right to one's personal information might suffice as injuries under Article III.").

141. *Id.* Remijas, 794 F.3d at 694.

One potential issue with the proposed framework is determining what do to in the event that a company is in compliance with the FTC's up-to-date standards and nonetheless suffers a data breach. Assuming that there was no negligent action on the part of the company, and the presumption against liability holds up, the FTC could be faced with the issue of how to provide a remedy for the affected consumers who have suffered a harm from the breach. The statute would resolve this by establishing a "victim's fund" for such a scenario, which would be funded out of the U.S. Treasury using a percentage of all fines levied against businesses for previous data breaches, or from general taxpayer funds if that pool of fines is inadequate. The victim's fund would ensure that there is at least some recourse for the affected consumers. However, the new regulation's primarily goal would be to maintain such a strong set of data security standards that no company that followed the FTC's guidelines would suffer a breach.

One final aspect of the FTC's current data security authority that would need to be overhauled is the classification of different types of personal data. Currently, several statutes grant the FTC specific authority to regulate the data security practices of companies within certain industries or to enforce regulations against certain types of protected data.[142] It may be time to reexamine these specialized statutes, as it is now evident that all types of personal data potentially carry tangible economic value for the owner.[143] In FCC Commissioner Ajit Pai's dissent to the *Data Privacy NPRM*, Pai criticized the proposed data privacy and security rules as unjustifiably imposing stricter guidelines on Internet Service Providers (ISPs) than members of other industries that collect the same types of consumer data.[144] A baseline regulatory scheme should be designed to encourage full protection of all data that has been collected from consumers, and ISPs along with any other business must be held to a higher standard than what currently exists. While it would certainly be unfair to only impose new rules on ISPs, an FTC-led effort to establish a universal data security standard across all industries would meet the dual purpose of ensuring the effective protection of consumer data while also maintaining a level commercial playing field.

An apparent impediment to the establishment of stronger data security measures is the closely-related yet highly contentious issue of data privacy. Matters of data privacy concern the scope of a company's ability to use consumer data, as opposed to the extent of its obligations to protect consumer data from unauthorized third parties. Issues like transparency and consumer choice in data collection are matters that relate strictly to privacy, and they deserve to be addressed. However, ensuring the protection of all consumer information is a necessary starting point. In our increasingly digital world, consumers will continue to distribute their payment information on a massive scale, and the protection of such commonly shared data should not be hindered while legislators battle over the more complex privacy issues regarding such data. If companies cannot be trusted to keep their customers'

142. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1641 (1970); Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998); Financial Services Modernization Act, Pub.L. 106–102 (1999).

143. *See* Cooper & LaSalle, *supra* note 131, at 14.

144. *Data Privacy NPRM* at 139 (Comm'r Pai, dissenting).

data safe from unauthorized access, then there can be no meaningful discussion on what types of data may be collected or how. Consumers would assume that any data they share with a business can easily fall into the wrong hands, and the resulting mistrust could prevent personal data from becoming the immense market that it has the potential to be.

IV. CONCLUSION

It is time for Congress to move forward with new legislation that grants the FTC statutory authority over the data security practices of U.S. businesses. The current "reasonableness" standard under which the FTC holds companies accountable for data breaches is outdated, does not provide sufficient guidance on what data security measures to take, and does not adequately protect the consumers who are directly harmed by data breaches.

The FCC Enforcement Bureau has provided a promising model for data security enforcement that applies specific, forward-looking, technical, and procedural requirements that not only seek to prevent future data breaches, but also allow companies a measure of flexibility in how they implement the recommended practices. Congress should enact new legislation that will assist the FTC in moving away from its vague "reasonableness" standard toward creating a specific set of security guidelines that remain up-to-date and provide companies with affirmative incentives for following them.

If the FTC can encourage businesses to employ cutting-edge data security practices, then breaches can be mitigated, as data systems grow more complex and personal information becomes an increasingly valuable economic asset. Maintaining a domestic market that is safe from hacks and data breaches will result in greater consumer trust in the economy, and will empower the individual to enjoy full control of a valuable asset that has thus far only served to benefit third parties.

The Quadrennial Review: The Federal Communications Commission's Latent Superpower & What Can Be Done to Free It

Bryan Schatz *

TABLE OF CONTENTS

* J.D., The George Washington University Law School, May 2017. Executive Editor and Notes Editor, *Federal Communications Law Journal*, 2016–17. B.S. Earth, Society and Environmental Sustainability, University of Illinois, Urbana-Champaign, December 2013. I want to thank my Notes Group Adjunct Professor, Kara Romagnino, for her help and guidance throughout the Note process; I want to thank the 2016-17 Federal Communications Law Journal staff for their tireless efforts; and I want to thank the Article Editors and Managing Editors involved in the publication process for their work in editing this Note. Lastly, I would like to thank my friends and girlfriend for their support throughout this process.

I. INTRODUCTION

In 1996, Congress authorized the Federal Communications Commission (the "FCC") to review its media ownership rules every four years as part of the Quadrennial Review ("QR"),[1] with the goal of determining whether or not the rules continue to be "necessary in the public interest."[2] The QR is a powerful tool for the FCC as it allows the FCC to advance diversity in the news and among media owners, foster competition in the industry, and promote localism[3]—all in the name of serving the public interest. Much like a superhero who gains his or her abilities by chance, the FCC has tried to figure out the extent of its QR powers and how these powers can best be employed. To date, the FCC has struggled to implement new rules after its QRs, effectively neutralizing the power of the QR.[4]

The QR can be the FCC's way to stay on top of the changing media markets and a tool for the FCC to protect the public from further concentration of media ownership[5] as the industry shifts from media accessed via print and television to media accessed over the Internet. The entire Communications Act, as amended, hardly contemplates the "Internet," mentioning it only a few times; the QR can serve as a way for the FCC to monitor changing media consumption avenues, such as the growth of Internet media consumption.[6] The Communications Act, though the most important governing statute regarding communications regulation, barely touches on the Internet and how it should be regulated for telecommunications purposes—despite the fact that the Internet is becoming

1. *See* Telecommunications Act of 1996, Pub. L. No. 104-104, § 202(h), 110 Stat. 56 (2012).

2. *Id.*

3. *See* Andrew Jay Schartzman et al., *Section 202(h) of the Telecommunications Act of 1996: Beware of Intended Consequences*, 58 Fed. Comm. L.J. 581, 582-84 (2006) (discussing the history of Section 202(h)).

4. By way of example, the 2010 and 2014 Quadrennial Reviews had an Order released on August 25, 2016. *See* 2014 Quadrennial Regulatory Review – Review of the Comm'n's Broad. Ownership Rules and Other Rules Adopted Pursuant to Section 202 of the Telecommunications Act of 1996, et al., *Second Report and Order*, FCC 16-107, at para. 1 (2016) [hereinafter *2010 & 2014 Quadrennial Review*], https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-107A1.pdf [https://perma.cc/S67M-9K8Z].

5. *See* James B. Stewart, *When Media Mergers Limit More Than Competition*, N.Y. TIMES (July 25, 2014), https://www.nytimes.com/2014/07/26/business/a-21st-century-fox-time-warner-merger-would-narrow-already-dwindling-competition.html?_r=0 [https://perma.cc/PFB8-EUZG] ("[I]n 1983, 50 companies owned 90 percent of the media consumed by Americans. By 2012, just six companies — including Fox (then part of News Corporation) and Time Warner — controlled that 90 percent, according to testimony before the House Judiciary Committee examining Comcast's acquisition of NBCUniversal.").

6. *See* Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (2012).

the primary sources for news.[7] Currently, more consumers are getting their news from the Internet and moving away from print and television media.[8] Under Section 202(h) of the Telecommunications Act, the FCC can promulgate new media ownership rules or modify the current rules every four years (the Quadrennial Review) and regulate the industry from which the public is accessing its news.[9]

Peter Parker's (Spiderman's alter-ego) uncle Ben warned Peter that "[w]ith great power there must also come—great responsibility!"[10] Applying that principle to the FCC and the power of the QR, this quote would state, "with great power comes great responsibility; enough responsibility to inundate the power and overwhelm it!" As it stands, the FCC's various responsibilities include following Section 553 informal rulemaking procedures,[11] holding self-prescribed public hearing sessions,[12] and navigating the inevitable legal challenges, which ensue after the proposal of any rule.[13]

Taking a step back and looking at the QR from a big picture standpoint provides some clarity as to the choices that the FCC must make to free the QR from its current place of ineptitude. As required by Section 202(h), the FCC reviews media ownership rules every four years; the proposed rules are challenged in court and then, shortly thereafter, another QR is due.[14] This initial review forces the FCC to expend valuable

---

7. *See* AMY MITCHELL ET AL., THE MODERN NEWS CONSUMER: NEWS ATTITUDES AND PRACTICES IN THE DIGITAL ERA 5–8, PEW RES. CTR. (July 7, 2016), http://assets.pewresearch.org/wp-content/uploads/sites/13/2016/07/07104931/PJ_2016.07.07_Modern-News-Consumer_FINAL.pdf [https://perma.cc/R592-XZV3].

8. *See generally 2010 & 2014 Quadrennial Review*, *supra* note 4, at para. 1; 2010 Quadrennial Regulatory Review – Review of the Comm'n's Broad. Ownership Rules & Other Rules Adopted Pursuant to Section 202 of the Telecommunications Act of 1996, 25 FCC Rcd 6086, at para. 48 (2010) [hereinafter *2010 Quadrennial Review*] ("Recent PEJ research shows that on a typical day, 61% of Americans get news online, which puts the Internet just behind television and ahead of newspapers as a source for news." (citations omitted)); *see also* Monica Anderson & Andrea Caumont, *How Social Media Is Reshaping News*, PEW RES. CTR. (Sep. 24, 2014), http://www.pewresearch.org/fact-tank/2014/09/24/how-social-media-is-reshaping-news/ [https://perma.cc/HG64-8KZ9].

9. *See 2010 Quadrennial Review Report and Order*, *supra* note 8, at n.2 ("In 2004, Congress revised the then-biennial review requirement to require such reviews quadrennially."); 2014 Quadrennial Regulatory Review – Review of the Comm'n's Broad. Ownership Rules & Other Rules Adopted Pursuant to Section 202 of the Telecommunications Act of 1996, 29 FCC Rcd 4371, at n.10 (2014) [hereinafter *2014 Quadrennial Review Report and Order*].

10. *See* Stan Lee, *Amazing Fantasy #15* (Aug. 1962); *see also* SPIDER-MAN (Columbia Pictures 2002), https://www.youtube.com/watch?v=_5d6rTQcU2U.

11. *See* 5 U.S.C. § 553 (2016); Prometheus Radio Project v. FCC (*Prometheus II*), 652 F.3d 431, 449 (3d Cir. 2011) (Scirica, J., dissenting)

12. *2014 Quadrennial Review Report and Order*, *supra* note 9, at para. 10.

13. *See, e.g.*, *Prometheus II*, 652 F.3d at 431; Fox Television Stations, Inc. v. FCC (*Fox I)*, 280 F.3d 1027, 1033 (D.C. Cir. 2002), *modified on reh'g,* 293 F.3d 537 (D.C. Cir. 2002); Sinclair Broad. Grp. v. FCC, 284 F.3d 148 (D.C. Cir. 2002).

14. Telecommunications Act of 1996, Pub. L. No. 104-104, § 202, 110 Stat. 56 (codified in scattered sections of 47 U.S.C.)

resources, time and consideration to study the current media ownership rules, and to deliberate and craft new rules or justifications for the standing rules. Then, the FCC expends valuable resources, time, and consideration in trying to justify its QR findings, when they are inevitably challenged in court. Regardless of the court's finding, the FCC must consider the media ownership rules once again when the next QR arrives, but now with the added wrinkle of needing to evaluate and consider the idiosyncrasies of the most recent judicial holding from the past-QR's legal challenge. *This* struggle is precisely why the QR has become inept.

New rules proposed under the FCC's QR power have yet to come to fruition,[15] because they are caught in a web of constant legal challenges and shifting lenses of judicial analysis.[16] This struggle of legal challenges that has plagued the FCC is not unique to the agency; it is part of a larger problem known as the "ossification" of rulemaking that has affected many other agencies.[17] Over the years, the QR process has changed and the FCC has tried to improve the process,[18] so as to stand a better chance in the face of legal challenges.[19] Still, more is needed before the FCC can be efficient and effective in using its QR power.

Congress, the courts, or the FCC must act now in order to free up the QR and allow the FCC to use this power to efficiently help the communications industry transition into the next age of media

15. *See FCC's Review of the Broadcast Ownership Rules*, FCC (Oct. 25, 2016), https://www.fcc.gov/consumers/guides/fccs-review-broadcast-ownership-rules [https://perma.cc/HWQ4-TVLY] (last visited Jan. 25, 2016) ("In July 2011, a court decision affirmed the Commission's decision in the 2006 quadrennial review to retain several of the rules, but vacated and remanded the modified newspaper/broadcast cross-ownership rule, as well as measures taken to foster ownership diversity."); *see generally 2010 & 2014 Quadrennial Review*, *supra* note 4.

16. *See generally* Peter DiCola, *Choosing Between the Necessity and Public Interest Standards in FCC Review of Media Ownership Rules*, 106 MICH. L. REV. 101, 117 (2007).

17. *See* Thomas O. McGarity, *Some Thoughts on "Deossifying" the Rulemaking Process*, 41 DUKE L.J. 1385, 1385–86 (1992). "Ossification" is the tightening of the informal rulemaking process which was created to be fluid and easy for agencies to promulgate rules. *See id.* As Professor McGarity explains, "Professor E. Donald Elliott, former General Counsel of the Environmental Protection Agency, refers to this troublesome phenomenon as the 'ossification' of the rulemaking process, and many observers from across the political spectrum agree with him that it is one of the most serious problems currently facing regulatory agencies." *Id.* (citing E. Donald Elliot, Remarks at the Symposium on "Assessing the Environmental Protection Agency After Twenty Years: Law, Politics, and Economics," at Duke University School of Law (Nov. 15, 1990); *see* Antonin Scalia, *Back to Basics: Making Law Without Making Rules,* REGULATION, July/August 1981, at 26 (characterizing the 1970s as the "era of rulemaking")).

18. *See FCC's Review of the Broadcast Ownership Rules*, *supra* note 15.

19. *See 2010 Quadrennial Review Report and Order*, *supra* note 8 at para. 2

consumption.[20] Section II of this note will explore the QR's past by looking at the legislative history, the current procedures employed and the procedural history, and the legal history; also, Section II will explain the current media ownership rules and why now is the time for the FCC to realize its QR powers. The next Section of this Note will analyze some of the potential solutions, which can help free up the QR and help the FCC promulgate and enforce new media ownership rules. The final Section will look at how Congress can act to provide procedural protections for the QR, the courts can alter the applicable level of scrutiny applied to the QR, and the FCC can enact a different type of rule to help empower the QR.

II. HOW THE SMALL MOLEHILL OF THE QUADRENNIAL REVIEW GREW TO BECOME A "HULK"-ING MOUNTAIN FOR THE FCC

To fully understand why action is needed to free up the QR, it is important to consider how each potential entity that could provide a solution has interacted with the QR in the past. Analyzing the legislative history will provide context for how Congress created the QR and some of its intentions whereas analyzing the legal history and looking at past challenges to rules proposed under the QR will help provide context for how the courts have approached proposed FCC media ownership rules. It is helpful then to note where each of the major media ownership rules currently stands. Ultimately, analyzing the QR procedures will provide context for how the FCC has wrestled with the QR.

A. Legislative History: How the Quadrennial Review Came to Be and Why It Was Inserted into the Telecommunications Act of 1996

The QR, as embodied in Section 202(h) of the Telecommunications Act, has very little legislative history to explain why it was drafted the way

20. *See* Prometheus Radio Project v. FCC (*Prometheus III*), 824 F.3d 33, 37, 61–62 (3d Cir. 2016) ("Several broadcast owners have petitioned us to wipe all the rules off the books in response to this delay—creating, in effect, complete deregulation in the industry. This is the administrative law equivalent of burning down the house to roast the pig, and we decline to order it. *However, we note that this remedy, while extreme, might be justified in the future if the Commission does not act quickly to carry out its legislative mandate.*") (emphasis added in italics). Dissenting, Circuit Judge Scirica indicated that an order compelling the FCC to act in regards to creating new broadcast ownership rules is a more efficient avenue than just admonishing the FCC as the majority opinion did.

that it was.[21] It appears that the rule was intended as a tool for large media corporations to get the national television ownership cap removed,[22] or at least progressively raised, every two years.[23] Because the FCC had to "justify" the cap at the level at which it was set, the two lobbyists who drafted Section 202(h) knew that this would be a difficult task for the FCC and would allow for industry challenges to any FCC media ownership determinations.[24] After the first Quadrennial Review, the FCC's determinations were challenged in the D.C. Circuit.[25] These first challenges led to the FCC raising the national media ownership cap ten percent from its previous level.[26] The national television ownership cap was eventually modified and led to a series of Congressional actions which lowered the cap from forty-five to thirty-nine percent, moved the biennial reviews to quadrennial, and lead to several other legal challenges to the findings of the original lawsuits as the FCC applied those holdings.[27]

Andrew Schwartzman, Harold Feld and Parul Desai, who all participated in some of the first cases concerning the QR and communications law experts, state in their article that "[d]espite the attempt to deregulate through the back door, it would seem that the courts have

---

21. S. REP. NO. 104-230, at 163-64 (1996) (Conf. Rep.) ("Subsection (h) directs the Commission to review its rules adopted under section 202 and all of its ownership rules biennially. In its review, the Commission shall determine whether any of its ownership rules, including those adopted pursuant to this section, are necessary in the public interest as the result of competition. Based on its findings in such a review, the Commission is directed to repeal or modify any regulation it determines is no longer in the public interest. Apart from the biennial review required by subsection (h), the conferees are aware that the Commission already has several broadcast deregulation proceedings underway. It is the intention of the conferees that the Commission continue with these proceedings and conclude them in a timely manner.").

22. The national television ownership cap limits the total amount of stations that an entity may own; the FCC enforces this rule through a cap which limits the amount of households (39%) that a single entity may reach. *See FCC's Review of the Broadcast Ownership Rules*, *supra* note 15.

23. *See* Schwartzman et al., *supra* note 3, at 582–84 (2006).

24. *See Id.* at 583—584 ("For a while, at least, it appeared that Section 202(h) would be a potent weapon. Although the Clinton-era FCC initially construed Section 202(h) as little more than a reporting requirement, News Corp., which reportedly had retained litigation counsel even before the FCC completed its first biennial review, mounted a successful judicial challenge, obtaining a ruling that temporarily gave a broad reading to Section 202(h).").

25. *See* Sinclair Broad. Grp. v. FCC, 284 F.3d 148, 152 (D.C. Cir. 2002); Fox Television Stations, Inc. v. FCC (*Fox I)*, 280 F.3d 1027, 1033 (D.C. Cir. 2002), *modified on reh'g,* 293 F.3d 537 (D.C. Cir. 2002).

26. *See* Schwartzman et al., *supra* note 3, at 585.

27. Consolidated Appropriations Act, 2004, Pub. L. No. 108–199, § 629, 118 Stat. 3, 99 (2004). The legislation also amended § 202(h) in two ways: (1) making the Commission's biennial review obligation quadrennial; and (2) insulating from § 202(h) review "rules relating to the 39 percent national audience reach limitation." *See id*.; *see also* Prometheus Radio Project v. FCC (*Prometheus I)*, 373 F.3d 372, 389 (3d Cir. 2004) ("In January 2004, while the petitions to review the Order were pending in this Court, Congress amended the 1996 Act by increasing from 35% to 39% the national television ownership rule's audience reach cap in § 202(c)."); Schwartzman et al., *supra* note 3, at 585-86.

resolved ambiguities relating to the interpretation of Section 202(h) in favor of making it a less intrusive provision."[28] While Section 202(h) may have avoided becoming a tool for "deregulatory" purposes, it still remains a potentially powerful tool for the FCC to use to usher in a new era of media consumption. Empowering the QR to fully realize its potential would allow the FCC to change the lens used by the QR; instead of being a deregulatory tool for the industry (as it was intended to be when it was drafted), the FCC can use the QR can become the FCC's ability to regulate the media industry and lead it into the next age of media consumption.

B. Legal History: What Shaped the Quadrennial Review into What It Is Today and How It Is Still Influenced by Past Challenges

Since the inception of the QR, the FCC's proposed new media ownership rules have been challenged regularly. One of the first cases to challenge the proposed FCC media ownership rules was *Fox Television Stations, Inc. v. FCC* (*Fox I*),[29] where the D.C. Circuit found that the FCC failed to sufficiently justify its decision to retain the national TV station ownership,[30] as well as cable/broadcast cross-ownership rules.[31] The FCC argued to the court and in its order that the national television station ownership rule helped prevent broadcasters from maintaining too much control of a market, which would threaten competition and diversity in the media marketplace.[32] In regards to the cable/broadcast cross-ownership rule, the FCC argued a variety of reasons to the court and in its order—generally related to competition and diversity—as to how the rule was in accordance with the public interest, but not *necessary* to the public interest, and thusly the FCC's justifications were found to be unpersuasive.[33] The court found that the cable/broadcast cross-ownership rule was so insufficiently justified that only a complete repeal of the rule was proper—despite a subsequent appeal challenging this assertion.[34]

Of note, this case also established that Section 202(h) carries with it a presumption of "deregulation" indicating that any rule that cannot be

28. *See* Schwartzman et al., *supra* note 3, at 586.

29. *See generally Fox I*, 280 F.3d at 1027.

30. The national TV station ownership rule does provides a cap on the total amount of television stations a single entity may own – based on the percent of households the stations reach. *See FCC's Review of the Broadcast Ownership Rules*, *supra* note 15 (for more information, please see Part II.C).

31. The cable/broadcast cross-ownership rule prevents a cable station and a broadcast station from being carried and from being owned by the same entity in a local market. Interestingly, the *Fox I* court never indicated what the cable/broadcast cross-ownership rule means in its opinion.

32. *See Fox I*, 280 F.3d at 1041–44.

33. *See id.* at 1051.

34. *See id.* at 1052.

justified as "*necessary* to the public interest"[35] should be repealed.[36] Contrastingly, the FCC interpreted the clause to turn on whether the rule *served a benefit* to the public interest.[37] On appeal, the same court modified its original opinion and indicated that any of its language regarding "necessary to the public interest" and the meaning of that term as construed by the *Fox I* opinion should be removed and was not intended to be precedential.[38] The appellate court in this case was likely highly analytical of any reasoning posited by the FCC because of the presumed deregulatory intent but the "strength" of the deregulatory intent of the QR seemed to weaken after the rehearing and modification of the meaning of the "necessary to the public interest" clause.

Shortly after *Fox I*, the D.C. Circuit heard *Sinclair Board Group, Inc. v. FCC*.[39] The FCC's local television ownership rule that was challenged "allows [for] common ownership of two television stations in the same local market if one of the stations is not among the four highest ranked stations in the market and eight independently owned, full-power, operational television stations remain in that market after the merger."[40] In *Sinclair*, the court determined that the FCC failed to explain why it was not arbitrary and capricious for the category of "non-broadcast media" to be excluded from its "eight voices exception" in the FCC record and the matter should be remanded to the FCC for reconsideration.[41] The court noted that the "eight voices exception" was unjustified and unneeded because there was insufficient explanation in the record to establish that the rule advanced anything that was "necessary to the public interest."[42] The court also employed an indispensable definition of "necessary,"[43] meaning that if the public interest could be served without this rule, then the rule was not necessary and indispensable to the public interest and should be repealed. The court was highly critical of the fact that the FCC failed to justify in the record why there would be two definitions to "voices" depending on the type of proposed rule.[44] Overall, the *Sinclair* court was thoroughly analytical

35. Sinclair Broad. Grp., Inc. v. FCC*,* 284 F.3d 148, 164 (D.C. Cir. 2002) ("This wait-and-see approach, however, cannot be squared with its statutory mandate . . . to repeal or modify any rule that is not necessary in the public interest." (citing Fox Television Stations, Inc., at 1042) (internal quotation marks omitted)) (emphasis added).

36. *See Fox I*, at 1033–34, 1048 ("Finally, and most important to this case, in § 202(h) of the Act, the Congress instructed the Commission, *in order to continue the process of deregulation*, to review each of the Commission's ownership rules every two years . . . .").

37. *See id.*, 280 F.3d at 1050; *See also* DiCola, *supra* note 16.

38. *See* Fox Television Stations, Inc. v. FCC, 293 F.3d 537, 540 (D.C. Cir. 2002). This secondary opinion (the "rehearing" portion of *Fox I*) was a quick appeal from the FCC in order to clarify some language of the *Fox I* opinion.

39. *See* Sinclair Broad. Grp., Inc. v. FCC*,* 284 F.3d 148 (D.C. Cir. 2002).

40. *Id.* at 152.

41. *See id.* at 152, 169.

42. *See id.* at 158–59, 163–64.

43. *See id.* at 159.

44. *See id.* at 162–65.

of any justification posited by the FCC—despite language in the opinion indicating the deferential arbitrary and capricious standard of review.[45]

In 2004, two cases impacted Section 202(h). *Cellco P'ship v. FCC* concerned a different provision contained within the Telecommunications Act, but the case turned on the definition of the word "necessary."[46] The D.C. Circuit found that the FCC's interpretation of the word "necessary" as "furthering the public interest" rather than "indispensable" to the public interest was valid and entitled to deference under the *Chevron* doctrine.[47] Later that year, the D.C. Circuit heard *Prometheus Radio Project v. FCC (*"*Prometheus I*").[48] Generally, the court found most of the radio ownership rules to be sufficiently supported by the record. Contrastingly, the court determined that the television ownership rules were all unsupported.[49] The court further noted that it would be very difficult for the FCC to sufficiently support numerical limits in proposed rules.[50] Additionally, *Prometheus I* ultimately set the definitions to be used in Section 202(h) analysis; "necessary" should follow the *Cellco* definition of "furthering the public interest" and not the *Fox I/Sinclair* definition.[51] Moreover, this court noted that the deregulatory presumption of Section 202(h) did not mandate a repeal of every rule that may have a weak justification because repealing every rule also required a sufficient justification for why that would serve the public interest.[52] In his dissenting opinion, Chief Judge Scirica highlighted the fact that the court was not really engaging in standard arbitrary and capricious review;[53] it was engaging in a very intense and thorough review and substituting its judgment for the FCC's—something it should not be doing.[54]

Later, the Third Circuit heard *Prometheus II*. The FCC attempted a quicker notice and comment type proceeding in an effort to hear some questions relevant to the QR by amending a standing notice of proposed rulemaking to include the fact that the FCC's decision will affect its QR determinations.[55] The court found this "quick" procedure to be contrary to

45. *See id.* at 159.

46. *See* 47 U.S.C. § 161(b) (2015) ("The Commission shall repeal or modify any regulation it determines to be no longer necessary in the public interest."); Cellco P'ship v. FCC, 357 F.3d 88 (D.C. Cir. 2004).

47. *See Cellco P'ship*, 357 F.3d at 97.

48. *See* Prometheus Radio Project (*Prometheus I*) v. FCC, 373 F.3d 372, 389 (3d Cir. 2004).

49. *See generally id.*

50. *See id.* at 430–35.

51. *See id.* at 391–95.

52. *See id.* at 395.

53. The Honorable Anthony Joseph Scirica served as Chief Judge for the Third Circuit Court of Appeals from 2003–2010 and served as a judge for the Third Circuit from 1987–2013. His dissent in *Prometheus I* was authored while he served as Chief Judge, and his dissent in *Prometheus II* was authored while he served as a circuit judge. For the sake of clarity throughout the article, he will be referred to as Chief Judge Scirica.

54. *See Prometheus I*, 373 F.3d at 435.

55. *See* Prometheus Radio Project v. FCC (*Prometheus II*), 652 F.3d 431, 445–49 (3d Cir. 2011).

APA notice and comment requirements,[56] discussed *infra*, and that the eligible entry definition employed by the FCC was arbitrary and capricious because there was no support for it in the record.[57] *Prometheus II* did have a slightly different tone to the court's analysis in that the review of the FCC's proposed rules was less searching and seemed to follow closer to the style of review Chief Judge Scirica indicated was proper in *Prometheus I*.[58]

In 2016, the Third Circuit heard *Prometheus III*.[59] To best understand the Court's opinion, it is essential to start with the Court's tone. The Court was mildly irritated that QR related issues were still pending before it.[60] Substantively, the Court presented several important holdings. *Prometheus III* began by declaring that it was "troubling is that nearly a decade has passed since the Commission last completed a review of its broadcast ownership rules."[61] The Court further explained that the QR "broke down" after *Prometheus II*.[62] *Prometheus III* analyzed both the FCC's delay to issue certain orders and the substance of an issued order.[63] In failing to create a new and updated definition of "eligible entry," the FCC cited "data concerns" for why a new definition could not be issued with the current record after Prometheus II; further the FCC promised to gather the data required to issue a new definition and in its next QR.[64] This promise from the FCC was insufficient to prevent the Court from requiring mediation between the parties to determine when the FCC could "promptly" issue an eligible entry definition.[65] The Court explained that the delay in completing a QR was "costly."[66] In an attempt to deregulate the entire field, Petitioners sought a vacatur of every media ownership rule; this attempt did not land with the Court and this relief was rejected.[67] Lastly, the 2014 Joint Sales Agreement Rule—intended to prevent a work-around to the local television ownership rule—was deemed to have been improperly promulgated without considering its effect on the local television ownership rule as part of the QR process and the FCC was required to include the Rule in its QR analysis.[68]

As the legal history indicates, when the FCC proposed new rules under its QR power, immediately thereafter, the rule was challenged. While the reviewing court changed in recent years from the D.C. Circuit to the

56. *See id.* at 449–54.
57. *See id.* at 468–72.
58. *See generally id.*
59. Prometheus Radio Project v. FCC (*Prometheus III*), 824 F.3d 33 (3d Cir. 2016)
60. *See, e.g.*, *Prometheus III*, 824 F.3d at 37 ("In some respects the Commission has made progress in the intervening years. In key areas, however, it has fallen short. These shortcomings are at the center of this dispute—the third (and likely not the last) round in a protracted battle over the future of the nation's broadcast industry.")
61. *Id.* at 37.
62. *Id.* at 38.
63. *Id.* at 40.
64. *Id.* at 45–48.
65. *Id.* at 50.
66. *Id.* at 51–52.
67. *Id.* at 52–54.
68. *Id.* at 54–60.

Third Circuit, each reviewing court applied a very thorough and searching look to the proposed rules and generally overturned the proposed rules (or some component thereof) for either substantive and procedural reasons—despite a thorough record, general procedural compliance, and reasoned analysis on the part of the FCC.

C. Current Media Ownership Rules: Complex, Confusing, and Convoluted Principles Governing Media Ownership

During the QR review, the FCC examines five different media ownership rules: the newspaper and broadcast cross-ownership rule ("NBCO"); the dual TV network ownership rule; the local TV multiple ownership rule ("Local TV Rule"); the local radio and TV cross-ownership rule ("LRTCO"); and the local radio ownership rule.[69] Along with these five rules, the FCC also has reviewed its national TV ownership rule ("NTO") under the QR and it is regularly considered with the QR because of its media ownership implications.[70]

The NBCO prevents an entity from owning a newspaper and a broadcast station within the same "contour."[71] In 2006, the FCC attempted to modify this rule, but *Prometheus II* indicated that the FCC failed to comply with applicable notice-and-comment procedural requirements in proposing the new NBCO rule and remanded the matter back to the FCC.[72] Recently, the FCC reiterated the importance of this rule, stating:

> The proliferation of (primarily national) content available from cable and satellite programming networks and from online sources has not altered the enduring reality that traditional media outlets are the principal sources of essential local news and information. The rapid and ongoing changes to the overall media marketplace do not negate the rule's basic premise that the divergence of viewpoints between a cross-owned newspaper and broadcast station "cannot be expected to be the same as if they were antagonistically run."[73]

---

69. *See FCC's Review of the Broadcast Ownership Rules*, *supra* note 15.

70. *See 2010 Quadrennial Review Report and Order*, *supra* note 8, at para. 7.

71. *See FCC's Review of the Broadcast Ownership Rules*, *supra* note 15. A contour is a geographic delineation of the market area which the broadcast provider can reach. *See* Prometheus Radio Project (*Prometheus I*) v. FCC, 373 F.3d 372, 387 (3d Cir. 2004). Of note, "contour" was redefined in light of the recent switch to digital television service and precisely how the contour and newspaper service areas overlap. *See 2010 & 2014 Quadrennial Review*, *supra* note 4, at para. 131.

72. *See* Prometheus Radio Project v. FCC (*Prometheus II*), 652 F.3d 431, 445–54 (3d Cir. 2011) (Scirica, J., concurring in part, dissenting in part) (finding that media owners may not have had formal notice, but were clearly on notice of NBCO rule from numerous prior formal FCC proceedings in which they had participated)

73. *See 2010 & 2014 Quadrennial Review*, *supra* note 4, at para. 129.

Further, the recent Order under the 2010 and 2014 Quadrennial Reviews, indicate a slight loosening of the Rule's restrictions; this is exemplified in the new exception to the rule permitting the acquisition of failing entities in the contour and case-by-case analysis of waivers to the Rule.[74]

The dual TV network ownership rule prevents any one of the top four broadcast networks (ABC, CBS, Fox and NBC) from merging together.[75] This rule was retained, despite a challenge to FCC reasoning, in *Prometheus II* because of the fact that these four broadcast networks clearly reach a larger audience than any other network and because any merger between these networks—due to the vertical integration of the four broadcast networks—would decrease diversity, programming and localism.[76]

The Local TV Rule states that a single entity can own two stations in a single designated market area ("DMA"), if: (1) "the digital [noise limited service contours] of the stations (as determined by [47 CFR § 73.622(e)] do not overlap; or (2) at least one of the stations is not ranked among the top-four stations in the market and at least eight independently owned television stations would remain in the DMA following the combination (the eight independent voices test)."[77]

The LRTCO employs a "sliding scale" to determine the maximum amount of radio and TV stations that can be owned by a single entity.[78] Under the LRTCO, if there are twenty or more independent media voices—defined as "full power TV stations and radio stations, major newspapers, and the cable system in the market"[79]—then an entity may own two TV and six radio stations or one TV and seven radio stations; [80] if there are between ten and twenty media voices, then an entity may own two TV and four radio stations; and if there are less than ten media voices, then an entity may own two TV stations and one radio station.[81] Also, an entity owning any local TV and radio stations must comply with the Local TV Rule and the local radio ownership rule.[82] The local radio ownership rule also employs a sliding scale, which outlines the number of radio stations an entity may own, depending on the size of the market.[83] Under the local radio ownership rule, there are four different tiers that break down the size of the market and the applicable ownership caps ranging from a maximum of eight stations that can be owned (if the market has forty-five or more stations) to a maximum

74. *See id.* at para. 132–33.

75. *See FCC's Review of the Broadcast Ownership Rules*, *supra* note 15.

76. *See Prometheus II*, 652 F.3d at at 463-64; *see also 2010 & 2014 Quadrennial Review*, *supra* note 4, at para. 218.

77. *2010 & 2014 Quadrennial Review*, *supra* note 4, at para. 7–18 (brackets and parenthesis added); *see also Prometheus II*, 652 F.3d at 458–61.

78. *See FCC's Review of the Broadcast Ownership Rules*, *supra* note 15.

79. *See id.*

80. *See 2010 & 2014 Quadrennial Review*, *supra* note 4, at para. 198.

81. *See FCC's Review of the Broadcast Ownership Rules*, *supra* note 15.

82. *See id.*

83. *See id.*

of five stations (if the market has fifteen or less stations).[84] Also, the local radio ownership rule prevents an entity from concentrating their ownership in one radio service (AM or FM) and places certain "sub-caps" on each radio service.[85] The rules, complex in nature, become even more complicated knowing that they are subject to regular review, amendment or repeal depending on how the upcoming QR goes.

D. Chains Made from Kryptonite: The Procedures That Bind the Quadrennial Review and How They Have Changed from Their Original Implementation

From the text of the Telecommunications Act, there is little to indicate the precise procedures the QR is supposed to follow. The FCC generally has elected to follow Section 553 informal rulemaking, notice-and-comment procedures.[86] Recently though, the FCC has self-imposed certain other procedures in order to create a more thorough record.[87]

1. Originally Prescribed Procedures and the "Ossification" Plague

Section 202(h) contains no direct instructions for the FCC for how to hold a QR and the proper procedures to apply. With that being said, in *Prometheus I*, the Third Circuit noted that it was proper for the FCC to follow Administrative Procedure Act ("APA") Section 553 procedures.[88] But following the Section 553 informal procedures causes much of the problems for the FCC in the QR; this is best evidenced in *Prometheus I* when the Third Circuit struck down the proposed rules.[89]

Part of the reason why the FCC has struggled in promulgating new media ownership rules is due to the fact that informal rulemaking has

84. *See id.*

85. *See id.*

86. *See, e.g.*, Prometheus Radio Project v. FCC (*Prometheus I*), 373 F.3d 372, 411 (3d Cir. 2004). Formal rulemaking must be explicitly triggered by precise language, such as "to be made on the record after opportunity for an agency hearing," in the rulemaking section of the agency's organic statute. *See* ROBERT L. GLICKSMAN & RICHARD E. LEVY, ADMINISTRATIVE LAW: AGENCY ACTION IN LEGALCONTEXT 48 (Robert C. Clark et al. eds., 2d ed. 2015). Formal rulemaking "contemplate[s] a hearing 'on the record' that closely resembles a judicial trial" and is governed by §§ 556 and 557 of the APA. *See id.* Informal rulemaking—or notice and comment rulemaking—is governed by § 553 of the APA and requires that "notice of a proposed rule be published in the Federal Register and must include the content of the rule, instructions for submitting comments, and other pertinent information." *See id.* at 47. Those interested in participating must be given an opportunity to submit written comments. *See id.* The agency must also explain why it adopted its precise final rule as part of the text of its final rule. *See id.*

87. *See* Prometheus Radio Project v. FCC (*Prometheus II*), 652 F.3d 431, 449 (3d Cir. 2011).

88. *See Prometheus I*, 373 F.3d at 411.

89. *See id.*

changed from its original conception. Notice-and-comment procedures were meant to be an efficient method of promulgating rules for an agency in an area of its expertise.[90] But as agencies began to promulgate rules in increasingly technical areas, agencies needed increased public participation from outside scientists for information, which caused heightened public analysis on the informal rulemaking process.[91] In effect, this changed a set of general procedures, which was intentionally deferential to the agency promoting its efficiency and expertise, to a highly involved process requiring public input and constant scrutiny.[92] The constant public scrutiny heightened awareness of regulated entities and created a system where every proposed rule was the subject to a legal challenge.[93] This shift is known as the "ossification" of the rulemaking process—a quick, fluid and efficient process has become solid and stagnant.[94]

Notice-and-comment rulemaking has never been the same. Across the board, many agencies have felt the consequences of ossification.[95] Specifically in the QR process, ossification required Congress to shift the biennial process to a quadrennial process, as we know it now.[96]

2. FCC's Self-Imposed Procedures as a "De-Ossification" Tool

To fight ossification and combat the stiffness caused by the increased scrutiny, the FCC has self-imposed additional procedures that go above the bare requirements to comply with Section 553. Most prominent amongst these efforts are the various public hearings held by the FCC across the country where interested parties can submit oral testimony and written materials to the FCC for its consideration in the QR.[97] Additionally, the FCC creates a dense record and iterates a thorough statement of basis of purpose in each of its proposed rules; all of these actions are undertaken with the intent to sufficiently support any conclusions the FCC makes. [98] The FCC

90. McGarity, *supra* note 17, at 1398.
91. *Id.* at 1398.
92. *Id.* at 1401.
93. *Id.* at 1401.
94. *Id.* at 1386 ("Professor E. Donald Elliott, former General Counsel of the Environmental Protection Agency, refers to this troublesome phenomenon as the "ossification" of the rulemaking process.")
95. *See generally* Richard J. Pierce, Jr., *Rulemaking Ossification Is Real: A Response to Testing the Ossification Thesis*, 80 GEO. WASH. L. REV. 1493 (2012)
96. *See* Schwartzman et. al., *supra* note 3, at 585; *cf.* Fox Television Stations, Inc. v. FCC (*Fox I)*, 280 F.3d 1027, 1039 (D.C. Cir. 2002), *modified on reh'g,* 293 F.3d 537 (D.C. Cir. 2002) ("We appreciate that § 202(h) requires the Commission to undertake a significant task in a relatively short time, but we do not see how subjecting the result to judicial review makes the Commission's responsibility significantly more burdensome, let alone so formidable as to be improbable [that Congress intended to not have the FCC determinations subject to judicial review].").
97. *FCC's Review of the Broadcast Ownership Rules* , *supra* note 15.
98. *See 2014 Quadrennial Review Report and Order*, *supra* note 9, at para. 9–10.

has yet to see any material benefit from these heightened procedures, but their potential benefits are clear.[99] With the extra procedures, the FCC creates a more thorough record and enhances its own understanding of the various stakeholders, which—in theory—help it sufficiently support its QR proposals.

III. THE TIME IS NOW FOR THE FCC TO REALIZE ITS QUADRENNIAL REVIEW POWERS.

In *Fox I*, the court struck down the broadcasters' arguments that the scarcity rationale, which justifies the FCC's ability to limit the free speech rights of broadcasters through the national television ownership cap, as no longer persuasive and can no longer justify the abridgment of free speech through the FCC caps.[100] The broadcasters attempted to argue that the scarcity rationale in past Supreme Court cases, which found the FCC had the power to limit free speech via the national television ownership cap, was no longer applicable because advancements in the marketplace provided for a sufficient number of other broadcasters to not threaten the availability of viewpoints for consumers.[101] The *Fox I* court rejected this argument—though agreeing with its substantive position—noting that whether or not the scarcity rationale continues to "make sense" is not for the court to decide because the Supreme Court already has.[102]

The debate as to why media ownership rules are important has been settled—but it was settled over a decade ago in the first case challenging the QR. More media is consumed over the Internet. The *Fox I* court noted that the scarcity rationale is implicated in ownership caps because of "the limited physical capacity of the broadcast spectrum."[103] Media consumed over the Internet, does not threaten the "limited physical capacity of the broadcast spectrum" in the same way that justified the continued employment of the scarcity rationale.[104]

Is now the time for the FCC to abandon the scarcity rationale and employ a new rationale for its media ownership rules that restrict the free speech of broadcasters? Is now the time for the FCC to create a new policy blending the scarcity rationale with another to continue its ability to protect the consumers' right to a variety of viewpoints? Is now the time for the FCC to lower the media ownership caps because broadcasters can circumvent these caps by "broadcasting" in an "uncapped" manner through the Internet? Is now the time to abandon all media ownership caps because the Internet provides more opportunities to viewpoints than the limited broadcast

99. *See supra* Part II.B.

100. *See Fox I*, 280 F.3d at 1045–46.

101. *See id.* at 1045.

102. *Id.* at 1046 (citing Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 638 (1994)) (affirming scarcity rationale).

103. *Id.*

104. *See 2014 Quadrennial Review Report and Order*, *supra* note 9, at para. 1–2.

spectrum ever could and there is no longer threat to a variety of viewpoints for the consumers?

No matter what the answer is to the above questions, the time *is* now for the FCC to realize its QR powers to answer any of those questions because if the QR continues to be stagnant, the old rules are not going to properly balance the First Amendment free speech right of broadcasters with the First Amendment right of consumers to have access to a variety of viewpoints.

A. In a Flash, Congress Can Prescribe Clean Air Act-Like Hybrid Rulemaking Procedures and Provide More Power to the FCC During the Quadrennial Review.

As mentioned before, there are various potential solutions, which Congress, the courts, and the FCC can implement in order to guide the QR to freedom from its current confines.

Hybrid rulemaking procedures[105]—a higher standard for the QR that must comply with informal notice-and-comment procedures of Section 553—could help the FCC more effectively promulgate media ownership rules.[106] Congress mandating the FCC utilize hybrid rulemaking is not entirely the solution because forced extra procedures will not help the QR alone. But the hybrid rulemaking procedures within the Clean Air Act ("CAA")[107] carry an advantage for the Environmental Protection Agency ("EPA"); if the EPA follows the hybrid rulemaking procedures, most procedural infirmities that occur during CAA rulemaking do not cause any proposed rule to be vacated, remanded, or repealed.[108] A similar provision protecting the FCC's QR practices would be beneficial.

105. Hybrid rulemaking procedures are those which "go beyond the requirements of notice and comment, but are less formal than a hearing under §§556 and 557[]" as required for formal rulemaking. *See* Glicksman & Levy, *supra* note 86, at 48. Hybrid rulemaking can be imposed by organic statute or can be self-imposed by the agency through the adoption of regulations governing its rulemaking process. *See Id.*

106. *See id.* at 361–62.

107. While the CAA is regularly involved in litigation, the majority of this litigation centers on the SIPs and FIPs the EPA mandates—not the structure of the hybrid rulemaking process. "A State Implementation Plan (SIP) is a collection of regulations and documents used by a state, territory, or local air district to reduce air pollution in areas that do not meet National Ambient Air Quality Standards, or NAAQS." *Basic Information About Air Quality SIPS*, U.S. EPA, https://www.epa.gov/sips/basic-information-air-quality-sips (last visited Oct. 18, 2017). "A Federal Implementation Plan (FIP) is an air quality plan developed by EPA under certain circumstances to help states or tribes attain and/or maintain the National Ambient Air Quality Standards (NAAQS) for common air pollutants." *Id.*

108. *See* 42 U.S.C. § 7607(d)(9)(D) (2015).

1. Clark Kent or Superman? The FCC's Self-Prescribed Procedures Are Nearly the Same as the Clean Air Act's Hybrid Rulemaking Requirements, But Without the Super-Impact.

The CAA mandates procedures that are more rigorous than Section 553 informal rulemaking procedures, but less stringent than formal rulemaking guided by Sections 556 and 557[109]—thusly coined "hybrid" rulemaking procedures. The EPA, as required by the CAA, must work with states to create various statewide, regional, and national plans (known as state implementation plans, or "SIPs" and "FIPs"), which reduce the levels of various air pollutants by establishing National Ambient Air Quality Standards ("NAAQS") that apply to pollution generated by both stationary and mobile sources.[110] The EPA is required to hold hearings with the state and has a higher level of support required in its final reports and orders.[111] These requirements exceed the informal notice-and-comment procedures contained within Section 553.

Similar to those requirements contained in the CAA's hybrid rulemaking system are the self-prescribed procedures the FCC has imposed on previous QRs. As enumerated above, the FCC has held numerous public hearings across the country to accumulate further information,[112] has generated dense, thorough records, and has explained a thorough basis and purpose for all proposed rules[113]—all of which are requirements for the EPA under the CAA's hybrid rulemaking system.[114]

These procedures exceed the bare minimum required in Section 553 informal rulemaking. The FCC effectively has self-imposed hybrid rulemaking procedures similar to those contained within the CAA. But, because the procedures are self-prescribed and not statutorily mandated, the FCC does not have the opportunity to enjoy the full benefit that the CAA affords the EPA for using the hybrid procedures.[115]

Under the CAA's hybrid approach, courts can only reverse or remand an agency action in narrow circumstances outlined in 42 U.S.C. § 7607(d)(9)(D): if the failure to follow the proscribed procedure was arbitrary and capricious, and an objection of "central relevance" to the rule comes before judicial review but after public hearing, and if ". . . the errors

---

109. *See* 42 U.S.C. § 7607(d) (2015); 5 U.S.C. §§ 553, 556-57 (2016).

110. *See Summary of the Clean Air Act*, EPA, https://www.epa.gov/laws-regulations/summary-clean-air-act [https://perma.cc/Q5DH-82PJ] (last visited Jan. 25, 2016).

111. *See* 42 U.S.C. § 7606 (2015).

112. *See FCC's Review of the Broadcast Ownership Rules* , *supra* note 15.

113. *See 2014 Quadrennial Review Report and Order*, *supra* note 9, at para. 9–14; *see generally*, *id.* (totaling over 300 pages).

114. 42 U.S.C. § 7607(d)(9)(D) (2015).

115. *See* Michael Dingerdissen, *Third Circuit Uses Procedural Grounds to Reject FCC's Weakening of Media Cross-Ownership Rules for A Second Time in Prometheus Radio Project v. FCC*, 6 J. LEGAL TECH. RISK MGMT. 1, 36–46 (2012); *see generally* Prometheus Radio Project v. FCC (*Prometheus II*), 652 F.3d 431 (3d Cir. 2011).

were so serious and related to matters of such central relevance to the rule that there is a substantial likelihood that the rule would have been significantly changed if such errors had not been made."[116] These circumstances arise in very few cases, and generally, when procedural infirmities are alleged, the court finds the error outside of the scope of required agency reconsideration.[117]

Air Pollution Control v. U.S. EPA highlights how impactful a procedural error must be in order for a court to overturn an agency proposal under section 7607(d)(9)(D).[118] On all alleged procedural infirmities committed by the EPA, the Sixth Circuit ruled in favor of the EPA after Jefferson County submitted its required "petition for interstate pollution abatement, filed pursuant to Section 126 of the Clean Air Act."[119] Jefferson County indicated that the EPA exceeded the statutory and court ordered deadlines to respond to Jefferson County's petition, but the county failed to establish that the procedural infirmity itself was "arbitrary and capricious" of the EPA because the EPA had "legitimate reasons" for its delay.[120] This provides a degree of deference for the EPA in any alleged procedural infirmities—along with the deference that would be accorded to the EPA for its substantive findings that are supported in its record.

Also, Jefferson County argued that when the EPA modified the applicable criteria for analyzing submitted petitions after Jefferson County's submission, it was denied due process.[121] In rejecting this claim, the court explained that "[t]he limited review authorized by section 7607(d)(9)(D) does not compel reversal here.[122] The procedures employed by the EPA, while not ideal, generally ensured that all parties were given ample opportunity to submit information and to comment on the EPA's determinations."[123] Further, the court even suggested that "Jefferson County's real quarrel seems to lie with the EPA's substantive

116. 42 U.S.C. § 7607(d)(8), (d)(9)(D)(i)-(iii) (2015).

117. *See* North Dakota v. U.S. EPA, 730 F.3d 750 (8th Cir. 2013) *cert. denied sub nom.* N. Dakota v. EPA, 134 S. Ct. 2662 (2014); Air Pollution Control Dist. v. U.S. EPA, 739 F.2d 1071, 1079 (6th Cir. 1984) ("Because the statute's conditions are stated conjunctively, a reviewing court may not reverse a decision of the EPA solely because the court determines that the Agency has not observed the procedures required by law. The EPA's failure to observe proper procedures must be arbitrary and capricious, and essentially, go to the heart of the decision-making process to justify reversal."); *see also* Am. Petroleum Inst. v. Costle, 665 F.2d 1176, 1184 (D.C. Cir. 1981) ("Reversal for procedural defaults under the Act will be rare because *the court must first find that the Administrator was arbitrary or capricious, that he overruled a relevant and timely objection on the point in question, and that the errors were so significant that the challenged rule would likely have been different without the error*." (emphasis added)).

118. *See generally Air Pollution Control Dist.*, 739 F.2d at 1079.

119. *See id.* at 1074, 1094.

120. *See id.* at 1079–80.

121. *See id.* at 1081–82.

122. *Air Pollution Control Dist.*, 739 F.2d at1082.

123. *See id.* at 1082.

determinations."[124] A similar assertion was made by the Court in *North Dakota v. U.S. EPA*, below.[125]

The *Air Pollution Control* case indicates a seemingly higher burden of pleading and proof on the petitioner when there is an alleged procedural infirmity in EPA determinations that follow hybrid rulemaking procedures, which appears to be more akin to the pleading with particularity requirement—a heightened burden of pleading—in cases of fraud or mistake.[126] This serves as a protection for the EPA, whose compliance with the extra, heightened procedures actually opens the door to more allegations of procedural error.

More recently, in *North Dakota v. U.S. EPA*, the Eighth Circuit highlighted the burden on a challenging party to indicate that the procedural violation was substantial enough that, were the violation to have not occurred, the rule would be "significantly changed,"[127] another element of the CAA procedural protection provision. After North Dakota submitted its SIPs for the reduction of pollutants outlined in the CAA, the EPA dismissed the North Dakota SIPs and issued its FIP in the same action.[128] The court noted that when a procedural violation is asserted, there must be some "demonstrat[ion] that vacating the final rule based upon this alleged procedural error is appropriate[]"[129] which effectively raises the bar on any entity alleging EPA procedural violations in CAA actions, as the standard requirement would merely be indicating a procedural violation exists and the court can decide on a less severe remedy. Here, the court needs to find an arbitrary and capricious procedural violation that had a substantial impact on the final rule before finding a remedy.

2. The Clean Air Act's Procedural Protections Provision Would Greatly Help the FCC and the Quadrennial Review.

Congress should pass new legislation which codifies the CAA hybrid rulemaking provisions in Section 202(h) because the FCC already follows these procedures and would see great benefit from the procedural protections. This proposal would likely be amenable to the FCC as it would "reward" the effort they have put into QRs. However, Congress may be

124. *See id.*

125. *See also* North Dakota v. U.S. EPA, 730 F.3d 750, 759 (8th Cir. 2013) *cert. denied sub nom.* N. Dakota v. EPA, 134 S. Ct. 2662 (2014) ("Although '[i]t may be poor policy to try to distinguish between the SIP and FIP in a single action [,]' *Oklahoma v. EPA,* 723 F.3d 1201, 1223 (10th Cir.2013), the State has failed to demonstrate that vacating the Final Rule based upon this alleged procedural error is appropriate.").

126. *See* FED. R. CIV. P. 9.

127. *See North Dakota,* 730 F.3d at 758–59 (quoting 42 U.S.C. § 7607(d)(9)(D)).

128. *See id.*

129. *See id.* at 759.

disinclined to amend a single, smaller provision of the 1996 Telecommunications Act. Moreover, regulated entities may also be disinclined to pass new legislation because it would further shield—in a Captain America-type way—FCC determinations from judicial review and potential reversal.

In applying these sentiments to the QR, the potential benefits become readily apparent. Both *Air Pollution Control* and *Prometheus II* dealt with time-based procedural infirmities.[130] While *Air Pollution Control* centered on the EPA exceeding statutory and court ordered deadlines and *Prometheus II* centered on the FCC failing to meet statutory deadlines, the *Air Pollution Control* court's reasoning is highly illuminating. The *Air Pollution Control* court was very critical of the fact that at no point did Jefferson County indicate that the EPA's failure to meet deadlines was because of "arbitrary and capricious" decision-making.[131] The court found that because there were "legitimate reasons" for the delay, the EPA's failure to meet the deadlines was presumptively not "arbitrary and capricious."[132]

This thinking could have changed the outcome of *Prometheus II*. In his dissent, Chief Judge Scirica opined that the challenging entities had notice of the proposed changes to the NBCO rule, and that the quicker notice-and-comment procedures employed by the FCC sufficiently apprised them of the ongoing nature of its consideration.[133] Chief Judge Scirica explained that there were several decisions over a long period of time that highlighted the ongoing nature of the FCC's consideration of the NBCO rule and that the further notice of proposed rulemaking (FNPRM) in 2006 was sufficient to keep the entities on notice.[134] In the context of Section 7607(d)(9)(D) procedural protections, the FCC had a "legitimate" reason for its employment of this procedure—it believed that the entities were sufficiently on notice—making the alleged NBCO procedural error insufficient to remand back to the FCC.[135]

North Dakota v. EPA indicates that unless the challenging entities could explain how the procedural violation was substantial enough that the rule would be "significantly changed," there could be no remand either.[136] The broadcasters in *Prometheus II* would have likely not have been successful in meeting this burden as the proposed NBCO rule in question was the same rule that was proposed a few years earlier—thus, demonstrating how the "procedural error" did not have a significant,

130. *See generally*, Air Pollution Control Dist. v. U.S. EPA, 739 F.2d 1071, 1079 (6th Cir. 1984); Prometheus Radio Project v. FCC (*Prometheus II*), 652 F.3d 431 (3d Cir. 2011).

131. *See Air Pollution Control Dist.*, 739 F.2d at 1079–80.

132. *See id.*

133. *See Prometheus II*, 652 F.3d at 472–75.

134. *See id.*

135. *See generally id.*

136. *See* North Dakota v. U.S. EPA, 730 F.3d 750, 758–759 (8th Cir. 2013) *cert. denied sub nom.* N. Dakota v. EPA, 134 S. Ct. 2662 (2014) (quoting 42 U.S.C. § 7607(d)(9)(D)).

substantive impact.[137] Without evidence of how the procedural error created a substantive impact on the final rule, the broadcaster's claims would have been insufficient to warrant a remand back to the FCC—if there were procedural protections for the FCC like those contained in the CAA.

Some degree of procedural protections will help the FCC be more effective in using its QR powers. While still subject to scrutiny regarding the substantive nature of its proposed rules, removing the power of regulated entities to challenge minor procedural infirmities of the FCC in the QR, would empower the FCC to fully realize the potential latent in the QR.

B. The Judicial System Can Lighten the Level of Scrutiny Applied to FCC Proposed Media Ownership Rules from the Quadrennial Review.

More broadly, the procedural protection provisions of the CAA could help protect the FCC's proposed media ownership rules by altering the applicable lens of judicial scrutiny for proposed rules or modifications under the QR. The procedural protections provision of the CAA also stands for "[t]he essential message of so rigorous a standard is that Congress was concerned that EPA's rulemaking not be casually overturned for procedural reasons, and we of course must respect that judgment."[138] This sentiment of respect to the agency's findings can be applied to the level of scrutiny applied by the courts in reviewing proposed media ownership rules during the QR.

1. The Current Scrutiny Applied to Proposed Media Ownership Rules Is Akin to A "Hard Look" and Should Be Lightened and More Deferential.

In *Prometheus I*, then-Chief Judge Scirica in his dissent, questioned the level of scrutiny the court was applying, arguing that it was improper and noting that he would have found that each proposal was sufficiently supported in the FCC record.[139] The "rigorous standard" for finding an error embodied in the CAA procedural protections provision, as applied to the QR, may guide the courts to employ a different lens of scrutiny which may uphold more FCC proposed rules—as Chief Judge Scirica would have held.

Even beyond the judicial scrutiny in the procedural protections provision, altering how thoroughly courts analyze FCC proposed rules may create a more effective QR. A "hard look" from the courts at agency action

---

137. *See Prometheus II*, 652 F.3d at 474 ("The *2006 FNPR* made clear that, on remand from *Prometheus I,* the FCC was planning a significant revision of the NBCO rule noticed by the *2001 NPRM* and appearing in the *2003 Order*, and was again considering tailoring cross-ownership limits to local markets. *See 2006 FNPR,* 21 FCC Rcd at 8848, ¶ 32.")

138. *See* Sierra Club v. Costle, 657 F.2d 298, 391 (D.C. Cir. 1981).

139. *See* Prometheus Radio Project v. FCC (*Prometheus I)*, 373 F.3d 372, 435 (3d Cir. 2004).

is not proper, and should be a more deferential approach to the agency determination[140]—should the agency have followed proper procedures (which the *State Farm* factors ensure).[141] But a "hard look" at the FCC's proposed media ownership rules is what occurs currently.

In *Prometheus I*, Chief Judge Scirica questioned the level of scrutiny being applied to FCC proposed rules:

> In my view, the Court's decision has upended the usual way the judiciary reviews agency rulemaking. Whether the standard is "arbitrary or capricious," "reasonableness," or some variant of a "deregulatory presumption," the Court has applied a threshold that supplants the well-known principles of deference accorded to agency decision-making. In so doing, the Court has substituted its own policy judgment for that of the Federal Communications Commission and upset the ongoing review of broadcast media regulation mandated by Congress in the Telecommunications Act of 1996.[142]

Chief Judge Scirica went further to explain that "[a]llowing the biennial (now quadrennial) review process to run its course will give the Commission and Congress the opportunity to monitor and evaluate the effect of the proposed rules on the media marketplace."[143]

Chief Judge Scirica argued that the way that the court analyzed the FCC's proposed rules was improper and harmed the effectiveness of the QR.[144] This line of argument—that courts are applying improperly thorough scrutiny, which then harms agency effectiveness—is exemplified best in *Ethyl Corp v. EPA*.[145] In *Ethyl Corp*, three Judges of the D.C. Circuit sitting *en banc* all posited different levels of scrutiny that the court should engage in when analyzing proposed EPA rules that followed Section 553 notice-

---

140. *See* Matthew Warren, *Active Judging: Judicial Philosophy and the Development of the Hard Look Doctrine in the D.C. Circuit,* 90 GEO. L.J. 2599, 2631–32 (2002).

141. Iterated in *Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29 (1983), the Supreme Court laid out a four part series of questions to ask in determining whether or not the agency rationale for any decision was arbitrary and capricious. The questions are: (1) did the agency rely on improper factors; (2) did the agency fail to consider a key component of the problem it was facing; (3) did the agency's final decision run contrary to the evidence before it; and (4) did the agency employ an explanation "so implausible" that it cannot be a result of the agency's expertise in the subject area and the data it had? *See* Glicksman & Levy, *supra* note 86, at 250; *Prometheus I*, 373 F.3d 440–41 (citing *Motor Vehicle Mfrs. Ass'n.*, 463 U.S. at 43).

142. *See Prometheus I*, 373 F.3d at 435.

143. *See id.*

144. *See id.* at 440 ("Although there are some similarities, I differ from the majority on the applicable standard of review. Moreover, I believe the majority's subsequent analysis oversteps the appropriate standard. In doing so, the majority substitutes its own judgment for policy decisions meant to be resolved by the Agency.").

145. *See* Ethyl Corp v. EPA, 541 F.2d 1, 66–70 (D.C. Cir. 1976) (Bazelon, C.J., concurring).

and-comment procedures.[146] The views ranged from a thorough scrutiny of the agency's proposed reasoning including highly technical areas of science, to avoiding the technical areas and analyzing strictly procedural compliance and thoroughness of reasoning.[147]

Since *Ethyl Corp*, the applicable lens of judicial scrutiny has been an issue for agencies attempting to promulgate rules. In the context of the QR, were the courts to lighten their scrutiny requiring a doctrinal shift, admittedly a tall task, the benefits would be enormous.

2. Lighter Scrutiny with Greater Deference to FCC Conclusions Would Allow the FCC to Be More Effective in Promulgating Rules During the Quadrennial Review.

Altering the applicable lens of judicial scrutiny has been considered as a potential solution to the ossification of the rulemaking process. In their articles targeting "deossification," four of seven solutions Professor proposes target the courts and their review of agency determinations and Professor McGarity discusses how altering the judicial review process may be a solution.[148] Specifically, in the context of rules proposed under the QR, *Fox I*, *Sinclair*, and *Prometheus I* all could have had the proposed rule upheld if the lens of review analyzing the substantive reasons for the proposed rule was slightly different. All the cases held that the FCC articulated at least *some* reasoning and rationale supporting its proposals, but that the record was insufficient to support those reasons, and thus, the rules

146. *See generally id*.

147. *See generally id.*

148. *See* Pierce, *supra* note 95, at 71–93; McGarity, *supra* note 17, at 1453 (employing a simile to describe proper lens of judicial review as "pass-fail prof" rather than current standard of "hard look" of evidence to indicate that despite disagreement with agency findings, a "pass-fail-prof"-court should only overrule if finding is arbitrary).

were remanded.[149] With a different scope of analysis, it is possible that the FCC's rules would have been upheld, which would have benefitted the QR because instead of employing the "hard look" scrutiny that has caused the FCC's rules to be rejected, the proposed rules would have stood. Generally, after the rules have been rejected by the court, the FCC reconsiders the matter in the next QR. If they were instead upheld, the FCC would have a standing baseline upon which it could build in subsequent QRs, which then could allow the FCC to allocate its resources to creating new rules to help transition to the Internet media age.

In *Prometheus I*, Chief Judge Scirica issued a forty-five page dissent finding each of the proposed rules amply supported in the FCC record.[150] His dissent started by iterating what he believed to be the proper scope of analysis—"arbitrary and capricious review" where the agency considers the relevant *State Farm* factors in determining whether or not the agency's reasoning was arbitrary and capricious:

> [T]he agency has relied on factors which Congress has not intended it to consider, entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise. The reviewing court should not attempt itself to make up for such deficiencies; we may not supply a reasoned basis for the agency's action that the agency itself has not given.[151]

The majority posited a similar standard.[152] However, the majority and dissent differed on the analysis applied to the evidence contained in the FCC

149. *See* Fox Television Stations, Inc. v. FCC (*Fox I)*, 280 F.3d 1027, 1036 (D.C. Cir. 2002), *modified on reh'g,* 293 F.3d 537 (D.C. Cir. 2002) ("The Commission gave three primary reasons for retaining the NTSO Rule. . . . In the *1998 Report* the Commission decided that retaining the CBCO Rule was necessary to prevent cable operators from favoring their own stations and from discriminating against stations owned by others. *1998 Report* ¶ 104 ('current carriage and channel position rules prevent some of the discrimination problems, but not all of them')."); Sinclair Broad. Grp. v. FCC, 284 F.3d 148 (D.C. Cir. 2002) ("Based on its finding that '[b]roadcast stations, particularly television stations, reach large audiences and are the primary source of news and entertainment programming for Americans,' and also because 'there remain unresolved questions about the extent to which [non-broadcast television] alternatives are widely accessible and provide meaningful substitutes to broad stations,' the Commission determined that the only medium to be counted for purposes of the 'eight-voices exception' is broadcast television, unlike the minimum voices exception in the radio-television cross-ownership rule, where certain local newspapers and cable television stations are counted."); *Prometheus I*, 373 F.3d at 386–88 (explaining FCC findings and reasoning in articulating its new media ownership rules); Prometheus Radio Project v. FCC (*Prometheus II*), 652 F.3d 431, 440–42 (3d Cir. 2011) (also explaining FCC findings and reasoning in articulating its new media ownership rules).

150. *See generally Prometheus I*, 373 F.3d at 435-80 (majority opinion).

151. *See Prometheus I*, 373 F.3d at 440–41 (citing Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983)).

152. *See Prometheus I*, 373 F.3d at 389-90.

record. The dissent argued that while there may have been errors in the reasoning of the FCC or questions that the court felt the FCC should have answered, those matters did not rise to the level of "arbitrary and capricious decision making" as indicated by the *State Farm* factors.[153] The majority, on the other hand, indicated that these unanswered or unaddressed elements of consideration were sufficient to overrule the FCC's determinations.[154]

The FCC in *Fox I* attempted to argue that its review of the media ownership rules under Section 202(h), and its determinations therein, should not be subject to judicial review.[155] The court rejected the FCC's arguments regarding statutory construction and the pragmatic argument advanced by the FCC to support its assertion and held that any determination under Section 202(h) is subject to judicial review.[156] Most important to this matter was the dismissive tone used by the court in rejecting the arguments advanced by the FCC.

In regards to the "pragmatic argument" employed by the FCC, the court held that the fact that the biennial reviews were subject to judicial review does not make the FCC's task more "burdensome" than if the final determinations of the FCC were not subject to subsequent judicial scrutiny.[157] This view, especially given the recent history of the QR and its numerous legal challenges, likely no longer would still be posited by the courts and was somewhat questionable to begin with considering the first review of media ownership rules was challenged and the subject of that very opinion. Overall, the court dismissed all of the legal and statutory construction arguments advanced by the FCC because of "the presumption that final agency action is reviewable" and the arguments advanced by the FCC did not provide "clear and convincing evidence" that this presumption should be overwhelmed.[158] Again, this conclusion by the court is questionable. Perhaps these arguments advanced by the FCC in *Fox I* should be given more credence or be regarded as further persuasive evidence that the current level of scrutiny applied is too demanding and should be lightened—at least to some degree.

While altering the level of judicial scrutiny is a broad solution, and would be difficult to implement,[159] its potential benefits to the QR and the FCC—and other agencies—is undeniable.

153. *See id.* at 445.
154. *See generally id.*
155. *See Fox I*, 280 F.3d at 1038–39.
156. *See id.*
157. *See id.* at 1039.
158. *See id.* at 1038–39 (citing Abbott Labs. v. Gardner, 387 U.S. 136, 140–41 (1967)).
159. *See* Pierce, *supra* note 95, at 95.

C. The FCC Can Elect to Issue Temporary Rules Along with Each Quadrennial Review to Avoid Immediate Legal Challenges to Its Proposed Rules.

Temporary rules are inherently less binding, expiring after a certain period of time.[160] By making the rules promulgated as part of the QR less binding and subject to immediate repeal if a secondary notice and comment series is not performed, regulated entities may be less "inclined to challenge [the rules]."[161] Professor McGarity discusses the fact that if the regulated entities know that a rule is subject to repeal, they may be less inclined to challenge it, especially provided the later, guaranteed notice and comment period.[162] While this seems somewhat circular in the context of the QR, which is already a later, guaranteed notice-and-comment period, "temporary rules" can still provide some benefit for the FCC and the regulated entities.

1. Temporary Rules Can Create an Opportunity for the FCC to "Experiment" and Gather Data Regarding Potential Rules or Amendments.

By changing the effectiveness and permanency of the FCC proposed rules under the QR, regulated entities may be less inclined to challenge the proposed rule. Primarily, this would allow the FCC to propose and issue rules that would be revisited at the next QR. Were the rule not to accomplish its purpose, the FCC—and regulated entities—would see the rule disappear with no further discussion. This solution would be amenable to both the FCC and the regulated entities. In order to make the temporary rule binding, the FCC would need to at the next QR propose the rule as "binding." This would give regulated entities a second bite at the apple to try and prove that the rule is not "in the public interest." These entities would be able to challenge the rule at its temporary stage and again when the rule was re-proposed as a binding rule. In the interim, the FCC would also be able to study the effects of the temporary rule as potential support to its final rule with sufficient evidence to survive legal challenges.[163]

---

160. *See* McGarity, *supra* note 17, at 1460 (proposing "tentative" rules as a solution for "deossification.")

161. *See id.*

162. *See id.*

163. *See, e.g.*, Fox Television Stations, Inc. v. FCC (*Fox I)*, 280 F.3d 1027, 1042 (D.C. Cir. 2002), *modified on reh'g,* 293 F.3d 537 (D.C. Cir. 2002) ("As the networks point out, however, 'such figures alone, without some *tangible evidence* of an adverse effect on the market, are insufficient to support retention of the Cap.' Finally, the Commission's reference in the *1998 Report* to the national advertising and the program production markets is wholly *unsupported and undeveloped*. . . . Consequently, we must conclude, as the networks maintain, that the Commission has no valid reason to think the NTSO Rule is necessary to safeguard competition." (emphasis added) (citation omitted)).

Essentially, the temporary rules would provide an "experiment period" for the FCC and regulated entities.[164] Temporary rules, used as experimental rules, are not very common and comprise a fraction of rules issued by an agency.[165] These temporary rules could empower the FCC to grant short-term, limited waivers to some of its standing rules—which follows along with the "deregulatory presumption" of the QR.[166] These "waiver periods" could then be analyzed to see if the FCC's goals were served or if the waiver were not "in the public interest." Alternatively, the FCC could issue rules, which lower various ownership caps in specific markets to determine if there is any benefit seen in "diversity, localism and competition." If the FCC did see the benefits it desired in the experimental market, it could reassert that temporary rule in the following QR and make the rule binding because it would have adequate support on the record from the experimental period to survive a subsequent challenge.

2. The Data from the Experimental Period Can Be Used by the FCC to Support Final Rules and Reduce Subsequent Litigation.

Collecting information during this experimentation period would allow the FCC to issue binding rules, which could survive legal challenges while allowing regulated entities a second opportunity to petition for altering a rule or maintaining it. As Professor McGarity further argued, temporary rules would have even greater value where "new information is constantly becoming available."[167] For the FCC and the QR, gathering more data during the "experimental" temporary rules period follows closely with this idea of "new information" being gathered, as well as the fact that in the context of changing media consumption avenues, new information is going to arise.

A prime example of a situation where the potential benefits of the FCC's use of experimental rules could have arisen is the "eight voices exceptions" issue addressed above. Had the FCC employed an experimental rule, using a single market to test out "nine voices" and another market to

164. *See* Zachary J. Gubler, *Experimental Rules*, 55 B.C. L. REV. 129 (2014). Experimental or temporary rules sound like they exist through a loophole, but are generally well established and function through the use of a "sunset" provision which sets when the rule will expire. *See* Jacob E. Gersen*, Temporary Legislation,* 74 U. CHI. L. REV. 247, 248–49 (2007)

165. *See* Gubler, *supra* note 164, at 149–50, 152 (finding one percent of all Securities and Exchange Commission rules to be experimental rules and explaining "[f]or example, during the same decade-long period ending on December 31, 2011, the Commodity Futures Trading Commission promulgated 259 rules, yet only two of these (0.8%) were structured as experimental rules. The results are similar at the Federal Trade Commission (0.8%), the National Transportation Safety Board (none), and the Federal Energy Regulatory Commission (none)").

166. *See* Prometheus Radio Project v. FCC (*Prometheus I)*, 373 F.3d 372, 384 (3d Cir. 2004).

167. *See* McGarity, *supra* note 17, at 1460.

test out "seven voices," the FCC would have had more data regarding the effects of any given number of "voices" in a market. The FCC's final determination of eight—or any other number—would then have been justified sufficiently with evidence, meaning that when the next QR was around, the FCC could amend the rule or sufficiently justify its rule without amending it.[168] While it may take more time for the FCC to finalize its rules, it would be more efficient because it would be apparent to all regulated entities and other interested parties that after the experimental rule, the FCC *does* have the data to back up its final rule.

Equally important, for each challenge where the line drawn by the FCC is deemed "arbitrary" or "lacking sufficient support," the FCC would, under the theory behind experimental rules, be able to gather sufficient information to justify its determinations. While an inherently circular argument—temporary rules provide a solution to rules that must be reviewed every four years—temporary rules may provide an amenable solution to both regulated entities and the FCC. Further, these rules provide an opportunity for the FCC to act by itself to free the QR from its current stagnant place, another inherent efficiency to this solution.

IV. CONCLUSION

With media consumption avenues changing, the FCC is currently empowered to lead the way and help the average consumer safely reach the media. The QR provides that power for the FCC. But with the QR ossified and the need for guidance as the transition from print and television media to online media looms, some changes must be made to free the QR and the FCC. Congress, the courts, and the FCC can act to help free the QR. In terms of efficiency, were Congress to prescribe that the FCC conduct hybrid rulemaking procedures, similar to those contained with the Clean Air Act, the FCC would likely see its proposed rules upheld more frequently. Further, it could signal to the courts that the scrutiny applied needs to change as well—two solutions in one action. But the easiest solution would be for the FCC to elect to issue temporary rules under the QR, instead of binding rules, in order to potentially avoid legal challenges to its determinations. In any event, the time is now for Congress, the courts, or the FCC to act to help free the QR.

168. *Cf. 2010 & 2014 Quadrennial Review*, *supra* note 4, at para. 53–59.

An New Dog With the Same Old Tricks: The Government's Open Data Initiatives

Monica Savukinas *

TABLE OF CONTENTS

* J.D., The George Washington University Law School, May 2017.

I. INTRODUCTION

Throughout modern history, prizes have been a key motivation behind the development of numerous technologies that today we take for granted. For example, in the late 1700s, the French government used a prize contest to push innovators to develop a new food preservation technology to better feed Napoleon's army.[1] The winner received 12,000 franc and the resulting technology eventually led to the modern process of canned foods.[2] The use of cash rewards for innovation has not been limited to governments. In 1919, Raymond Orteig, a New York hotel owner who was born in Paris, offered $25,000 for completion of the first successful transatlantic flight from New York to Paris.[3] In 1927, Charles Lindbergh won that prize in the Spirit of St. Louis.[4]

Since 2009, the number of Open Data Initiatives (ODIs) sponsored by government agencies has increased dramatically.[5] These activities have seen a resurgence in recent years thanks, in large part, to President Barack Obama's actions to make additional funds available for ODIs and to push Congress to create statutory authority for agencies to host these initiatives.[6] Common goals cited in support of these events, besides the development of new technologies, are to obtain a broad range of participants, to be of low cost to the government, increased private investment, education and captivation of the public, and increased competition.[7] These contests have been particularly successful in highly technical fields, such as the National Aeronautics and Space Administration's (NASA) Lunar Lander Challenge.[8]

---

1. *See* DEBORAH S. STINE, CONG. RESEARCH SERV., R40677, FEDERALLY FUNDED INNOVATIVE INDUCEMENT PRIZES 1 (2009).

2. *Id.*

3. *See* Tim Brady, *The Orteig Prize*, 12 J. AVIATION/AEROSPACE EDUC. & RESEARCH 45, 46 (2002).

4. *Id.* at 58-59.

5. *See About*, CHALLENGE.GOV, https://www.challenge.gov/about [https://perma.cc/DX4Y-3SFU] (last visited Apr. 7, 2017) (stating that since 2010, over 740 competitions were launched with more than $250 million award in prizes).

6. *See* Gottlieb & Rawicz, Federal Inducement Prizes, 15-9 Briefing Papers 1 (2015); *but see* Office of Mgmt. & Budget, Exec. Office of the President, *Information for Agencies Memoranda*, https://www.whitehouse.gov/omb/information-for-agencies/memoranda [https://perma.cc/U6WL-QAJG] (no mention of the use of challenges or prize contests in memoranda issued by the Trump administration).

7. *See* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES ON GUIDANCE ON THE USE OF CHALLENGES AND PRIZES TO PROMOTE OPEN GOVERNMENT 1-2 (Mar. 8, 2010) [hereinafter Guidance on the Use of Challenges and Prizes], http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-11.pdf [https://perma.cc/QJH3-Y7UY]; NATIONAL ACADEMY OF ENGINEERING, CONCERNING FEDERALLY SPONSORED INDUCEMENT PRIZES IN ENGINEERING AND SCIENCE 1 (April 30, 1999), http://www.nap.edu/catalog/9724.html [https://perma.cc/FJ5Q-RY83]; Stine, *supra* note 1, at 2.

8. *See* Stine, *supra* note 1, at 16-17 ("For the Lunar Lander Challenge, twelve private teams spent nearly 70,000 hours and the equivalent of $12 million trying to win $2 million in prize money.").

The most common example of an ODI is a prize contest. Simply put, in a prize contest, the government offers a set award, typically a monetary sum and occasionally a government contract, in return for achieving a set goal with pre-determined criteria.[9] There are two categories of prize contests – recognition prizes and incentive or inducement prizes.[10] Recognition prizes award work done in the past for a purpose other than the contest itself, such as the Nobel Peace Prize.[11] Incentive or inducement prizes award work done specifically for a set contest or goal.[12] This note focuses on and uses the term "prize contests" in reference to an incentive or inducement prize.

In recent years, several agencies have begun to host and sponsor events known as hackathons as part of this push for ODIs.[13] Hackathons go by many names, such as codeathons, developer days, apps challenges, hackfests, hackdays, or codefests.[14] Hackathons are typically shorter than prize contests, as they are generally held in a single weekend.[15] Hackathons can be used to push for innovation within an agency,[16] or to spur innovation in the private sector overseen by the agency.[17]

Another innovation strategy gaining in popularity is for agencies to work directly with developers to provide the necessary tools for private innovation.[18] These tools include open data and Application Programming Interfaces (APIs).[19] An API is like the buttons on a calculator – it is the

---

9. *See* Steven L. Schooner & Nathaniel E. Castellano, *Eyes on the Prize, Head in the Sand: Filling the Due Process Vacuum in Federally Administered Contests*, 24 FED. CIRCUIT B.J. 391, 399-400 (2015).

10. *See* Guidance on the Use of Challenges and Prizes, *supra* note 7, at 3 ("Experts often make a distinction between 'recognition' prizes that honor past achievements, and 'inducement' or 'incentive' prizes that encourage participants in the competition to achieve a particular goal").

11. *Id.*

12. *Id.*

13. *See generally Hackathon for Combat Feeding Mobile Apps*, U.S. DEP'T DEFENSE, http://combatfeedinghack.devpost.com/ [https://perma.cc/JF9A-BMUB] (last visited Apr. 9, 2016) (hosted by the Department of Defense); *GSA Digital Innovation Hackathon*, GEN. SERVS. ADMIN., http://open.gsa.gov/Digital-Innovation-Hackathon-Fall2015/ (last visited Nov. 6, 2015); *International Space Apps Challenge*, NAT'L AERONAUTICS & SPACE ADMIN., https://2016.spaceappschallenge.org/ (last visited Apr. 9, 2016); *Earth Day Hackathon*, Gen. Servs. Admin, http://open.gsa.gov/EarthDayHackathon/ (last visited Apr. 9, 2016) (co-hosted by six agencies).

14. *See* ZACHARY BASTIAN, THE POWER OF HACKATHONS: A ROADMAP FOR SUSTAINABLE OPEN INNOVATION, WASHINGTON, DC: WOODROW WILSON INTERNATIONAL CENTER FOR SCHOLARS 1 (2013), https://www.wilsoncenter.org/sites/default/files/power_hackathons.pdf; Melissa Phipps, *Collaboration Meets Competition: The Power of the Hackathon*, Gen. Assembly Blog, https://blog.generalassemb.ly/collaboration-meets-competition-power-hackathon/ (last visited Oct. 11, 2015).

15. *See* Bastian, *supra* note 14, at 1; Phipps, *supra* note 14.

16. *See* Earth Day Hackathon, *supra* note 13 (GSA Simplying Sustainable Procurement hackathon to "[m]ake it easier for contracting officers to determine whether products on the web meet federal sustainability requirements.").

17. *Id.* (USDA hackathon to "[d]evelop a prototype of a tool that allows users to quickly and easily access shade scores for any neighborhood in the United States.")

18. *See Reports and Research: Data*, FCC, https://www.fcc.gov/reports-research/data (last visited Jan. 20, 2015).

19. *See id.*

interface that allows a user to submit inputs and then returns an output. In addition to his support for ODIs, President Obama has also pushed federal agencies to increase the availability of open data.[20] In a 2013 executive order, President Obama specifically ordered agencies to make resources, such as data, open and available in a machine readable format usable to the public in order to "fuel entrepreneurship, innovation, and scientific discovery."[21]

This notes analyzes the Federal Communications Commission's (FCC's) use of ODIs and open data as part of the government's push for innovation at federal agencies. It begins with a discussion, including benefits and deficiencies, of three innovation tools – prize contests, hackathons, and open data. Next, Part III discusses the White House's innovation policy and goals, both for the federal government at large and specifically for the FCC. The latter portion includes a brief overview of the structure and history of the FCC, with a particular focus on the FCC's technical resources. Part IV discusses the implications of the FCC's use of these innovation tools on the technology and communication sectors, arguing that the FCC should increase its use of prize contests, hackathons, and open data to encourage innovation.

II. RECENT INNOVATION TOOLS: NEW NAMES, SAME OLD CONCEPTS

While the monikers for recent innovation tools, such as hackathons, might be relatively new, the concepts are no different than in the days of Napoleon and Lindbergh. The core motivator behind the creation of these tools is the exchange of innovation for a reward – whether it be cash, publicity, or a government contract.

A. Prize Contests: An Old Dog with Same Old Tricks

Prize contests are tools that governments across the globe and private parties have used for centuries to spur innovation.[22] Some examples include the Government of the French Republic's prize to develop a better way to preserve food for soldiers and the Orteig Prize for the first non-stop flight from New York to Paris, which was awarded to Charles Lindbergh.[23]

---

20. *See generally* Office of the Press Secretary, Exec. Office of the President, *Executive Order – Making Open and Machine Readable the New Default for Government Information* (May 9, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government- (hereinafter *Executive Order on Open Data*); *but see* https://www.whitehouse.gov/, White House, (no memoranda related to open data issued by the Trump administration based on a lack of relevant results for the search term "open data").

21. *Id.*

22. Stine, *supra* note 1, at 1.

23. *Id.*; Schooner & Castellano, *supra* note 9, at 392.

1. Authority and Guidance for Prize Contests Are Not Straightforward

While prize contests have been used for centuries,[24] most of the current statutory authority related to these contests is not straightforward. In 2007, President George W. Bush signed the America COMPETES Act into law.[25] The purpose of the Act was "[t]o invest in innovation through research and development, and to improve the competitiveness of the United States."[26] This Act appropriated funds to select agencies for various initiatives, including prize contests.[27] Early in his presidency, President Obama vocalized his support for prize contests as a tool for innovation.[28] In March 2010, the White House Office of Management and Budget (OMB) issued a memorandum to the heads of executive departments and agencies, outlining how agencies could implement prize contests.[29] This included a description of how departments and agencies could host prize contests without direct statutory authority.[30] The Trump administration has issued no guidance, positive or negative, on the use of prize contests.[31]

In 2010, President Obama signed the reauthorization of the America COMPETES Act into law.[32] This Act amended the Stevenson-Wydler Technology Innovation Act (Stevenson-Wydler Act) to specifically grant authority to all departments and agencies to conduct prize contests.[33] The

24. Stine, *supra* note 1, at 1.

25. *See* America Competes Act, Pub. L. No. 110-69, 121 Stat. 573 (2007).

26. *Id.*

27. *See generally id.* at Title II (National Aeronautics and Space Administration), Title III (National Institute of Standards and Technology), Title IV (National Oceanic and Atmospheric Administration), Title V (Department of Energy), Title VII (National Science Foundation).

28. *See generally* Tom Kalil & Robynn Sturm, *Congress Grants Broad Prize Authority to All Federal Agencies*, WHITE HOUSE: BLOG (Dec. 21, 2010), https://obamawhitehouse.archives.gov/blog/2010/12/21/congress-grants-broad-prize-authority-all-federal-agencies. [https://perma.cc/AVL3-3AD]

29. *See* Guidance on the Use of Challenges and Prizes, *supra* note 7, at 1.

30. *Id.* at 5-10 (explaining how authority might exists in one of the following: grants and cooperative agreements, necessary expense doctrine, authority to provide non-monetary support, procurement authority, other transactions authority, agency partnership authority, public-private partnership authority).

31. *See generally* White House, https://www.whitehouse.gov/. (last visited Nov. 25, 2017).

32. *See generally* John P. Holdren, *America COMPETES Act Keeps America's Leadership on Target*, White House: Blog (Jan. 6, 2011), https://obamawhitehouse.archives.gov/blog/2011/01/06/america-competes-act-keeps-americas-leadership-target.

33. America Competes Reauthorization Act of 2010, Pub. L. No. 111-358, § 105, 124 Stat. 3989, (2010) ("In General.-The Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3701 et. seq.) is amended by adding at the end the following: Sec. 24 Prize Competitions . . . . (b) In General.-Each head of an agency, or the heads of multiple agencies in cooperation, may carry out a program to award prizes competitively to stimulate innovation that has the potential to advance the mission of the respective agency." (quotation marks omitted)).

America COMPETES Act expired in 2013 and has not been renewed,[34] but the Stevenson-Wydler Act still stands as amended.[35] The Stevenson-Wydler Act provides broad guidance on how to set-up and run a prize contest, including different contest structures,[36] participant eligibility,[37] liability,[38] intellectual property,[39] and funding.[40] The language in these sections is vague and provides little guidance to agencies. For example, the intellectual property section contains two sentences stating that an agency needs a participant's written consent to gain an intellectual property (IP) interest in a submission and that an agency may negotiate for a license to use IP developed for a competition.[41]

In administering a prize contest, agencies and departments can rely either on the Stevenson-Wydler Act,[42] or one of the other authorities outlined in the OMB's 2010 memorandum.[43] In forming and implementing these contests, agencies are given wide latitude so as to develop a contest that fits with the goals and resources of that particular agency.[44] The agency does not necessarily need to fund or administer the contest.[45] Rather, agencies are able, and encouraged, to work with third parties in administering contests.[46] Given the wide range of discretion and the varying goals and interests of government agencies, contests have ranged anywhere from a few days with no prize money,[47] to a multi-year contest with a $900,000 grand prize.[48] Since

34. *See* Jon Groteboer, *Update on America COMPETES Reauthorization Act of 2015*, Harv. Off. Sponsored Programs: Blog (June 8, 2015), http://osp.finance.harvard.edu/blog/update-america-competes-reauthorization-act-2015 (noting that the House of Representatives passed a reauthorization of the Act in 2015).

35. *See* The Stevenson-Wydler Technology Innovation Act of 1980, 15 U.S.C. § 3719(b) (2016) ("Each head of an agency, or the heads of multiple agencies in cooperation, may carry out a program to award prizes competitively to stimulate innovation that has the potential to advance the mission of the respective agency.").

36. *See* 15 U.S.C. § 3719(c).

37. *See* 15 U.S.C. § 3719(g).

38. *See* 15 U.S.C. § 3719(i).

39. *See* 15 U.S.C. § 3719(j).

40. *See* 15 U.S.C. § 3719(m).

41. *See* 15 U.S.C. § 3719(j).

42. *See generally* 15 U.S.C. § 3719.

43. *See* Guidance on the Use of Challenges and Prizes, *supra* note 7, at 5-10.

44. *Id.* at 3; 15 U.S.C. § 3719(c-d).

45. Stine, *supra* note 1, at 21-22; 15 U.S.C. § 3719(m)(1) ("Support for a prize competition…may consist of Federal appropriated funds and funds provided by the private sector for such cash prizes. The head of an agency may accept funds from other Federal agencies to support such competitions.").

46. *See* Guidance on the Use of Challenges and Prizes, *supra* note 7, at 5; 15 U.S.C. § 3719(m).

47. *See Developing with Accessibility*, FCC, https://www.fcc.gov/events/developing-accessibility (last visited Apr. 9, 2016) (two-day event hosted by the FCC in 2012 to "promote the concept and practice of developing applications within accepted accessibility guidelines, thereby mazimizing their usability for everyone, including persons with disabilities").

48. *See Power Beaming Challenge*, NAT'L AERONAUTICS & SPACE ADMIN., http://www.nasa.gov/offices/oct/early_stage_innovation/centennial_challenges/beaming_tether/ (last visited Mar. 1, 2016) ("NASA and the Spaceward Foundation awarded $900,000 to LaserMotive LLC of Seattle, WA for their winning performance in the Power Beaming Challenge competition at the NASA Dryden Flight Research Center" after holding competitions in 2005, 2006, 2007 and 2009).

agencies are given broad discretion over how to organize their ODIs,[49] it is up to the agency to determine whether a long-term event is more appropriate, or whether the agency's needs are better served by a short-term event.

B. Prize Contests Benefits Are Clear for the Government, Yet Uncertain for Participants

The prize contest benefits to the government are quite clear. One of the most important benefits is that the investment risk of innovation shifts from the government to the private sector while providing the government access to new talent, entrepreneurs, and technology.[50] Under a prize contest, the government only awards a prize if and when a participant achieves the objective.[51] Under a standard government contract, however, the government awards the prize before the contractor even begins the work.[52] Since prize contests typically do not have any educational or experiential requirements, the government has the opportunity to hear from relatively unknown participants that otherwise would be shut out from a government contract.[53]

While the benefits of prize contests to the participants are not as certain, there are some known benefits outside of the government. For starters, it is clear that the private sector benefits from increased investment in innovation, typically at a value above the prize itself.[54] Further, if there is a winner, he or she typically receives some type of monetary benefit.[55] However, sometimes this sum may barely cover the participant's expenses.[56] Besides monetary benefits, there are intangible benefits for the winner, such as free publicity,

---

49. *See* Guidance on the Use of Challenges and Prizes, *supra* note 7, at 3-5.

50. *See Prizes and Challenges*, White House Off. Soc. Innovation & Civic Participation, https://obamawhitehouse.archives.gov/administration/eop/sicp/initiatives/prizes-challenges (last visited Apr. 9, 2016) (listed benefits include: "Pay only for success and establish an ambitious goal without having to predict which team or approach is most likely to succeed. Expand the government's reach to citizen solvers and entrepreuners of diverse backgrounds, skillsets, and experience").

51. *See* Schooner & Castellano, *supra* note 9, at 399.

52. *See* Schooner & Castellano, *supra* note 9, at 393-94.

53. *Id.* at 402.

54. *See generally* Nat'l Econ. Council et al., A Strategy for American Innovation: Securing Our Economic Growth and Prosperity 12 (2011), https://obamawhitehouse.archives.gov/sites/default/files/uploads/InnovationStrategy.pdf ("Under the right circumstances, prizes have a number of advantages over traditional grants and contracts. Prizes allow the sponsor to set an ambitious goal without selecting the team or approach that is most likely to succeed, to increase the number and diversity of minds tackling tough problems, to pay only for results, and to stimulate private-sector investment that is many times greater than the cash value of the prize.").

55. *See* Gottlieb & Rawicz, *supra* note 6, at 2 ("Government payout occurs only if an acceptable solution is presented.").

56. *See* Schooner & Castellano, *supra* note 9, at 400-01 ("For example, the winner of the Goldcorp Challenge reported that…the values of the prize barely covered their expenses…").

reduced barriers to entry,[57] access to government resources, and networking.[58] Further, the winner can receive prestige and recognition at an accelerated pace that cannot be quantified.[59] Some contest winners even receive government contracts.[60] For small entrepreneurs, winning one of these contests could be the jumpstart they need to launch a successful business. While losing participants could also gain some of these intangible benefits, they almost certainly lose their monetary investment. [61]

1. Legal Uncertainity: The Great Unknown of Prize Contests

For winning and losing participants alike, one drawback to prize contests is the lack of legal precedent related to these events. There is no clear legal procedure to challenge a decision and no certain liability structure exists.[62] An example of this problem is the Federal Trade Commission's (FTC's) Robocall Challenge.[63] In 2012, the FTC held a prize contest, called the Robocall Challenge, in which the agency asked participants to develop technology that could identify and block robocalls.[64] The FTC offered $50,000 in cash participant with the winning solution.[65] The FTC ultimately split the award between two participants - Serdar Danis and Aaron Foss.[66]

---

57. *Id.* at 394-95, 401.

58. *See* Stine, *supra* note 1, at 7 (benefits to competitors of a Department of Defense competition included "access to DOD-paid and validated laboratory grade testing in close-to-operatinal conditions, and to DOD civilian and military professionals who provided direct feedback and real-time techicial assessments. Competitors were also able to interact with other teams, which enhanced collaborative discussions and networking opportunities on topics of common interest.").

59. *See* Schooner & Castellano, *supra* note 9, at 400-01 ("For example, the winner of the Goldcorp Challenge reported that… 'it would have taken [our company] years to get the recognition in North America that this [single] project gave us overnight.' SpaceX, the 2004 winner of the XPrize competition, quickly morphed from an upstart, relatively unknown rival into a feared maverick, capturing a significant market share from the well-established aerospace industry titans.").

60. *Id.*

61. *Id.* at 395 ("For every ebullient prizewinner, contests breed potentially unlimited losers, many of whom invested heavily in their efforts."); Gottlieb & Rawicz, *supra* note 6, at 2 ("there usually are more losers than winners.").

62. *See* Schooner &Castellano, *supra* note 9, at 396 ("[T]here is no evidence that the U.S. government has anticipated prize contest disputes, let alone provided an obvious, well-defined, or straightforward means for contestants to obtain judicial or administrative review or, more broadly, any form of due process to resolve those disputes."); Gottlieb & Rawicz, *supra* note 6, at 6 ("The authors of this paper have not seen the adoption of any such appeal procedures in agency prize contests under the Stevenson-Wydler Act.").

63. *See generally* Frankel v. U.S., 118 Fed. Cl. 332 (2014) (holding that CFC had jurisdiction to hear a challenge to the winner of a prize contest, but lacked jurisdiction to award the injunctive relief sought).

64. *See FTC Robocall Challenge*, Devpost, http://robocall.devpost.com/ (last visited Jan. 20, 2015).

65. *Id.*

66. *See generally FTC Announces Robocall Challenge Winners*, FTC (April 2, 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-announces-robocall-challenge-winners.

David Frankel, who entered the challenge, but did not win, filed a protest with the Government Accountability Office (GAO), arguing that the FTC did not abide by the rules of the contest.[67] The GAO ultimately dismissed Mr. Frankel's claim for lack of jurisdiction because "the Contest did not involve an award or proposed award of a contract."[68] Mr. Frankel next brought a breach of contract claim before the United States Court of Federal Claims (CFC).[69] While the CFC agreed that it had jurisdiction to hear Mr. Frankel's breach of contract claim, the Court found that it lacked jurisdiction to award the injunctive relief sought by Mr. Frankel.[70] The CFC held that because the Robocall Challenge was not a "procurement," Mr. Frankel could not obtain injunctive relief.[71]

By denying Mr. Frankel injunctive relief, the CFC made it difficult for Mr. Frankel, and future contest participants, to recover significant damages.[72] As discussed above, it is common for the monetary incentive to be insignificant when compared to the prestige and free publicity that comes with winning.[73] With no definitive legal structures in place to challenge the FTC's selection of a contest winner, participants may think twice about investing their time and resources in such contests.[74] This limitation could further deplete the number of participants in such contests,[75] and make it less likely that a prize contest will showcase the best and brightest work.

C. Hackathons: A New Dog with the Same Old Tricks

While a "hackathon" might sound novel, it is basically a shorter, less lucrative prize contest. Similar to the resurgence in prize contests, hackathons have gained popularity in recent years, particularly in the technology sector.[76] There is not a strict definition for a hackathon, but there are some basic characteristics.[77] For example, whereas in a prize contest almost all of the work takes place at separate sites over a period of days to months, hackathons take place at one site typically from one day to no more than a week.[78] Hackathons started informally in the 1990s, and began to gain wider attention

67. *Frankel*, 118 Fed.Cl. at 334.
68. *Id.*
69. *Id.*
70. *Id.* at 335 ("Having reviewed plaintiff's complaint, defendant's motion [to dismiss], and the briefing on that motion, this court believes that it has jurisdiction to consider plaintiff's breach of contract claim, which also appears to state a claim under RCFC 12(b)(6), but lacks jurisdiction to consider plaintiff's requests for injunctive relief.").
71. *Id.* at 336-37 ("the Federal Circuit…rejected the argument that section 1491(b)(1) grants this court protest jurisdiction over non-procurement disputes." (citing Res. Conservation Group, LLC v. U.S., 597 F.3d 1238, 1244-45 (Fed.Cir. 2010)) (citations omitted)).
72. *See* Ralph C. Nash, *Breach of Contest Rules: The Court of Federal Claims has Jurisdiction*, 28 Nash & Cibinic Rep. 148, 148 (2014).
73. *See* Schooner & Castellano, *supra* note 9, at 400-01.
74. *See* Schooner & Castellano, *supra* note 9, at 398 ("At worst, hiding the jurisdictional ball may dissuade future participation in prize contests.").
75. *See id.*
76. *See* Phipps, *supra* note 14.
77. *See* Bastian, *supra* note 14, at 1.
78. *See* Phipps, *supra* note 14.

at the latter end of that decade.[79] Since that time, technology companies have sponsored both internal and external hackathons to spur innovation.[80] While hackathons typically have some type of monetary reward, they also provide the possibility that a big investor will see an idea and sponsor it.[81] In recent years, hackathons have expanded from the technological field into politics, minority achievement, sports, the media,[82] and cross-border transactions.[83]

1. Hackathons Have All The Benefits of Prize Contests

Like prize contests, hackathons have the ability to attract a wide variety of participants, including small, entrepreneurial players who otherwise might not have the opportunity to compete for such prizes.[84] Further, hackathons allow governments to see and evaluate a broad range of ideas that might otherwise be absent from policy considerations[85] and to engage and educate the public.[86] In order for a government hackathon to be a successful event, a hackathon must have "organizational support, open data, careful planning and managed expectations."[87] Agencies can host hackathons on their own,[88] in partnership with other agencies,[89] or as a public-private partnership.[90] A

79. *Id.*

80. *Id.* (stating that Facebook's Like button, timeline feature, and gender identification options were there result of internal hackathons, and that Google, Yahoo!, and Foursquare have held external hackathons open to attendees inside and outside of the company).

81. *Id.* ("The most well-known story of hackathon startup success is GroupMe, which was born out of TechChrunch's Disrupt NYC hackathon in 2010. The company went on to be acquired by Skype for $85 million just a year later.").

82. *Id.* ("Last year a group in Pakistan held a hackathon to solve political issues. At Startup Weekend Oakland earlier this year there was a hackathon for black male achievement. Public Broadcasting's POB series has regular hackthons to reinvent documentaries on the Web. A Spartan hack event in August is designed to help improve the sport of obstacle course racing.").

83. *See* Alexander Panetta, *Teams of Computer Coders Gather to Tackle Canada-U.S. Border Snags*, Toronto Metro News (Feb. 25, 2016, 4:44 PM), http://www.metronews.ca/news/canada/2016/02/25/teams-of-computer-coders-gather-to-tackle-canada-u-s-border-snags.html (weekend hackathons in Chicago and Toronto to develop "software that slashes through the red tape that gums up trade across the Canada-U.S. border").

84. *See* Stuart Minor Benjamin & Arti K. Rai, *Fixing Innovative Policy: A Structural Perspective*, 77 GEO. WASH. L. REV. 1, 13 (2008).

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

86. *See* Stine, *supra* note 1, at 1-2.

87. Bastian, *supra* note 14, at 4.

88. *See generally*, *Hackathon for Combat Feeding Mobile Apps*, *supra* note 13 (hosted by the U.S. Army Natick Soldier Research, Development, and Engineering Center).

89. *See generally Earth Day Hackathon*, *supra* note 13 (co-sponsored by six agencies).

90. *See generally Canada-US Hackathon: Get North America Trading Again*, ILL. INST. TECH. IDEA SHOP [hereinafter *Canada-US Trading Hackathon*], https://crossborderhackathonchicago.splashthat.com/ (last visited Apr. 9, 2016) (organized by the Department of Homeland Security, State Department, the US Chamber of Commerce, Dickinson-Wright, and Northof41.org with corporate sponsors such as Amazon, Salesforce.com, IBM, and Microsoft).

public-private partnership could increase the size of the prize[91] or the resources at the event itself,[92] both of which could increase participation in the hackathon.

2. But, Hackathons Come with a Unique Set of Baggage

While hackathons share many of the benefits and drawbacks of prize contests, they have their own unique set of problems.[93] Even though hackathons are typically a low-cost investment, they may involve more cost and planning than a traditional prize contest.[94] Prize contest participants can have a vast geographic background.[95] A hackathon, however, requires a physical location, as well as resources and supplies, including reliable wireless access, data, and even snacks.[96] Without standardized datasets, it is difficult to achieve, much less sustain, a working and beneficial product.[97] A more detailed discussion of how the push for the FCC to use open data to solve this problem follows in the next section. Despite the costs incurred by the host of a hackathon, it may still be a more cost-effective strategy than investing internal resources to develop the needed technology.[98]

Hackathons also pose a problem for the government in that, unlike prize contests, they do not necessarily shift the investment risk away from an agency. It is not uncommon for hackathons to be one-off projects that lose steam once the event ends.[99] At the end of a hackathon, it is possible, and common, for no one to achieve the end goal of creativing a viable solotion to the particular challenge.[100] Whereas if no one succeeds in a prize contest, the government can simply never award the prize. Equally troublesome is the fact that the government is unlikely to get back the costs incurred from the space and resources provided in a hackathon, even if no one achieves the stated objective.

---

91. 15 U.S.C. § 3719(m)(1) ("[F]inancial support for the design and administration of a prize competition or funds for a cash prize purse…may consist of Federal appropriated funds and funds provided by private sector for-profit and nonprofit entities.").

92. *See Canada-US Trading Hackathon*, *supra* note 89 ("We have also assembled a top notch list of corporate partners . . . to have the most cutting edge platforms for teams to utilize as part of their project submissions . . . .").

93. *See App Contests are Stupid*, Chief Seattle Geek Blog (Jul. 2, 2013), https://schrier.wordpress.com/2013/07/02/apps-contests-are-stupid/.

94. *See* Bastian, *supra* note 14, at 5 ("Planning a hackathon is impossible without hardworking staff and support from Agency leadership.").

95. *See* Stine, *supra* note 1, at 17 ("A measure of diversity is seen in the geographic distribution of participants (from Hawaii to Maine) that reaches far beyond the locales of the NASA Centers and major aerospace industries.").

96. *See* Phipps, *supra* note 14.

97. *See App Contests are Stupid*, *supra* note 93; Bastian, *supra* note 14, at 1.

98. *See* Bastian, *supra* note 14, at 9 ("[A]mbitious goals are hampered by the reality of overstretched budgets and limited resources.")

99. *See* Stine, *supra* note 1, at 2.

100. *See* Bastian, *supra* note 14, at 8-9 ("it is unlikely that a working application can be developed in a weekend.").

An additional issue with hackathons may be the difficulty in attracting top talent. Hackathons are commonly hosted in a set, physical location where participants must be present to participate.[101] If there are significant time and travel costs, it is unlikely that entrepreneurial startups would have the money to travel to the event. Additionally, since the monetary reward is typically less lucrative than prize contests,[102] there is less incentive to spend time and resources in participating. Some larger, annual hackathons allow for remote participation, but that is not always an option.[103]

A further challenge is that there is little to no statutory authority for hackathons.[104] As discussed above in the Robocall Challenge litigation, participants may be discouraged from participating if there is no due process structure in place.[105] Besides due process concerns, hackathons have the additional problem that there is no clear authority for the government to award a prize in the first place. While hackathons can be analogized to short-term prize contests, and thus fall under the America COMPETES Act amendment to the Stevenson-Wydler Act,[106] there is no guaranty that a Court will share this view.

Another legal hurdle to hackathons are intellectual property concerns. Even if the agency relies on the Stevenson-Wydler Act for authority, the Acct only provides two broad statements on how to handle IP issues.[107] If the government does not rely on this Act for authority and there is no IP agreement in place, it is unclear who would own the rights to the resulting product – the sponsor or the individual.[108] Government sponsored hackathons generally require that any submissions be "open source," and cite to the open

101. *See* Phipps, *supra* note 14.

102. *Compare* Stine, *supra* note 1, at 2, 16-17 ($2 million in prize money for the Lunar Lander Challenge), *with Hackathon for Combat Feeding Mobile Apps*, *supra* note 13 ($6,000 in prize money for a DoD hackathon).

103. *Compare* THE WHITE HOUSE OFFICE OF SCI. & TECH. POLICY, IMPLEMENTATION OF FEDERAL PRIZE AUTHORITY: FISCAL YEAR 2014 PROGRESS REPORT 242 (2015), https://www.whitehouse.gov/sites/default/files/microsites/ostp/NSTC/fy14_competes_prizes_-_may_2015.pdf (NASA International Space Apps Challenge had sixty-nine teams compete virtually in 2014), *with Canada-US Trading Hackathon*, *supra* note 89 (requirement that teams be present at venue).

104. *See* Bastian, *supra* note 14, at 5 ("One structural issue is that, unlike other challenges and prizes, hackathons have no specific statutory authorization.")

105. *See* Schooner & Castellano, *supra* note 9, at 398.

106. *See generally* THE WHITE HOUSE OFFICE OF SCI. & TECH. POLICY, IMPLEMENTATION OF FEDERAL PRIZE AUTHORITY: FISCAL YEAR 2013 PROGRESS REPORT 32-35, 106-08 (2014), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/competes_prizesreport_fy13_final.pdf [https://perma.cc/Y2B8-WNE9] (lists the following events involving hackathons as falling under authority of America Competes Act: Department of Energy Apps for Vehicles, National Science Foundation Mozilla Ignite).

107. *See* 15 U.S.C. § 3719(j) (2012) (government cannot gain an IP interest without participant's written consent, and government may negotiate for a license to use the IP).

108. *See* Bastian, *supra* note 14, at 6-7.

source definition by the Open Source Initiative,[109] but not all hackathon rules are clear on what open source means. Would the outcome be different if the individual is an employee of the sponsor? To avoid potential conflicts, it is important that the agency specify that the product is not solely owned by the participant.[110]

D. Open Data: A Modern Necessity to the Success of Prize Contests and Hackathons

In order to host a successful prize contest or hackathon, open data is key. President Obama's May 2013 executive order on open data policy defines open data as "publically available data structured in a way that enables the data to be fully discoverable and usable by end users."[111] The White House's open data policy requires that agencies publish their data online, with a presumption in favor of openness, and continue to improve the quality of data provided.[112] However, at the time this note was published, the Trump administration has not issued agency guidance regarding open data.[113] While a federal open data policy has numerous benefits, including operational efficiencies, cost reduction, improved services, and increased public access to information,[114] open data is particularly relevant to ODIs and hackathons because participants often rely on government data.[115] For example, the Department of Energy's Apps for Vehicles contest specifically called for the use of vehicle open data to develop apps that "improve vehicle safety, fuel efficiency, and comfort."[116]

---

109. *Compare International Space Apps Challenge*, *supra* note 13 (legal section states that "[y]ou agree that any original content . . . is freely available without restriction or is licensed as open source as defined by the Open Source Intitiative"), *and* Gen. Servs. Admin., *Government-wide Earth Day Hackathon*, Challenge.gov, https://www.challenge.gov/challenge/government-wide-earth-day-hackathon/ [https://perma.cc/3ZKV-82M8] (last visited Apr. 9, 2016) (requiring the final submission be open source code and explaining the requirements of the Open Source Initiative), *with Hackathon for Combat Feeding Mobile Apps*, *supra* note 13 (rules section stating that IP release should be "those typical of open source" with no additional explanation).

110. *See* Bastian, *supra* note 14, at 7.

111. *See* OFFICE OF MGMT. & BUDGET, MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES ON OPEN DATA POLICY-MANAGING INFORMATION AS AN ASSET 1, 5 (2013) [hereinafter Memorandum on Open Data Policy], https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf [https://perma.cc/E4RK-MCKU].

112. *Id.*; Bastian, *supra* note 14, at 4.

113. *See generally* White House, https://www.whitehouse.gov (last visited Sept. 30, 2017).

114. *See* Memorandum on Open Data Policy, *supra* note 111, at 1.

115. *See generally* Bastian, *supra* note 14, at 3-5 ("Consumable, web-ready data is the lifeblood of any hackathon.").

116. *See* Cristin Dorgelo & Ian Kalin, *DOE Vehicle Data Challenge Fuels Innovation*, White House: Blog (Apr. 11, 2013), https://obamawhitehouse.archives.gov/blog/2013/04/11/doe-vehicle-data-challenge-fuels-innovation [https://perma.cc/T4QF-QXBV].

Important criticisms of open data conern security and privacy issues.[117] While open data can be highly useful, data containing personally identifiable information (PII) must be protected by the government.[118] The Privacy Act restricts the government's access to and dissemination of personally identifiable data,[119] but this may not be enough to quell the concerns of privacy activists.[120] For example, the Consumer Finance Protection Bureau (CFPB) has a public database of consumer complaints, which contains narratives submitted by consumers.[121] To ensure that the narrative is scrubbed of PII before publication, it goes through one computer review and two human reviews.[122] While this process helps ensure the protection of PII, there is still the potential for typos, coding error, or programming error.

Another issue with moving to open data is the cost. President Obama's executive order concerning open data did not make any statements related to funding.[123] The OMB's open data policy memorandum requires the use of internal agency resources to execute these goals.[124] While it concedes that these goals may require additional resources, it instructs agencies to consider the downstream cost benefits that should result.[125] The resources needed are not only financial, but also include technical staff with knowledge to oversee such projects.[126]

---

117. *See* Bastian, *supra* note 14, at 6.

118. *See* Memorandum on Open Data Policy, *supra* note 110, at 10.

119. *See* Bastian, *supra* note 14, at 6 (citing *The Privacy Act of 1974*, U.S. Dep't Justice, https://www.justice.gov/opcl/privacy-act-1974 [https://perma.cc/YR3E-TY2U] (last visited June 29, 2013)).

120. *See* David Perera, *Privacy Act protections obsolete, say critics and lawmakers*, FierceMarkets (Aug. 1, 2012), http://www.fiercegovernmentit.com/story/privacy-act-protections-obsolete-say-critics-and-lawmakers/2012-08-01 [https://perma.cc/B44F-9ATX] (reporting on criticisms that the Privacy Act is outdated and "leaves data mining unregulated for privacy); *see also* Sandra Fulton, *Beware the Dangers of Congress' Latest Cybersecurity Bill*, Am. Civil Liberties Union: Blog (June 27, 2014), https://www.aclu.org/blog/national-security/beware-dangers-congress-latest-cybersecurity-bill?redirect=blog/national-security-technology-and-liberty/beware-dangers-congress-latest-cybersecurity-bill [https://perma.cc/B6P5-UPER] (criticizing the Cybersecurity Information Sharing Act of 2014).

121. *See generally* CONSUMER FIN. PROT. BUREAU, NARRATIVE SCRUBBING STANDARD, CFPB OFFICE OF CONSUMER RESPONSE (2015), http://files.consumerfinance.gov/a/assets/201503_cfpb_Narrative-Scrubbing-Standard.pdf [https://perma.cc/WC47-A3FC].

122. *Id.* at 3.

123. *See Executive Order on Open Data*, *supra* note 20.

124. *See* Memorandum on Open Data Policy, *supra* note 111, at 12.

125. *Id.*

126. *See id.*

III. FEDERAL INNOVATION POLICY: STAYING AFLOAT IN THE MODERN WORLD

Federal agencies have broad goals that are cast over a wide variety of stakeholders.[127] Throw in the complications of politics, and it is not difficult to understand why federal agencies are failing to develop the latest mobile application or the newest surgical device. Throughout President Obama's second term, however, he used the federal government as a renewed source to encourage innovation.[128] While President Donald Trump established a White House Office of American Innovation (OAI) in March 2017 to further encourage innovation, it is not clear how this policy will be executed under the current administration.[129]

A. President Obama Encourages Agencies to Use ODIs for Innovation

As part of President Obama's effort to increase an open and transparent government, the executive office encouraged the use of ODIs, such as prize contests, as a way for agencies to push innovation.[130] As of 1999, there was only one explicit prize contest sponsored by a US government agency: the Department of Commerce's Malcolm Baldrige National Quality Award.[131] But all of that started to change in 2009 when the White House put out a white paper on a strategy for innovation, stressing the need for investment in technological research and advancement.[132] The Department of Commerce's white paper specifically called for the use of prize contests to encourage innovation in the face of difficult problems.[133] Shortly thereafter in 2010, the OMB followed up to this white paper with a memorandum to government agencies on how to establish prize contests in support of innovation.[134]

---

127. *See* Steve Denning, *How to Make Government Innovative Again*, FORBES: BLOG (Mar. 6, 2012, 1:27 PM EST), https://www.forbes.com/sites/stevedenning/2012/03/06/could-government-invent-a-130mph-driverless-car/#455db2bb320f [https://perma.cc/8RXW-K32L].

128. *See generally* Guidance on the Use of Challenges and Prizes, *supra* note 7.

129. *See Presidential Memorandum on The White House Office of American Innovation*, White House (Mar. 27, 2017), https://www.whitehouse.gov/the-press-office/2017/03/27/presidential-memorandum-white-house-office-american-innovation [https://perma.cc/8RSH-97TR] (the memorandum establishes the OAI and briefly states its mission and responsibilities, but provides no other guidance as to how the policy will be carried out).

130. *See* John Kamensky, Inducement Prizes, Contests, and Challenge Awards, IBM CTR. BUS. GOV. (Jan. 5, 2011, 10:41 A.M.), http://www.businessofgovernment.org/blog/business-government/inducement-prizes-contests-and-challenge-awards.

131. *See* Concerning Federally Sponsored Inducement Prizes in Engineering and Science, *supra* note 7, at 3.

132. *See* EXEC. OFFICE OF THE PRESIDENT, A STRATEGY FOR AMERICAN INNOVATION: DRIVING TOWARDS SUSTAINABLE GROWTH AND QUALITY JOBS 3 (2009), https://files.eric.ed.gov/fulltext/ED511653.pdf [https://perma.cc/J3UL-8KNP].

133. *Id.* at 17-18.

134. *Id.* at 3-11 (providing broad guidance on, *inter alia*, how to fit the prize to the goal, choose partners, locate the necessary legal authority, and manage IP concerns).

By 2010, a host of government agencies were using prize or challenge contests to develop and promote innovation, ranging from the development of astronaut gloves in a NASA contest to the creation of student-made videos promoting the environment sponsored by the Environmental Protection Agency.[135] In January 2011, Congress amended the Stevenson-Wydler Act.[136] Since that time, over 740 competitions have been launched with more than $250 million awarded in prizes.[137]

The same day that President Obama issued an executive order concerning open data,[138] an OMB memorandum outlining this open data policy was released, which stated that one goal of the order was to "increase public access to valuable government information."[139] The OMB's memorandum provide specific examples of the public benefits of open data, including the use of Global Positioning System (GPS) data in improving navigation systems and location-based applications.[140] The order requires that agencies use data standards to make data available to the public in machine-readable and open formats.[141] In evaluating its use of ODIs and open data, agencies should keep in mind that these tools were encouraged at the behest of President Obama, and the Trump Administrations' views on the use of these tools are unclear.

B. *The FCC's Increased Use of ODIs and Open Data: Steps in the Right Direction*

The FCC has not been prolific in its use of ODIs. In the White House reports to Congress on use of federal prize authority for fiscal years 2011-

135. *See* Guidance on the Use of Challenges and Prizes, *supra* note 7, at 1.

136. *See* Gottlieb & Rawicz, *supra* note 6, at 1, n.7, ("America COMPETES Reorganization Act of 2010, Pub. L. No. 111-358, § 105, 124 Stat. 3982, 3989 (Jan. 5, 2011) (amending Stevenson-Wydler Innovation Act of 1980, 15 U.S.C.A. § 3701 *et seq*., by adding § 24, 'Prize competitions,' codified at 15 U.S.C.A. § 3719)").

137. *See About*, Challenge.gov, https://www.challenge.gov/about/ [https://perma.cc/HVS6-VBRL] (last visited Apr. 7, 2017).

138. *See Executive Order on Open Data*, *supra* note 20.

139. *See* Memorandum on Open Data Policy, *supra* note 111 ("Making information resources accessible, discoverable, and usable by the public can help fuel entrepreneurship, innovation, and scientific discovery – all of which improve Americans' lives and contribute significantly to job creation.").

140. *Id.*

141. *Id. at* 1-2.

2014, not a single FCC action is reported.[142] However, the FCC has used ODIs as a source for innovation since at least as early as 2011.[143]

1. The FCC's History and Structure is Not Conducive to Internal Innovation

The FCC was not created to develop telecommunication innovations, but rather to stabilize the telecommunications industry.[144] The FCC is guided by two statutes - the 1934 Communications Act and the Administrative Procedure Act (APA).[145] Congress enacted the Communications Act, which created the FCC and granted it authority "with respect to interstate and foreign commerce in wire and radio communication."[146] The FCC has a broad jurisdictional scope, but its procedures are more rigidly defined by statutes, such as the APA.[147] The APA sets forth policies that apply to various government agencies, including the FCC and that allow for meaningful participation prior to final decisions, known as "notice and comment" rulemaking.[148]

Since the 1996 Telecommunications Act, which sought to "promote competition[,] reduce regulation…and encourage the rapid deployment of new telecommunications technologies,"[149] the FCC has placed greater emphasis on innovation and prioritized it above other goals.[150] However, innovation is not the sole goal of the FCC.[151] Rather, the FCC, like most agencies, must concern itself with traditional government objectives, such as "public safety, universal access to communications, procedural fairness and consumer protection."[152] With the White House's push for innovation, and the FCC's competing goals, it is unclear as to how the FCC will successfully achieve its goal to increase innovation.

---

142. *See* IMPLEMENTATION OF FEDERAL PRIZE AUTHORITY: FISCAL YEAR 2014 PROGRESS REPORT, *supra* note 103, at 54-56, 197-201; IMPLEMENTATION OF FEDERAL PRIZE AUTHORITY: FISCAL YEAR 2013 PROGRESS REPORT, *supra* note 106, at 28-29, 109-10; THE WHITE HOUSE OFFICE OF SCI. & TECH. POLICY, IMPLEMENTATION OF FEDERAL PRIZE AUTHORITY: FISCAL YEAR 2012 PROGRESS REPORT 23-24, 80 (2013), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/competes_prizesreport_dec-2013.pdf [https://perma.cc/2CFU-A6G6]; THE WHITE HOUSE OFFICE OF SCI. & TECH. POLICY, IMPLEMENTATION OF FEDERAL PRIZE AUTHORITY: FISCAL YEAR 2011 PROGRESS REPORT 23 (2012), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/competes_report_on_prizes_final.pdf [https://perma.cc/FV2E-FK4X].

143. *See Open Internet Apps Challenge*, Devpost.com, https://openinternetapps.devpost.com/rules [https://perma.cc/3WXV-UEK5] (last visited Jan. 24, 2016).

144. *See* Bernthal, *supra* note 85, at 617.

145. *Id* at 635.

146. *See generally* Communications Act of 1934, 47 U.S.C. § 151 (1934).

147. *See* Bernthal, *supra* note 85, at 635-36.

148. *Id* at 636.

149. *See generally* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (Jan. 3, 1996).

150. *See* Bernthal, *supra* note 84, at 623.

151. *Id.*

152. *Id.*

The FCC has limited internal resources to devote to analyzing and developing new rules and policies, particularly in technical fields, such as engineering and economics.[153] The FCC Commissioners are not required to have any technical background, and are frequently appointed for political reasons, rather than for their technological expertise.[154] For example, the current FCC Chairman, Ajit Pai, is an attorney.[155] The experience of the two other FCC Commissioners is primarily rooted in either the legal or policy fields.[156] Furthermore, Chairman Pai's staff has predominantly legal or policy backgrounds, with the exception of one economist, Jay Schwarz.[157]

A leadership staff with predominatly legal and policy backgrounds is by no means unique to the FCC and is quite common for other federal agencies, such as the FTC.[158] While the FCC Commissioners may not be engineers, they have extensive experience in the telecommunications industry.[159] And it has been established that technical expertise is not a necessary component to run a highly successful and innovative organization.[160] While the FCC Commissioners may not have technical backgrounds, there are other staff at the FCC that could provide this expertise. For example, the FCC's Strategic Planning and Policy Office contains

153. *Id.* at 637.

154. *Id.* at 637-38.

155. *See generally Ajit Pai: FCC Chairman: Bio*, FCC, https://www.fcc.gov/about/leadership/ajit-pai [https://perma.cc/N9AB-SU7Y] (last visited Apr. 7, 2017).

156. *See generally Mignon Clyburn: Commissioner: Bio*, FCC, https://www.fcc.gov/about/leadership/mignon-clyburn?qt-leadership_tabs=0#qt-leadership_tabs [https://perma.cc/YFN4-TGMP] (last visited Apr. 7, 2017) (public service and media background); *Michael O'Rielly: Commissioner: Bio*, FCC, https://www.fcc.gov/about/leadership/mike-orielly?qt-leadership_tabs=0#qt-leadership_tabs [https://perma.cc/3UJX-ZL9J] (last visited Apr. 7, 2017) (policy background).

157. *See generally Ajit Pai: FCC Chairman: Staff*, FCC, https://www.fcc.gov/about/leadership/ajit-pai?qt-leadership_tabs=1#qt-leadership_tabs [https://perma.cc/W5HV-LH9H] (last visited Apr. 7, 2017) (Chief of Staff Matthew Berry, Senior Counsel Nicholas Degani, Acting Media Advisor Alison Nemeth, Acting Wireless Advisor Rachel Bender, and Acting Public Safety and Consumer Protection Advisor Zenji Nakazawa are all attorneys; Policy Advisor Nathan Leamer has a policy background; and Acting Wireline Advisor Jay Schwarz is an economist).

158. *Maureen K. Ohlhausen: Acting Chairman*, FTC, https://www.ftc.gov/about-ftc/biographies/maureen-k-ohlhausen [https://perma.cc/R7W5-G3DP] (last visited Apr. 7, 2017) (legal background); *Terrell McSweeney: Commissioner*, FTC, https://www.ftc.gov/about-ftc/biographies/terrell-mcsweeny [https://perma.cc/8BP4-AT36] (last visited Apr. 7, 2017) (legal background).

159. *See Ajit Pai: FCC Chairman: Bio*, *supra* note 155 (nearly two decades of experience in telecommunications).

160. *See.,* Dylan Love, *Steve Jobs Never Wrote Computer Code for Apple*, Bus. Insider (Aug. 29, 2013), http://www.businessinsider.com/steve-jobs-never-wrote-computer-code-for-apple-2013-8 [https://perma.cc/3S69-ZM8N] (stating that Steve Jobs, former CEO of Apple, was not an engineer and did not write code).

economists and technologists who report directly to the Chairman on issues related to innovation and competition.[161]

While the FCC's leadership's expertise is comparable to that of most US agencies, it is different when compared to telecommunications agencies in other countries.[162] A 2010 study on various telecommunications regulatory agencies revealed that comparable agencies in Canada, France, Sweden, and the United Kingdom had at least a mix of lawyers, economists and engineers among senior managers.[163] At the FCC, however, there was only one engineer and no economists at the time of that study.[164] How is the leadership at the FCC supposed to drive innovation without any significant experience in technology themselves? One resource, according to the Obama administration, is ODIs.[165]

2. The FCC's Use of ODIs: A Steady and Cautious Start

The FCC began its response to President Obama's push for innovation with open data – a key component for the success of ODIs. In June 2010, the FCC launched the Data Innovation Initiative.[166] As part of this initiative, the FCC created the position of Chief Data Officer (CDO) to run a new team charged with handling data throughout the FCC.[167] As part of this process, the FCC has released public notices to seek input on what type of data should be created, what can be eliminated, and which datasets need improvement.[168] Currently, the FCC's data website has available for download over 40 specialized FCC databases, such as radio call signs and equipment authorization, over 150 datasets, and a searchable baseline inventory of spectrum and holders of commercial spectrum usage rights.[169] Additionally, the FCC has over ten APIs available for public use.[170]

---

161. *See Chief and Deputy Economists of the FCC*, FCC, https://www.fcc.gov/general/chief-and-deputy-chief-economists-fcc#block-menu-block-4 [https://perma.cc/T8VU-DE5E] (last visited Apr. 9, 2016); *Chief and Deputy Technologists of the FCC*, FCC, https://www.fcc.gov/general/chief-and-deputy-chief-technologists-fcc#block-menu-block-4 [https://perma.cc/UN98-RA2X] (last visited Apr. 9, 2016).

162. *See* Bernthal, *supra* note 84, at 638.

163. *See* J. SCOTT MARCUS & JUAN RENDON SCHNEIR, DRIVERS AND EFFECTS OF THE SIZE AND COMPOSITION OF TELECOMS REGULATORY AGENCIES 16 (2010), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1675705 [https://perma.cc/JV3P-BJPJ].

164. *Id.*

165. *See* A STRATEGY FOR AMERICAN INNOVATION: DRIVING TOWARDS SUSTAINABLE GROWTH AND QUALITY JOBS, *supra* note 132, at 17-19.

166. *See generally Data Innovation Initiative*, FCC, https://www.fcc.gov/general/data-innovation-initiative [https://perma.cc/85H7-2LNF] (last visited Jan. 22, 2016).

167. *Id.*

168. *Id.*

169. *See generally Data*, FCC, https://www.fcc.gov/reports-research/data [https://perma.cc/ZN8C-6LY5] (last visited Jan. 22, 2016).

170. *See Developers*, FCC, https://www.fcc.gov/reports-research/developers [https://perma.cc/9GHJ-2GLH] (last visited Jan. 22, 2016).

The FCC's first prize contest since the White House's push for innovation projects was the Open Internet Apps Challenge hosted in 2011.[171] This contest was developed by the FCC's first CDO, Greg Elin, as part of the FCC's new mission to increase development of APIs and engage developers.[172] The Open Internet Apps Challenge was a four-month event with a maximum $1,500 prize.[173] Since then, the FCC has hosted additional contests, both on its own and in partnership with other organizations as seen in Table 1, which shows a summary of recent FCC challenges.

Table 1

Name of Challenge	**Prizes**	**Sponsor(s)**	**Duration**	**Grand Prize Winner(s)**
Open Internet Apps[174]	$1,500	FCC	Feb. 1 – Jun.1, 2011	MobiPerf (University of Michigan & Microsoft Research); Detecting ISP Traffic and Discriminatio n and Traffic Shaping (Georgia Institute of Technology); Netalyzr: Illuminating The Edge Network (The ICSI Netalyzr Project)
Apps for Communities [175]	$100,000	FCC, James L. Knight Foundation	Apr. 14 – Oct. 3, 2011	Yak.us (Ryan Resella)
Chairman's Awards in Advancement in	Recognitio n	FCC	Annual awards since 2010	2015 winners include Blind Square, no CAPTCHA reCAPTCHA

171. *See generally* Colby Hochmuth, *FCC's data guru Greg Elin eyes new opportunity*, fedscoop, https://www.fedscoop.com/fcc-chief-data-officer-greg-elin-departure/ [https://perma.cc/C8YP-94GZ] (last visited Nov. 6, 2015).

172. *Id.*

173. *See generally Open Internet Apps Challenge*, *supra* note 140.

174. *Id.*

175. *Apps for Communities Challenge*, Devpost.com, http://appsforcommunities.devpost.com/ (last visited Nov. 6, 2015) (co-sponsored by the FCC and the James L. Knight Foundation).

Accessibility (AAAs)[176]			announced in June	(Google), Convo Lights, Beam Messenger, Video Meetings with BlueJeans (AT&T), Talking Guide (Comcast), OpenAIR (Knowbility)
Developing with Accessibility [177]	None[178]	FCC	Sept. 6-7, 2012	N/A
PDF Liberation[179]	Unknown	FCC, Sunlight Foundation [180]	Jan. 17-19, 2014	What Word Here

The first four challenges detailed in Table 1 deal with spurring innovation to benefit the public, rather than benefiting the FCC itself. The Open Internet Apps Challenge called for the creation of an app that measures a user's broadband provider's compliance with open internet.[181] The Apps for Communities challenge called for the creation of an app that makes "local public information more personalized, usable, and accessible for all Americans," particularly for those people "that are least likely to be online." [182] Additionally, the Chairman's Awards for Advancements in Accessibility is an annual event that calls for the creation of tools and the development of ideas to make technology accessible for individuals with disabilities.[183] Each year the FCC announces anywhere from four to seven specific challenges within this category, such as developing an alternative to

176. *Chairman's Awards for Advancements in Accessibility*, FCC, https://perma.cc/Z7JT-5SK (last visited Nov. 6, 2015).

177. *Developing with Accessibility*, *supra* note 47.

178. *Id.* (describing the goal as "increased collobration" rather than focusing on a specific result).

179. *PDF Liberation*, https://pdfliberation.wordpress.com/2014/01/21/hackathon/ [https://perma.cc/3FMC-BXCW] (last visited Jan. 22, 2016).

180. *Id.* (These were the main sponsors of the Washington, DC event. Additional sponsors for similar events in other cities included Knight-Mozilla OpenNews, Rally.org, Public Sector Credit Solutions, OpenGov, Smart Chicago, Pediacities – A Product of Ontodia, Inc., Artifex Software, Inc., Quandl, and Civic Ninjas).

181. *Open Internet Apps Challenge*, *supra* note 140.

182. *See Apps for Communities Challenge*, *supra* note 175.

183. *See Chairman's Awards for Advancements in Accessibility*, *supra* note 176.

the Completely Automated Public Turing Test to Tell Computer and Humans Apart (CAPTCHA), which "present[s] accessibility barriers to persons with visual or cognitive disabilities."[184] Similarly, the goal of Developing with Accessibility was to allow API developers to collaborate and share on ways to make APIs accessible to people with disabilities.[185]

On the other hand, the FCC's most recent challenge, PDF Liberation, could potentially benefit both the FCC itself, as well as public users of the FCC's data.[186] The goal was to develop an application that can easily convert the FCC's press releases, which are in PDF format, to a text format so that the releases can be easily searched and analyzed.[187] The event not only had multiple private sponsors, in addition to the FCC, but there were also various challenges that dealt with converting PDF files to a text format, ranging from IRS Non-Profit Reports to New York City Council and Community Board Documents.[188] The PDF Liberation challenge is an excellent example of the technical benefits that the FCC can reap from hackathons, particularly in the use of data development and standardization, and how that technology can be shared with other organizations.

IV. THE FCC'S ADOPTION OF ODIS: IMPLICATIONS FOR TECHNOLOGICAL INNOVATION

The resources used by the FCC to spur innovation can affect which sector sees innovation, such as private versus public, and how quickly that innovation occurs. In order to maximize public benefits and the growth of the US telecommunications sector, the FCC should increase the number of prize contests it sponsors with a focus on private-sector innovation, and limit its use of hackathons to short-term, internal goals. In order for these prize contests and hackathons to succeed, it is imperative that the FCC issue clear rules and guidance and continue its communication with private developers regarding open data.

A. The FCC Should Increase Its Use of Prize Contests for Private Innovations

To achieve its innovation policy goals, the FCC should increase the number of prize contests it sponsors. These prize contests should focus on innovation outside of the FCC, for the benefit of the public. While prize

184. *See FCC Extends Deadline for Nominations for the Fourth Chairman's AAA and Invites the Submission of Additional Information*, FCC (Feb. 24, 2015)., https://apps.fcc.gov/edocs_public/attachmatch/DA-15-252A1_Rcd.pdf.

185. *See Developing with Accessibility*, *supra* note 47.

186. *See generally* Kathy Kiely, *PDF Liberation: Why It Matters And How You Can Help*, Sunlight Found.: Blog, https://sunlightfoundation.com/2014/01/24/pdf-liberation-why-it-matters-and-how-you-can-help/ [https://perma.cc/K9HH-B87R] (Jan. 24, 2014).

187. *See generally PDF Liberation Hackathon – Federal Communications Commission Challenge*, GitHub (Jan. 17, 2016), https://github.com/pdfliberation/pdf-hackathon/blob/master/challenges/fcc-daily-releases.md [https://perma.cc/48BV-RUKE].

188. *See PDF Liberation*, *supra* note 179.

contests will not directly benefit the FCC, they will serve the FCC's mission by promoting innovation within the telecommunications industry.[189] For example, an app that can detect and block robocalls may not have much use *within* a government agency, but the public would certainly be interested in such a technology.[190]

Encouraging the development of desirable technology will help keep the US at the top of the international telecommunications industry.[191] One of the largest benefits of prize contests is increased private investment spending, typically above and beyond the value of the actual prize.[192] By rewarding and publicizing these private innovators, the US will ensure that private innovation in the telecommunications sector continues to thrive.

The FCC could sponsor prize contests both with broad and specific goals. An example of a prize contest with a broad goal would be one that awards a monetary prize for the most innovative telecommunications app. A contest with a specific goal, however, would award a monetary prize for developing a specific technology, such as an app that standardizes the various text message formats used by different cell phone developers and wireless service providers. While a specific prize contest has the benefit of developing technology with pre-determined usefulness, a broad prize contest could result in the development of technology that the FCC never considered. A balance could be found by hosting a broad prize contest every few years, with specific prize contests hosted when the FCC sees a real need for a specific technology that does not exist yet.

Agencies are authorized to work with third parties in funding and administering prize contests.[193] If its funds are limited, the FCC should work with third parties, such as private telecommunications companies, non-profits, and think tanks, to develop and administer prize contests. After all, these are the parties with the most technical expertise, and the FCC, and the public, could greatly benefit from stakeholder collaboration.

B. The FCC Should Increase Its Use of Hackathons for Internal Innovation

Given the limited benefit that hackathons can provide to government agencies, the FCC should limit using hackathons to issues *within* the FCC. One data problem that the FCC, and other agencies, face is that it has various data collections in all different formats, which can make comparisons

189. *See* Guidance on the Use of Challenges and Prizes, *supra* note 7, at 1.

190. *See generally FTC Robocall Challenge*, *supra* note 63.

191. Bernthal, *supra* note 84, at 625-26.

192. *See* Stine, *supra* note 1, at 16-17 ("For the Lunar Lander Challenge, twelve private teams spent nearly 70,000 hours and the equivalent of $12 million trying to win $2 million in prize money.").

193. *See id.* at 1 ("Encouraging the formation of a public-private partnership to fund and administer a prize.").

difficult.[194] Starting in 2000, the FCC requires the submission of "uniform and reliable data" from certain telecommunications companies,[195] but this does not account for data submitted from other parties, such as lobbyists and stakeholders, during notice and comment periods.

Hackathons are an excellent tool to help the FCC standardize its data since it allows for focused thought on one particular issue, such as PDF readability, at a low cost to the FCC.[196] In order to benefit from hackathons, the FCC needs to be vigilant in continuing to work on a solution within the agency after the hackathon, since hackathons typically result in a temporary, but not a definitive solution.[197]

One successful structure may be for the FCC to sponsor a hackathon, but to allow a private party more familiar with the particular technological hurdle to handle organizing the event, as was done in the PDF Liberation Challenge.[198] For example, the FCC could work with a third party that specializes in data analytics to develop a tool that standardizes international telecommunications data to the same standards as the FCC's internal data. Another option could be for the FCC to work in partnership with other agencies, as in the government-wide Earth Day hackathon.[199]

C. The FCC Must Provide Clear Rules and Procedures for ODIs

With the use of either prize contests or hackathons, the FCC needs to ensure that proper and detailed rules are in place, including an appeals structure to challenge the results. As evident in *Frankel v. United States*, there is currently no clear legal structure by which to challenge the results of these events since the CFC and the GOA both ruled that these contests are not procurements.[200] The FCC needs not only to create an appeals structure, but also to guarantee an unbiased judge as part of the appeals process. If the process appears to be nothing more than the agency covering its liability and protecting its decision, participants may be discouraged from investing so much time and energy into what they perceive to be a flawed and biased process.[201]

---

194. *See FCC Reform Agenda*, FCC (Feb. 2010), https://apps.fcc.gov/edocs_public/attachmatch/DOC-296363A1.pdf [https://perma.cc/77EZ-KG54] (data goals include standardizing and automating future data collections, linking and standardizing current databases to form a single system). *But see Measuring Broadband America*, FCC, https://www.fcc.gov/general/measuring-broadband-america [https://perma.cc/XB6X-3J2K] (last visited Apr. 9, 2016) (FCC efforts to collect and standardize fixed and mobile broadband data).

195. *Report and Order Modernizing the FCC Form 477 Data Program*, WC Docket No. 11-10, 1, 3 (2013).

196. *See PDF Liberation Hackathon – Federal Communications Commission Challenge*, *supra* note 187.

197. Bastian, *supra* note 14, at 9.

198. *See PDF Liberation Hackathon*, *supra* note 179.

199. *See, e.g.*, *Earth Day Hackathon*, *supra* note 13.

200. *See Frankel*, *supra* note 63, at 332, 334.

201. *See* Schooner & Castellano, *supra* note 9, at 398.

In drafting rules and a structure for these events, it is critical that the FCC provide guidance on intellectual property rights.[202] What happens if a submission does not win, but the FCC uses the submission for another purpose? Does that participant have any right to ownership or compensation? If a participant does win, does she retain the right to sell or license the technology to other parties? Any ODI should have an IP section in its rules, with a detailed description of all terminology.[203] Some government ODIs, particularly hackathons, have relied on the Open Source Initiative requirements, which ensure protection of the government's interest while also encouraging collobration and openness.[204] These requirements are an excellent starting point, particularly for technology ODIs.

D. The FCC Should Continue Its Open Dialogue with Developers and Its Push for Open Data

A key component to ensuring the success of hackathons and prize contests is open data.[205] The FCC needs to ensure that there is sufficient open data in place for private parties to innovate – whether it be for a prize contest, hackathon, or independent interest. One way to ensure that open data is sufficient is to have an accessible, ongoing dialogue with participants.[206] Technology and data standards are constantly changing, which can require both developing new technology and putting to rest obsolete formats. Through the "Developer" section on its website, the FCC has already begun such a dialogue.[207] Given the importance of open data to the success of ODIs and hackathons, it is critical for the FCC to continue to monitor the data provided and to work regularly with the developer community in order to provide new data, update current data to new formats, and tp remove obsolete data.

V. CONCLUSION

The US is, and continues to be, a leader in the telecommunications field. While much of this innovation has developed in the private sector, the FCC plays a critical role in ensuring that there are sound policies in place to encourage continued innovation. While the FCC should continue hire more staff with technological expertise, particularly in the area of data, the FCC

202. *See* Bastian, *supra* note 14, at 6-7.

203. *See, e.g.*, *Earth Day Hackathon*, *supra* note 13.

204. *See generally The Open Source Definition*, Open Source Initiative, https://opensource.org/osd-annotated [https://perma.cc/UV7B-RYM2] (last visited Apr. 9, 2016) (requirements related to free redistribution, source code, derived works, integrity of the author's source code, no discrimination of persons or groups, no discrimination against fields of endeavor, distribution of license, license must not be specific to a product, license must not restrict other software, and license must be technology-neutral).

205. *See* Bastian, *supra* note 14, at 9.

206. *Id.* at 5 (an important consideton is "what types of information would be most useful and interesting to the public").

207. *See Developers*, FCC, https://www.fcc.gov/reports-research/developers [https://perma.cc/9GSK-6KFW] (last visited Jul. 27, 2017)

should also increase its use of hackathons and prize contests as a source of innovation. Open data is a key tool in that policy. It is increasingly important for the FCC to continue its open dialogue with the private telecommunications sector. While the FCC should continue that dialogue through its traditional tools, such as the notice and comment period, it should also expand that dialogue to discuss tools with whice developers, engineers, and economists – namely prize contests, hackathons and open data are more familiar. To aid in this process, the FCC should create an advisory committee composed of members with diverse backgrounds to advise the Commission on how best to use these tools.

Communications Law: Annual Review

Staff of the Federal Communications Law Journal

TABLE OF CONTENTS

Ameren Corp. v. FCC

No. 16-1683, 2017 WL 3224187 (8th Cir. July 31, 2017)

Ryan Farrell *

In *Ameren Corp. v. FCC*,[1] the United States Court of Appeals for the Eighth Circuit. denied a petition for review by utility companies of a November 2015 FCC order that governed the rates utility companies may charge telecommunications providers for attaching their networks to utility-owned poles.[2] The FCC's order equitized the rates utility companies could charge telecommunications and cable providers.[3] The Eighth Circuit panel held that the 2015 order was a permissible construction of the Pole Attachments Act.[4]

The debate over rates for pole attachments has gone on for several decades. Congress first addressed this issue by enacting the Pole Attachments Act .[5] This legislation gave the FCC the authority to determine whether pole attachment rates by providers of cable and telecommunications providers are "just and reasonable."[6] The statute also set forth a lower and an upper bound for "just and reasonable" rates.[7] The lower bound rate "assures a utility the recovery of not less than the additional cost of providing pole attachments."[8] The upper bound rate was "determined by multiplying the percentage of the total usable space…which is occupied by the pole attachment by the sum of the operating expenses and actual capital costs of the utility attributable to the entire pole."[9] The FCC set the upper bound rate, known as the Cable Rate, by multiplying the space factor (the space occupied by an attachment divided by the total useable space on the pole), the net cost of a bare pole, and a carrying charge rate.[10]

Initially, Section 224 applied to only cable providers.[11] However, Congress amended Section 224 as part of the Communications Act rewrite in 1996, expanding the FCC's authority to cover pole attachments by telecommunication providers.[12] Until 2011, the FCC determined the "cost"

---

* J.D. candidate, The George Washington University, May 2018. Managing Editor, *Federal Communications Law Journal*, 2017–18.

1. Ameren Corp. v. FCC, No. 16-1683, 2017 WL 3224187 (8th Cir. July 31, 2017).
2. *Id.* at *1
3. *See Id.* at *2
4. *Id.* at *4
5. *See* 47 U.S.C. 224 (2012).
6. *See Ameren Corp.* at *2. (citing 47 U.S.C. 224(b)(1)
7. *Id.*
8. *Id.*
9. *Id.* (citing 47 U.S.C. 224(d)(1)
10. *Id.*
11. *Id.*
12. *Id.*

for the Telecom Rate the same as for the Cable Rate. The FCC also calculated the space factor differently by apportioning two-thirds of the costs of the unusable space. This resulted in the Telecom Rate often being higher than the Cable Rate. Industry stakeholders began to voice concern that the risk of having to pay the Telecom Rate possibly deterred cable providers from expanding their services.[13]

The FCC attempted to implement equalization between the two rates in an April 2011 order.[14] The order reinterpreted the word "cost" in the underlying statute and defined it as 66 percent of the pole's fully allocated cost for an urban area, and 44 percent of a non-urban area. Under this order, the Telecom Rate approximated the Cable Rate.

Electric utility companies challenged this rule in court, alleging it was inconsistent with Section 224.[15] Specifically, the utilities' argued that "cost" in Sec. 224(e) must mean the fully allocated costs of a pole, and not 66 or 44 percent of the pole's fully allocated costs as set forth in the April 2011 order.[16] The D.C. Circuit upheld the April 2011 rule and rejected the utilities' petition for review.[17] The D.C. Circuit, applying *Chevron* analysis, held that the term "cost" in Sec. 224(e) is ambiguous, and the FCC's interpretation of the statute was reasonable in attempting to pursue equalization between the Cable Rate and the Telecom Rate.[18]

Despite the April 2011 order, the FCC found in 2015 that the order had failed to equalize the Telecom and Cable rates.[19] In another effort to achieve equalization, the FCC adopted another order in November 2015.[20] The November 2015 order was a response to utilities rebutting the presumptions of 5 attachers in an urban area, and 3 attachers in a non-urban area, increasing the Telecom rate.[21] The November 2015 order eliminated the distinction between urban and non-urban areas, and adopted one universal definition of "cost" – basing it on the average number of attachers to a pole within an area. The utilities brought a legal challenge to the November 2015 order, seeking a petition for review by the Eighth Circuit.

Like the D.C. Circuit when reviewing the FCC's April 2011 analysis, the Eighth Circuit court applied Chevron analysis to the November 2015 order. [22] Also like the D.C. Circuit in 2011, the Eighth Circuit found the word "cost" in Section 224 as ambiguous, and found that the FCC's order was a

13. *Id.* at *2

14. Implementation of Section 224 of the Communications Act, A National Broadband Plan for Our Future, *Report and Order and Order on Reconsideration*, 26 FCC Rcd. 5240 (2011) [hereinafter *2011 Broadband Order*]

15. *See* *2 (citing Am. Elec. Power Serv. Corp. v. FCC, 708 F.3d 183 (D.C. Cir.), *cert. denied* 134 S.Ct. 118, 187 (2013)).

16. *Id.*

17. *Id.* *2

18. *Am. Elec. Power*, 708 F.3d at 186, 189–90.

19. In the Matter of Implementation of Section 224 of the Act, *Order on Reconsideration*, 30 FCC Rcd. 13731 (2015) (hereinafter *November 2015 Order*]

20. *Id.*

21. *Id.* at 13738, ¶ 18

22. *See Ameren Corp,* at *2–3

reasonable interpretation of the ambiguity.[23] The court contrasted the definition of "cost" in 224(d) and 224(e).[24] In 224(d), Congress used "cost" to set forth the lower and upper bounds. By contrast, Congress did not specify what type of cost should be used to calculate the Telecom rate.[25]

The Utilities had argued that Congress had intended to establish two different rates in Sec. 224(d)(1) and 224(e), and that the November 2015 order went against Congress' intention.[26] The court rejected this argument, and noted that because "cost" in Sec. 224 is ambiguous, the same "cost" definition need not be used to determine the upper bound cable rates, and the Telecom rate.[27]

The Court ultimately found that the interpretation was reasonable and deferred to the FCC's approach.[28] This represents the second time a legal challenge to the FCC's order by utility companies opposing the equalization of the Cable and Telecom rates was defeated by Federal Courts.

23. *Id.*
24. *See Id.*
25. *Id.*
26. *Id.*
27. *Id.*
28. *Id*. at 1014.

Bais Yaakov of Spring Valley v. FCC

852 F.3d 1078 (D.C. Cir. 2017)

Kristin Capes *

In *Bais Yaakov of Spring Valley v. FCC*,[1] the United States Court of Appeals for the District of Columbia Circuit vacated an FCC Order which interpreted the FCC's 2006 Solicited Fax Rule to be lawful.[2] The Court held that a provision of the 2006 Solicited Fax Rule, which required businesses to include an opt-out notice in their solicited fax advertisements, was unlawful.[3]

BACKGROUND

When the Junk Fax Prevention Act was enacted in 2005, it placed strict limitations on who companies could send unsolicited fax advertisements to, and required that all unsolicited fax advertisements include an opt-out notice.[4] Under the Junk Fax Prevention Act, the FCC was given the authority to make regulations to implement the act.[5] In 2006, the FCC issued the Solicited Fax Rule, which included a provision requiring businesses who send out solicited fax advertisements to include opt-out notices.[6]

In 2010, Petitioner Anda requested a declaratory judgment from the FCC establishing that they were not required to include opt-out notices in their fax advertisements to entities who had given them permission to send the facsimiles.[7] Petitioner Anda requested the declaratory judgment in response to earlier litigation they had been defendants in.[8] The earlier litigation was a class action suit, in which the plaintiffs sought $150 million in damages from Petitioner Anda because their fax advertisements did not meet the requirements of the FCC's Solicited Fax Rule.[9] Many of plaintiffs who sought damages for the lack of opt-out notices on Petitioner Anda's fax advertisements were businesses who had given Petitioner Anda express permission to send fax advertisements.[10]

---

* J.D. candidate, The George Washington University Law School, May 2017. Production Editor, *Federal Communications Law Journal*, 2017–18.

1. Bais Yaakov of Spring Valley v. FCC, 852 F.3d 1078 (D.C. Cir. 2017).
2. *See Id.*
3. *Id.* at 1083.
4. *Id*. at 1080.
5. *Id.*
6. *Id.* at 1079.
7. *Id.* at 1081.
8. *Id.*
9. *Id.*
10. *Id.*

In response to Petitioner Anda's declaratory judgment request, the FCC stated that it did have the authority under the Junk Fax Prevention Act to require companies to include opt-out notices in their solicited fax advertisements, but that they would give a waiver out for any faxes sent without notices prior to April 30, 2015.[11] In response to the FCC's ruling, Petitioner Anda and the other companies who had joined onto the declaratory judgment request sought a review of the decision from the United States Court of Appeals for the District of Columbia Circuit.[12]

ANALYSIS

The United States Court of Appeals for the District of Columbia Circuit held that the Junk Fax Prevention Act did not give the FCC authority to require businesses to include opt-out notices in their solicited fax advertisements.[13] The Court held the act included a distinct line between unsolicited fax advertisements and solicited fax advertisements.[14] While the FCC argued that the language within the act does not prohibit such a rule and therefore they were within their authority to make such a regulation, the Court disagreed. The Court stated that "the FCC may only take action that Congress has *authorized*." Accordingly, the FCC could not reach beyond the plain language of the Act as they had when they created the Solicited Fax Rule.[15]

CONCLUSION

The United States Court of Appeals for the District Court Circuit found the provision in the FCC's Solicited Fax Rule that required solicited fax advertisements to include an opt-out notice unlawful, and vacated the FCC's Order.[16]

11. *Id.*
12. *Id.*
13. *Id.* at 1082.
14. *Id.*
15. *Id.*
16. *Id*. at 1083.

Chelmowski v. FCC

No. 15-1425, 2016 U.S. App. LEXIS 7000 (D.C. Cir. Apr. 18, 2016) (per curiam)

Ryan Farrell *

In Chelmowski v. FCC,[1] the Court of Appeals for the District of Columbia dismissed a motion for production of documents, as well as a separate motion for a *Vaughn* index containing certain FCC documents. The order signifies the finality of certain agency decisions made by the FCC.[2]

The petitioner, James Chelmowski, had been engaged with the FCC.[3] Chelmowski filed a formal complaint against AT&T Mobility LLC, which was dismissed by the FCC on July 10, 2015.[4] In October 2015, the FCC's Enforcement Bureau issued an Order on Reconsideration denying the petition for reconsideration of the July 2015 dismissal.[5] One month later, Chelmowski filed a petition review of the staff-level Order on Reconsideration in the D.C. Circuit Court of Appeals.[6]

On September 11, 2015, Chelmowski filed two FOIA requests with the FCC, seeking documents related to informal complaints he made to the FCC.[7] The FCC responded on September 17, claiming the documents had been withheld without explanation.[8] Chelmowski appealed the FCC's FOIA decision to withhold to the Office of General Counsel.[9] The FCC supplied additional documents to Chelmowski.[10] Chelmowski subsequently filed motions in the appeal to the D.C. Circuit seeking release of records the FCC withheld from disclosure under VOIA, as well as a *Vaughn index of the documents and portions* withheld by the FCC.[11] The FCC subsequently

* J.D. candidate, The George Washington University, May 2018. Managing Editor, *Federal Communications Law Journal*, 2017–18.

1. Chelmowski v. FCC, No. 15-1425, 2016 U.S. App. LEXIS 7000 (D.C. Cir. Apr. 18, 2016) (per curiam)
2. *Id.*
3. *See* Brief for Respondent, Opposition to Motion for Request for Documents & Motion For a Vaughn Index, at *2, Chelmowski v. FCC, No. 15-1425, 2016 U.S. App. LEXIS 7000 (D.C. Cir. Apr. 18, 2016) [hereinafter *FCC Motion*] Chelmowski subsequently filed requests for records containing internal FCC information in the Northern District of Illinois. *See also Chelmowski v. FCC*, No. 16-5587, 2017 WL 736893 (N.D. Ill. Feb. 24, 2017) (Coleman, J.)
4. *Id.*
5. James Chelmowski v. AT&T Mobility, *Order on Reconsideration*, DA 15-1175 (EB Oct. 16, 2015)
6. *FCC's motion*, *supra* note 3, at *2
7. *Id.*
8. *Id.* at *2-3.
9. *Id.* at *3.
10. *Id.*
11. *Id.* at *4

moved to dismiss the claims, claiming that Chelmowski did not properly seek judicial review, and that the D.C. Circuit lacked jurisdiction to address his claims.[12]

The two questions for the Court were as follows. First, are orders from the Chief of the FCC's Enforcement Bureau final reviewable orders? Second, does the D.C. Circuit have jurisdiction to address the claims? The D.C. Circuit court answered no to both questions dismissed both motions.

In addressing the first question, the FCC noted that "The filing of an application for review under this subsection shall be a condition precedent to judicial review of any order, decision, report, or action taken to a delegation under paragraph (1) of this subsection."[13] In addressing the second question, the FCC found Chelmowski did not follow proper judicial review in this case, noting that original jurisdiction to review an agency's final disposition regarding a FOIA request lies in the District Court, and not in the D.C. Circuit.[14] As such, the FCC's motion to dismiss on both counts was granted.

12. *Id.* at *4–5
13. Richman Brothers Records, Inc. v. FCC, 124 F.3d 1302, 1303 (D.C. Cir. 1997).
14. *FCC Motion* at *1

FTC v. AT&T Mobility LLC

835 F.3d 993 (9th Cir. 2016)

Rosie Brinckerhoff *

In *FTC v. AT&T Mobility*, the United States Court of Appeals for the Ninth Circuit dismissed an action brought by the Federal Trade Commission (FTC) against AT&T under Section 5 of the FTC Act, for failing to disclose to its customers its practice of throttling data speeds for consumers with unlimited mobile data plans. In interpreting the Section 5 common carrier exemption to be status-based, the Court held that AT&T is immune from Section 5 liability due to its status as a common carrier. Convoluting the jurisdictional boundaries between the FTC and the Federal Communications Commission (FCC), the Court's analysis in *FTC v. AT&T Mobility LLC* exposes the possibility that even engaging in a negligible amount of common carrier service may be enough to qualify all of an entity's activities for the common carrier exemption.

BACKGROUND

Pursuant to Section 5 of the FTC Act, the FTC is authorized to "prevent persons, partnerships, or corporations, *except . . . common carriers subject to the Acts to regulate commerce* . . . from using . . . unfair or deceptive acts or practices in or affecting commerce."[1] Section 5(a)(2) contains a list of industries that enjoy a jurisdictional carve-out from FTC authority. This list includes banks, airlines, federal credit unions, and of particular relevance in the instant case, common carriers.[2]

The FTC Act contains no explicit definition of "common carrier."[3] However, "common carrier" is defined in the Communications Act of 1934 as "any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or interstate or foreign radio transmission of energy."[4] Pursuant to the Communications Act of 1934, the FCC enjoys regulation and enforcement capabilities of common carriers.[5]

Giving rise to a jurisdictional overlap between the FTC and the FCC, "[a]cts to regulate commerce" is defined in the FTC Act as including the

* J.D. candidate, The George Washington University, May 2018. Executive Editor, *Federal Communications Law Journal*, 2017–18.

1. 15 U.S.C. § 45(a)(2) (emphasis added).
2. *Id*.
3. 15 U.S.C. § 44.
4. 47 U.S.C. § 153(11).
5. 47 U.S.C. § 151.

Interstate Commerce Act of 1887,[6] the Communications Act of 1934, and "all Acts amendatory thereof and supplementary thereto."[7]

In the instant case, the FTC filed suit against AT&T in 2014 under its Section 5 enforcement authority asserting that, despite AT&T's unequivocal marketing promises of unlimited data, the company began throttling data speeds for its customers with unlimited mobile data plans.[8] At the core of the FTC's claim was that AT&T was promising unlimited mobile data to its customers that it failed in fact to provide. The FTC's initial complaint did not challenge the overall fairness of AT&T's data throttling practices per se; rather, the FTC's primary grievance was that AT&T acted deceptively in failing to adequately disclose to its customers the extent of its data throttling program.[9]

The central dispute in the initial 2014 litigation between the FTC and AT&T was the scope of the common carrier exemption. AT&T argued that the exemption was status-based, meaning that entities enjoying the common carrier status cannot be regulated by the FTC under Section 5, even when "providing services other than common carri[er] services."[10] The FTC argued that the common carrier exemption was activity-based, meaning "the common carrier ex[emption] applies only if an entity has the status of a common carrier and is actually engaging in common carrier specific-services."[11]AT&T subsequently filed a motion to dismiss in the United States District Court for the Northern District of California arguing that the company is immune from Section 5 liability due to its exemption under the statute as a "common carrier[] subject to the Acts to regulate commerce."[12]

Injecting a new layer of complexity to the case, while AT&T's motion to dismiss was pending before the District Court, the FCC issued an order reclassifying mobile data service from its existing status as a non-common carrier service to a common-carrier service.[13] Although the order explicitly stated that reclassification would not apply retroactively,[14] AT&T argued to the District Court that the Reclassification Order would in effect strip the FTC's Section 5 enforcement authority for any past or future conduct by AT&T.[15]

The District Court denied AT&T's motion to dismiss, agreeing with the FTC's interpretation of Section 5 as constituting an activity-based exemption for common carriers, rather than a status-based exemption.[16] AT&T

6. 49 U.S.C. Subtitle IV.
7. 15 U.S.C. § 44.
8. FTC v. AT&T Mobility LLC*,* 835 F.3d 993, 995 (9th Cir. 2016).
9. *Id*. at 996.
10. FTC v. AT&T Mobility LLC*,* 87 F. Supp. 3d 1087, 1091 (N.D. Cal. 2015).
11. *Id*.
12. 15 U.S.C. § 45(a)(2).
13. FTC v. AT&T Mobility LLC*,* 835 F.3d 993, 996 (9th Cir. 2016).
14. *Id*.
15. *Id*.
16. *Id*.

subsequently appealed the District Court's decision to the United State Court of Appeals for the Ninth Circuit.[17]

ANALYSIS

The central issue on review by the Ninth Circuit was "whether the common carrier exemption in section 5 is status-based, such that an entity is exempt from regulation as long as it has the status of a common carrier under the 'Acts to regulate commerce,' or is activity-based, such that an entity with the status of a common carrier is exempt only when the activity the FTC is attempting to regulate is a common carrier activity."[18] In essence, the issue before the Ninth Circuit boiled down to whether Section 5's common carrier exemption applied to AT&T as a total entity, or whether only those AT&T activities duly classified as common carrier activities should be exempt from FTC jurisdiction.

By way of textbook-style statutory interpretation, the Ninth Circuit court split from the District Court's finding, ultimately finding the FTC Act's common carrier exemption to be status-based.[19] Pursuant to this interpretation, the Ninth Circuit concluded that the FTC was precluded from bringing a Section 5 enforcement action against AT&T due to the company's established status as a common carrier.[20]

In reaching its conclusion, the Ninth Circuit court focused on the plain language of Section 5 of the FTC Act.[21] The Court compared the statute's common carrier exemption to the other exemptions enumerated in Section 5.[22] In particular, the Court discussed the exemptions for banks, federal credit unions, savings and loan institutions, and air carriers and foreign air carriers, all of which the FTC acknowledged as status-based exemptions.[23] Due to the striking similarities between the statute's common carrier language and that of the other Section 5 exemptions, the Court reasoned that the "common carrier" exemption should be read similarly as a status-based exemption.[24]

Additionally, the Court looked to both the legislative history and the congressional intent behind the various Section 5 exemptions, specifically focusing on the statute's exemption for "entities 'subject to' the Packers and Stockyards Act."[25] Although the Packers and Stockyards Act exemption was originally status-based, the Court explained that Congress amended the statute's language to "exempt entities 'insofar as they are subject' to the Packers and Stockyards Act," essentially making the exemption activity-

17. *Id*. at 997–98.
18. *Id*.
19. *Id*. at 998.
20. *Id*.
21. *Id*. at 999.
22. *Id*. at 998.
23. *Id*.
24. *Id*.
25. *Id*. at 1002.

based.[26] The Court found this to be highly significant because Congress only amended the Packers and Stockyards Act exemption, leaving all of the other Section 5 exemptions unchanged. According to the Court, if Congress had so intended to, it could have amended or altered the common carrier exemption to explicitly clarify that the exemption is activity-based.[27] Because Congress amended one part of the Section 5 exemptions and left all of the other exemptions unchanged, the Ninth Circuit split from the District Court by ultimately concluding that Congress must not have intended to effectuate a transfer from a status-based to an activity-based exemption for common carriers under Section 5 of the FTC Act.[28]

CONCLUSION

The Ninth Circuit ultimately reversed the District Court's holding, concluding that AT&T enjoyed a status-based common carrier exemption and is therefore not within the FTC's jurisdiction. The Court declined to consider the issue of whether the FCC's Reclassification Order could be applied to AT&T retroactively.[29] The Court further declined to address the effect of overlapping regulations and oversight between the FTC and FCC common carrier regulation, refraining from comment on how to reset and rectify the boundaries between the agencies' respective jurisdictions.[30] The Ninth Circuit's analysis leaves open the possibility that so long as any segment of a company's business is classified as a common carrier, then all of a company's business activities fall outside of the scope of FTC jurisdiction. As of May 9, 2017, the U.S. Court of Appeals for the Ninth Circuit issued an order granting the FTC's request for rehearing *en banc* of the court's decision for dismissal.[31] The rehearing is currently pending before the Ninth Circuit.

26. *Id*. at 1002.
27. *Id*. at 998.
28. *Id*. at 1002.
29. *Id*. at 1003.
30. *Id*.
31. FTC v. AT&T Mobility LLC, No. 15-16585, 2017 U.S. App. LEXIS 8236 (9th Cir. Cal. May 9, 2017).

Global Tel*Link v. FCC

859 F.3d 39 (D.C. Cir. 2017)

Negheen Sanjar *

In *Global Tel*Link v. FCC*,[1] the United States Court of Appeals for the District of Columbia Circuit granted in part and denied in part petitions for review of the FCC's order regulating inmate calling services ("ICS") by setting permanent rate caps and ancillary fee caps for interstate and intrastate ICS calls.[2]

I. BACKGROUND

The Communications Act of 1934 ("1934 Act") granted the FCC regulatory authority over interstate telephone services, but left the regulation of intrastate telephone services primarily to the states.[3] This authority over interstate telephone services includes the authority to ensure all charges related to interstate calls are "just and reasonable."[4] The 1934 Act includes a presumption against the FCC's assertion of regulatory authority over intrastate communications.[5] However, the Telecommunications Act of 1996 ("1996 Act") gave the FCC some authority regarding intrastate activities.[6] The 1934 Act's presumption against FCC authority over intrastate communications is still in effect where Congress has remained silent, meaning that the FCC cannot regulate an aspect of intrastate communications that is not governed by the 1996 Act on the grounds that it has an ancillary effect on matters within the Commission's primary jurisdiction.[7]

In an effort to promote competition among payphone service providers, Congress enacted § 276 of the 1996 Act, which grants the FCC the authority to regulate, "inmate telephone services in correctional institutions, and any ancillary services."[8] This section further authorizes the FCC to act in a manner that promotes competition in the market.[9] Section 276 also preempts any state

* J.D. candidate, The George Washington University Law School, May 2018. Associate, *Federal Communications Law Journal*, 2017–18.

1. Global Tel*Link v. FCC, 859 F.3d 39 (D.C. Cir. 2017).
2. *See id.* at 44–45.
3. The Communications Act of 1934, 47 U.S.C. § 152(b).
4. 47 U.S.C. § 201(b).
5. 47 U.S.C. § 152(b).
6. *See* 859 F.3d at 45.
7. *See id.* at 45–46.
8. 859 F.3d at 46; *see also* 47 U.S.C. § 276(d)
9. *See* 859 F.3d at 46.

requirements that are inconsistent with FCC regulations pursuant to that section.[10]

Correctional facilities obtain telephone services through long-term exclusive contracts, for which payphone providers submit bids.[11] Site commissions, which usually consist of 20% to 63% of the provider's profits, are given considerable weight in a correctional facility's decision to award an ICS contract.[12] Once these contracts are awarded, competition ceases for the duration of the contract and any subsequent contract renewals, granting the ICS provider a locational monopoly.[13] The cost of the site commission is passed on to the inmates and their families.[14]

Concerned with what the FCC viewed as a "prime example of market failure" and ICS fees, the FCC set permanent rate caps for interstate and intrastate ICS calls and imposed other restrictions on ICS providers.[15] The FCC set the rate caps using a ratemaking method based on industry-averaged cost data, which excluded site commissions.[16] Later, the FCC raised the rate caps to account for a portion of the site commissions.[17]

In the instant case, various ICS providers filed separate petitions challenging the FCC's rate caps and ancillary fee caps for intrastate ICS.[18] Numerous state and local correctional authorities, governments, and correctional facility organizations also filed petitions and intervened on behalf of the Petitioners.[19] A putative class in a separate case regarding ICS fees as well as multiple inmate advocacy groups intervened on behalf of the Commission.[20]

ANALYSIS

Before delving into the Petitioners' complaints, the Court first decided whether the issue was moot.[21] Prior to oral argument, counsel for the FCC filed a letter advising the Court of changes in the agency's composition and informed the Court that as a result of those changes, counsel for the FCC would abandon the argument that the FCC has the authority to cap intrastate rates, and that the FCC lawfully considered industry-wide averages in setting rate caps.[22] The Court found that there was no basis for dismissing these

10. *See id.*
11. *See id.* at 46–47.
12. *See id.*
13. *See id.*
14. *See id.*
15. *Rates for Interstate Inmate Calling Services ("Order")*, 30 FCC Rcd. 12763, 12775-76, 12838-62 (2015).
16. *See id.* at 12818–38.
17. *Rates for Interstate Inmate Calling Services ("Reconsideration Order")*, 31 FCC Rcd. 9300 (2016).
18. *See* 859 F.3d at 48.
19. *See id.*
20. *See id.*
21. *See id.* at 49.
22. *See id.* at 48–49.

claims as moot because the FCC has not acted to revoke the Order, signifying that there has been no voluntary cessation.[23] Furthermore, neither the FCC, the Petitioners, nor the Intervenors urged for a declaration of mootness.[24]

The Court also addressed the question regarding the application of the *Chevron* framework when an agency no longer seeks deference.[25] Because the FCC abandoned its position regarding intrastate rate caps and the application of industry-wide averages in setting the rate caps, it would be nonsensical for the Court to determine whether the abandoned positions warrant *Chevron* deference.[26] Although *Chevron* deference does not apply to the abandoned issues, the Court still maintains jurisdiction to address those issues using the best reading of the statutory provisions at issue, and the rules of statutory construction.[27]

After determining *Chevron* inapplicable, the Court assessed the merits of the Petitioners' challenges to the Order.[28] The Petitioners challenged the FCC's authority to set permanent rate caps and ancillary fee caps for intrastate ICS calls.[29] Petitioners asserted that the FCC's § 276 mandate to ensure ICS providers are fairly compensated did not override the § 152(b) prohibition from regulating intrastate, "charges, classifications, practices, services, facilities, or regulations".[30] Petitioners also argued that § 276 did not give the FCC ratemaking authority over intrastate rates comparable to that of § 201.[31] Finally, Petitioners contended that the intrastate rate caps were nonsensical in light of the evidence demonstrating that ICS providers have higher costs than the rate caps.[32] The Court agreed with the Petitioners because the Order based its imposition of intrastate rate caps on a "just, reasonable and fair" test which is not articulated in the relevant portion of the statute, the Order conflated the FCC's grant of authority under § 276 and § 201, and misconstrued judicial precedent as well as FCC precedent in support of imposing intrastate rate caps to ensure providers are "fairly compensated".[33]

Next, the Petitioners argued that the exclusion of site commission payments from the costs the FCC used to set ICS rate caps was unlawful because ICS providers are required by state and local governments to pay site commissions, making site commissions a cost of providing service much like a tax or fee, which the FCC recognizes as recoverable costs.[34] Furthermore, the FCC acknowledged that rate caps were below providers' costs once site commission are taken into account, which violates the "fair compensation"

23. *See id.* at 49–50.
24. *See id.* at 49.
25. *See id.* at 50.
26. *See id.*
27. *See id.* at 50–51.
28. *See generally id.* at 51–59.
29. *See id.* at 51.
30. *Id.*
31. *See id.*
32. *See id.*
33. *See id.* at 51–55.
34. *See id.* at 55.

requirement under § 276, the "just and reasonable" requirement under § 201, and the Constitution's Takings Clause.[35] The Court found that the use of the average industry-wide cost in calculating rate caps was arbitrary and capricious because the site commissions are clearly a cost of doing business seeing as they are either mandated by state statute, or by state correctional facilities.[36]

Petitioners argued further that even if the site commissions were excluded, the rate caps were set too low to ensure compensation for each completed call because the FCC's rate caps are below average costs and would deny cost recovery for a significant portion of inmate calls.[37] Petitioners further contended that the FCC relied on data from outlier ICS providers who represent 0.1 percent of the market, and ignored evidence demonstrating the cost of ICS varies depending on the region services are provided in.[38] The Court found that the FCC did not engage in reasoned decision-making when it set rate caps for the reasons stated by the Petitioners, and because the averaging calculations are unreasonable seeing as they make above-average costs unprofitable, which violates the mandate for fair compensation contained in § 276.[39] Similarly, the Petitioners argued that the imposition of ancillary fees caps for interstate calls is impermissible.[40] The Court remanded the issue to the FCC because the Court could not determine from the record whether ancillary fee caps could be segregated between intrastate and interstate calls.[41]

In addressing the Petitioners' challenge of the video visitation requirements, the FCC asserted that regardless of whether video visitation services are a form of ICS, they are nonetheless under the agency's jurisdiction.[42] The Court disagreed finding that the FCC must first explain how its statutory authority extends to video visitation services under either § 201(b) for interstate calls, or § 276(d) as an inmate telephone service for interstate or intrastate calls.[43] In addition, the Petitioners challenged the site commission payment reporting requirement under 47 C.F.R. § 64.6060(a)(3). The FCC agreed with the Petitioners that the definition of site commission payments should be read as incentive payments designed to influence the selection of a monopoly service provider as opposed to an ordinary tax.[44] In light of this agreement, the Court found that there is no merit to the Petitioners' challenge.[45]

Finally, Petitioner Pay Tel separately challenged the FCC's refusal to preempt state ICS rate caps that are lower than those the Commission set in

35. *See id.* at 55.
36. *See id.* at 55–57.
37. *See id.* at 57.
38. *See id.*
39. *See id.* at 57–58.
40. *See id.* at 58.
41. *See id.*
42. *See id.*
43. *See id.*
44. *See id.*
45. *See id.*

the Order.[46] Petitioner Pay Tel also argued that its due process rights were infringed upon when the FCC denied Pay Tel timely access to key cost data that the FCC used in setting rate caps.[47] The Court held the preemption and due process claims moot because the Court vacated the portion of the Order imposing intrastate rate caps.[48]

CONCLUSION

In sum, the Court vacated the provisions of the Order regarding the imposition of intrastate rate caps, the use of averaged industry-wide cost data in the calculation of the Order's rate caps, the provision instituting video visitation reporting requirements, and the Order's exclusion of site commission from the FCC's cost calculus.[49] The Court also denied the petitions for review of the site commission reporting requirements and dismissed the preemption and due process claims as moot.[50] Finally, the Court remanded the Petitioners' challenge of the ancillary fee caps to the FCC for consideration as to whether the proposed fee caps can be segregated between the permissible caps on interstate calls and the impermissible proposed caps on intrastate calls.[51]

46. *See id.* at 59.
47. *See id.*
48. *See id.*
49. *See id.* at 45.
50. *See id.*
51. *See id.*

Montgomery County v. FCC

Nos. 08-3023/15-3578, 2017 U.S. App. LEXIS 12431 (6th Cir. July 12, 2017)

Lindsey Bergholz *

I. INTRODUCTION

In *Montgomery County v. FCC*,[1] the United States Court of Appeals for the Sixth Circuit held that while the FCC's "mixed-use" rule and interpretation of the term "franchise fee" were arbitrary and capricious, the FCC was not required to invalidate "most-favored-nation" clauses. The Court also held that the FCC made a good faith effort to comply with the Regulatory Flexibility Act ("RFA"). Though local franchising authorities have objected to these FCC's regulations for the past decade, this case marks the first time the Court has granted in part a local government's petition for review.[2]

BACKGROUND

In the 1950's, the American public began to have widespread access to cable television.[3] The Communications Act of 1934 ("the Act") gave the FCC the ability to regulate state and local franchising authorities in regards to cable franchises, and, in 1968, the Supreme Court "affirmed the FCC's regulatory authority over cable television[.]"[4] In 1984, Congress passed the Cable Act,[5] which preserved a role for local franchising authorities ("LFAs") by giving franchising discretion to states and localities.[6] Under the Cable Act, the FCC shared regulatory authority over cable with LFAs, who had "retained discretion to decide whether to grant cable franchises to applicants in their communities."[7]

---

* J.D. candidate, The George Washington University, May 2018. Associate, Federal *Communications Law Journal*, 2017–18.

1. Montgomery Cty. v. FCC, Nos. 08-3023/15-3578, 2017 U.S. App. LEXIS 12431 (6th Cir. July 12, 2017).
2. *See id.* at *2.
3. *See* All. for Cmty. Media v. FCC, 529 F.3d 763, 767 (6th Cir. 2008).
4. *Id.* at 767 (citing United States v. Southwestern Cable Co., 392 U.S. 157, 178 (1968)).
5. Cable Communications Policy Act of 1984, Pub. L. 98-549 (to be codified at 47 U.S.C. §§ 601–639).
6. *See* 47 U.S.C. § 541(f) (2012); *see also* Union CATV v. City of Sturgis, 107 F.3d 434, 441 (6th Cir. 1997) (quoting H.R. REP. NO. 98-934, at 19) ("It is the Committee's intent that the franchise process take place at the local level where city officials have the best understanding of local communications needs and can require cable operators to tailor the cable system to meet those needs.").
7. All. for Cmty. Media, 529 F.3d at 767.

Section 621 of the Cable Act requires cable companies to receive a franchise prior to offering service and gives LFAs the ability to dole out these franchises.[8] In 1992, Section 621 was amended[9] by Congress to prevent LFAs from monopolizing jurisdictions.[10] In 2006, the FCC implemented the "First Order," which set out the FCC's statutory interpretations of Section 621 and procedural compliance guidelines.[11] In the First Order, the FCC declined to preempt state regulations, and only addressed "decisions made by county- or municipal-level franchising authorities."[12] However, the First Order did lay out "reasonableness" guidelines for I-Nets[13] and Public Educational and Governmental ("PEG") facilities, and calculation guidelines for franchise fees.[14] The First Order also preempted "most-favored-nation clauses"[15] which LFAs used to require new cable providers to meet expectations that incumbent providers were exempt from, and limited "LFAs' jurisdiction . . . only to the provision of cable services over cable systems[,]" so that mixed-use networks no longer fell under LFAs' control.[16]

In 2007, the FCC released the Second Order, and then a Reconsideration Order clarifying the Second Order. Together, these new orders expanded the First Order's regulations on new entrants to incumbent cable operators. The Second Order touched upon LFAs, PEG facilities,[17] I-Nets,[18] franchise fees,[19] most-favored-nation clauses,[20] and mixed-use networks[21]—and in several of these areas, the LFAs' authority and jurisdictional reach shrunk.

ANALYSIS

Petitioners are local governments that argue the Second Order and Reconsideration Order are arbitrary and capricious and could not pass a *Chevron* analysis, because the orders deprive "local governments of their jurisdiction under the Cable Act, apply[] franchise fee caps where they do not

8. *See* 47 U.S.C. § 541(b), (e)–(f) (2012).
9. The Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779.
10. *See* All. for Cmty. Media, 529 F.3d at 768.
11. *See* Implementation of Section 621(a)(1) of the Cable Communications Policy Act, 72 Fed. Reg. 13230-01 (proposed Mar. 21, 2007) (to be codified at 47 C.F.R. pt. 76) [hereinafter "First Order"].
12. First Order, *supra* note 11, at n.2.
13. Montgomery Cty., 2017 U.S. App. LEXIS 12431, at *16 ("Institutional networks provide various services to non-residential subscribers, rather than just video services to residential subscribers (which is all that the mixed-use rule seems to allow local franchising authorities to regulate).").
14. *See* First Order, *supra* note 11, at para. 5.
15. *Id.* at para. 140.
16. *Id.* at para. 121.
17. Implementation of Section 621(a)(1) of the Cable Communications Policy Act, 22 FCC Rcd 19633, para. 14 (2007) [hereinafter "Second Order"].
18. *Second Order*, *supra* note 17, at para. 14.
19. *Id.* at para. 11.
20. *Id.* at para. 20.
21. *Id.* at para. 16–17.

apply such that they constrain franchises . . . and fail[] to recognize the instances where LFA's have authority over cable systems[.]"[22] Ultimately, the Court vacated the FCC's interpretation of "franchise fee" for in-kind, cable-related noncash exactions and vacated the mixed-use rule as applied to incumbent cable operators for being arbitrary and capricious.[23] However, the Court upheld the FCC's decision not to invalidate most-favored-nation clauses, and found the FCC did make a reasonable, good faith effort to comply with the Regulatory Flexibility Act ("RFA").[24]

In regards to franchise fees, the Court found that the Reconsideration Order's categorizations of Section 622 to include "in-kind payments" expressly went against the FCC's First Order, and constituted a total reversal with "no explanation" of the statutory support for such reversal.[25] Citing *Encino Motocars*,[26] the Court reminded the FCC that "if an agency wants the federal courts to adopt (much less defer to) its interpretation of a statute, the agency must do the work of actually interpreting it."[27]

The Court similarly found the Second Order had insufficient reasoning to support the FCC's new mixed-use rule. The FCC's statutory basis for the mixed-use rule in the First Order "does not by its terms support the FCC's extension of the mixed-use rule to incumbent cable operators in the Second Order."[28] The Court determined that the FCC's mixed-use rule was arbitrary and capricious because the FCC failed to cite any other statutory explanation for their decision, despite the lack of statutory support for the Second Order's mixed-use restrictions.[29] However, the Court explicitly rejected Petitioners' challenges to the "most-favored-nation" clauses.[30] The Court rejected this challenge because Petitioners failed to provide "any evidence, as opposed to speculation, that the FCC's decisions in this area will somehow thwart Congress's intent as expressed by the Act's plain terms."[31]

The Court also disagreed with the argument that the FCC's Reconsideration Order fell short of meeting the Regulatory Flexibility Act's ("RFA") statutory requirements.[32] Petitioners argued that the FCC had "failed to meet the 'purely procedural' requirements of the Regulatory Flexibility Act."[33] The Court disagreed with Petitioners' emphasis procedures, and instead sided with the FCC, finding "the agency made a 'reasonable, good faith effort' to comply with the [RFA's] requirements."[34] Ultimately, much of

22. Brief of Petitioner at 3–4, Montgomery Cty. v. FCC., No. 08-3023 (6th Cir. Feb. 26, 2016).
23. *See* Montgomery Cty., 2017 U.S. App. LEXIS 12431, at *14, *18–19.
24. *See id.* at *19–25.
25. *See id.* at *13, *14.
26. *Encino Motorcars, LLC v. Navarro*, —— U.S. ——, 136 S.Ct. 2117, 2125 (2016).
27. Montgomery Cty., 2017 U.S. App. LEXIS 12431, at *13, *14.
28. *Id.* at *17.
29. *See id.* at *18.
30. *See id.* at *19–21.
31. *Id.* at *21.
32. *See id.* at *23–24.
33. *Id.* at *23.
34. *Id.* at *24.

the FCC's Second Order and Reconsideration Order will remain unchanged. The Court left the majority of the FCC's franchise fee additions untouched, and the Court did not change the PEG requirements, incidental exclusions, or the five-percent fee caps set out in the Second Order.[35]

CONCLUSION

The FCC's mixed-use rule and franchise fee interpretations as outlined in the Second Order and Reconsideration Order have been remanded back to the FCC so the agency can give a timely and sufficient explanation for the vacated orders.[36] Until then, the FCC cannot "treat 'in-kind' cable-related exactions as 'franchise fees[,]'" or apply "the mixed-use rule to incumbent cable providers that are not common carriers[.]"[37]

35. *See id.*
36. *See id.* at *14, *19.
37. *Id.* at *14, *18.

National Association of Regulatory Utility Commissioners v. FCC

851 F.3d 1324 (D.C. Cir. 2017)

Kristin Capes *

In *National Association of Regulatory Utility Commissioners v. FCC*,[1] the United States Court of Appeals for the District of Columbia Circuit denied a petition for review of an FCC Order which changed the way Voice-over-Internet-Protocol service providers obtain North American Numbering Plan telephone numbers.[2]

I. BACKGROUND

Under the Communications Act, communication services are classified in two groups: telecommunications services and information services.[3] One important distinction between the two types is that, unlike information services, telecommunications services are treated as "common carriers" as defined by Title II of the Communications Act.[4] Prior to the challenged Order, in order for an I-VoIP service provider to be issued telephone numbers, the I-VoIP had to: (1) "produce evidence of either a state certificate of public convenience and necessity [ ] or a Commission license," (2) "partner with a carrier…and pay that carrier a Primary Rate Interface service fee," or (3) get a waiver from the FCC allowing the I-VoIP service provide to "obtain numbers directly from the Numbering Administrators." [5] The challenged Order revised the process by which I-VoIPs could obtain telephone numbers, allowing the I-VoIPs direct access to obtaining telephone numbers "without regard to whether they are [common] carriers."[6] However, the challenged Order did not establish I-VoIPs as telecommunications services or information services; rather, the FCC mentioned in the Order that they had not yet classified I-VoIPs into a specific communication service category.[7]

The National Association of Regulatory Utility Commissioners challenged the Order on two grounds: (1) the Order incorrectly classified I-

* J.D. candidate, The George Washington University Law School, May 2017. Production Editor, *Federal Communications Law Journal*, 2017–18.

1. Nat'l Ass'n of Regulatory Util. Comm'rs v. FCC, 851 F.3d 1324 (D.C. Cir. 2017).
2. *See Id.*
3. *Id.* at 1326.
4. *Id.*
5. *Id.*
6. *Id. (quoting* Order App. C.)
7. *Id.*

VoIP service providers as Title II telecommunications services, or (2) the Order gave Title II telecommunications services rights to I-VoIP service providers without those providers being classified as Title II providers.[8] The FCC claimed that the National Association of Regulatory Utility Commissioners (NARUC) lacked standing to challenge the Order because they had no proof of injury-in-fact to their members.[9] Vontage Holdings Corporation, who acted as an intervenor in the case, claimed that NARUC lacked standing to challenge the Order because the Order did not "change the rights or responsibilities" of NARUC's members.[10]

ANALYSIS

In NARUC's Opening Brief, they claimed that standing was self-evident on the basis of their claims against the FCC. The court rejected that argument, holding that standing was not self-evident.[11] Additionally, the court noted that if standing is not self-evident, then the moving party must provide evidence supporting each element of standing.[12] For NARUC to meet the requirements of standing as defined by Article III of the Constitution, NARUC had to show that: "(1) at least one of its members was injured in fact…; (2) the injury was caused by the Order; and (3) the court can redress the injury."[13] In their Reply Brief, NARUC introduced two theories of standing.[14]

NARUC's first theory of standing was that by not classifying I-VoIPs as telecommunication services the FCC is impeded on the states' ability to regulate I-VoIPs in the same manner they regulate common carriers while giving I-VoIPs Title II benefits.[15] The court held that NARUC's first theory of standing failed because it linked the perceived injury to the FCC's refusal to classify I-VoIPs rather than the actual holding of the Order.[16] Additionally, the NARUC failed to provide evidence supporting their assertion that they have been injured by the FCC's refusal to classify I-VoIPs in the Order.[17]

NARUC's second theory of standing was that its members were harmed by the holding of the Order by permitting "I-VoIP providers the option to bypass either becoming State-certified or dealing with a State-certified carrier."[18] NARUC claimed their members were harmed by the changes instituted by the Order because of the burden it places on the states.[19] The

8. *Id.* at 1325.
9. *Id.* at 1327.
10. *Id.*
11. *Id.*
12. *Id.*
13. *Id*.
14. *Id.*
15. Id. At 1328.
16. *Id.* at 1328.
17. *Id.*
18. *Id.*
19. *Id.*

court held that NARUC's second theory of standing failed because the NARUC failed to provide any evidence to support their assertion that the state commission procedures have become more burdensome due to the new regulations instated by the Order.[20]

CONCLUSION

The United States Court of Appeals for the District of Columbia Circuit dismissed the petition on the grounds that the Court lacked jurisdiction to decide the issue because the National Association of Regulatory Utility Commissioners' failed "to show that it [had] standing to challenge the Order."[21]

20. *Id.* at 1329.
21. *Id.* at 1325.

National Association of Telecommunications Officers & Advisors v. FCC

862 F.3d 18 (D.C. Cir. 2017)

Lindsey Bergholz *

I. INTRODUCTION

In *National Association of Telecommunications Officers & Advisors v. FCC*[1] the Court of Appeals for the District of Columbia Circuit upheld the FCC's reversal of "a decades-old, rebuttable presumption that determined whether state and local franchising authorities may regulate cable rates."[2] The D.C. Circuit held that the FCC's rule, shifting the presumption to favor cable providers over local franchising authorities, was neither arbitrary nor capricious, and was a permissible interpretation of the statutory language.[3]

BACKGROUND

The Cable Act[4] gives the FCC the ability to decide whether a franchising authority can regulate cable rates.[5] If the FCC "finds that a cable system is subject to effective competition," then neither the FCC nor "a State or franchising authority" will have the ability to regulate rates.[6] However, if the FCC "finds that a cable system is not subject to effective competition," the FCC can regulate the rates for cable programming services or delegate rate regulations to the franchising authorities.[7]

Soon after Congress passed the Cable Act, the FCC clarified that the cable providers carry the burden of proving they are not "subject to effective competition" if they wish to rebut the presumption that their rates can be

* J.D. candidate, The George Washington University, May 2018. Associate, Federal *Communications Law Journal*, 2017–18.

1. Nat'l Ass'n of Telecomms. Officers & Advisors v. FCC, 862 F.3d 18 (D.C. Cir. 2017).
2. *Id.* at 21.
3. *See id.* at 25.
4. Cable Television Consumer Protection and Competition Act of 1992, Pub. L. No. 102-385, 106 Stat. 1460 [hereinafter "the Cable Act"].
5. *See* 47 U.S.C. §§ 543(a)(2), (l)(1) (2012).
6. *Id.* § 543(a)(2).
7. *Id.*

regulated.[8] This presumption, outlined in the 1993 Rate Order, required cable systems to prevent rate regulation by proving that a competitor not only offered services in that community, but that those services were "actually available" to consumers.[9] When the 1993 Rate Order's presumption was adopted the "vast majority" of regulated regions only had one cable service.[10] The presumption has played an important role in rate regulation authority because, practically speaking, "given the sheer number of franchise areas….[the FCC could not] make an affirmative finding…as to the presence or absence of effective competition" in each area without excessive and unreasonable delay in issuing approvals.[11]

In 2015, the FCC publicly recognized the role multichannel video programming distributors ("MVPDs") and direct broadcast satellites ("DBS") have come to play in the cable landscape; the FCC concluded this rise in competition justified flipping the presumption from assuming no competition, to assuming competition.[12] The FCC's original presumption of no competition was adopted before MVPD and DBS service had "enter[ed] the market…in any significant way."[13] After the 2015 adjustment that recognized the mass availability of DBS and MVPDs, local franchising authorities could no longer regulate cable rates unless they provide evidence that the cable system exists without competition.[14]

ANALYSIS

The petitioners in this case are broadcasters and franchising authorities. The petitioners challenged the FCC's statutory authority to revise the 1993 Rate Order, and also argued the FCC's new presumption of effective competition is arbitrary and capricious.[15] In the end, the Court ruled the FCC did have the authority to bar franchising authorities from regulating cable rates under Section 543 until those authorities have proven that their franchise region has effective competition.[16] The Court also ruled that the FCC's

8. Implementation of Section of the Cable Television Consumer Protection & Competition Act of 1992: Rate Regulation, 8 FCC Rcd 5631, para. 39 (1993), *on reconsideration*, 9 FCC Rcd 4316 (1994), *rev'd in part on other grounds*, Time Warner Entertainment Co., L.P. v. FCC, 56 F.3d 151 (D.C. Cir. 1995) (the FCC "stated that since the Act makes the absence of effective competition a prerequisite to regulators' legal authority over basic cable rates, it would be reasonable to require local franchising authorities to provide evidence of the lack of effective competition as a threshold matter of jurisdiction") [hereinafter "1993 Rate Order"].

9. *Id.* at para. 29 (clarifying 47 U.S.C. § 543(l)(1)(B)(i)).

10. Amendment to the Commission's Rules Concerning Effective Competition, 30 FCC Rcd 6574, para. 3 (2015) [hereinafter "Amended Rules 2015"].

11. 1993 Rate Order, *supra* note 8, at para. 41.

12. *See* Amended Rules 2015, *supra* note 10, at para. 6–12.

13. Amended Rules 2015, *supra* note 10, at para. 3.

14. *See* Amended Rules 2015, *supra* note 10, at para. 13.

15. *See* Nat'l Ass'n of Telecomms. Officers & Advisors, 862 F.3d at 6.

16. *See id.* at 13–14.

rebuttable presumption of effective cable operator competition was reasonable.[17]

Petitioners specifically argued that the FCC's "termination of previously issued certifications violate the Communications Act for three reasons."[18] First, petitioners argued the FCC did not follow proper procedures under Sections 543(a)(2) and (l)(1)(B).[19] In response to petitioners' argument that the FCC was procedurally deficient, the Court cited *National Cable & Telecommunications Association v. Brand X Internet Services*,[20] which held that "whether the Order implements 'a lawful construction of the …. Act [must be decided] under Chevron.'"[21] The Court concluded the FCC acted within its delegated authority because the FCC "provided ample evidence" to support its determination, and was therefore reasonable.[22]

Second, petitioners "challenge[d] the [FCC's] authority to revoke a previous certification" under Section 543(a)(5) of the Communications Act.[23] Relying on the plain text of Section 543(a)(5), the Court held the FCC would actually have defied "a clear congressional directive if it continued to regulate rates after finding effective competition," and, therefore, was acting in accordance with the "overall statutory scheme."[24] Third, petitioners argued that the FCC's rule violated the STELAR Act, which requires the FCC "to establish a streamlined process for filing of an effective competition petition."[25] The Court determined the FCC did not eliminate the filing process, it only changed the filing process, and because the language at issue in this case was ambiguous with respect to "the procedures the [FCC] must use in a new 'streamlined process,'… the [FCC's] chosen procedures are a reasonable interpretation" under Chevron step two.[26]

The Court also addressed petitioners' claims that the FCC's rule was arbitrary and capricious. Citing *Chemical Manufacturers. Association v. Department of Transportation*,[27] the Court ruled that the FCC did have "a sound and rational connection between the proved and inferred facts" when establishing its presumption.[28] The Court agreed that the FCC's evidence on MVPD availability "combined with the 'ubiquitous' national presence of DBS providers[] supports a rebuttable presumption" that the FCC's statutory requirements have been met.[29] Finally, the Court rejected the argument that

17. *See id.* at 11, 18.
18. *Id.* at 7.
19. *See id.* at 7.
20. Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967 (2005).
21. Nat'l Ass'n of Telecomms. Officers & Advisofrs, 862 F.3d at 7 (citing Chevron U.S.A. Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837 (1984)).
22. Nat'l Ass'n of Telecomms. Officers & Advisors, 862 F.3d at 9.
23. *Id.* at 7.
24. *Id.* at 15.
25. *Id.* at 7, 15.
26. *Id.* at 18.
27. Chem. Mfrs. Ass'n v. Dep't of Transp., 105 F.3d 702, 705 (D.C. Cir. 1997).
28. Nat'l Ass'n of Telecomms. Officers & Advisors, 862 F.3d at 20 (citing Chem. Mfrs. Ass'n. 105 F.3d at 705) (internal citations omitted).
29. Nat'l Ass'n of Telecomms. Officers & Advisors, 862 F.3d at 22.

the FCC's "selection bias" poisoned the FCC's statistical evidence, noting the FCC provided "reasonable assurance the effect of any selection bias is quite modest and does not make the [FCC's] inference unreliable, let alone irrational."[30]

CONCLUSION

The FCC has successfully defended its new order, lifting the burden of proving effective cable competition exists off of cable providers, and placing the burden of proving a lack of effective competition exists onto local regulating authorities. It remains to be seen whether this case paves the way for other deregulatory presumption flips, or stands alone as a response to changing cable market realities.

30. *Id.* at 24.

Neustar, Inc. v. FCC

857 F.3d 886 (D.C. Cir. 2017)

Jane Lee *

In *Neustar, Inc. v. FCC*, [1] the United States Court of Appeals for the District of Columbia Circuit denied petitions for review of FCC's orders naming another telecommunications provider, Telcordia, to replace Neustar as the local number portability administrator ("LNPA").

The Telecommunications Act of 1996 requires telecommunications providers to provide "portability" of telephone numbers, permitting customers to keep their current phone numbers when they switch carriers.[2] In its 1996 First Report and Further Notice of Proposed Rulemaking, the FCC concluded that it is in the public interest for the number portability databases to be administered by one or more neutral third parties, and thus the LNPA was created.[3]

In 2009, upon the petition of Telcordia to "institute a competitive bid process for the LNPA contract," the FCC began a collaborative public process and released bid documents.[4] After reviewing the bids, the North American Numbering Council recommended Telcordia as the LNPA, which Neustar objected to on procedural grounds concerning the selection process and on substantive grounds regarding costs and bidders' qualifications.[5] Reasoning that the LNPA selection does not require notice-and-comment rulemaking, and that the proceeding is properly viewed as an informal adjudication in its March 2015 Order, the FCC approved the recommendation of Telcordia as the LNPA.[6]

Neustar argued, however, that the selection must be accomplished by a rulemaking to amend the existing rules, mainly to be in accordance with the Administrative Procedure Act ("APA")'s definition of a "rule."[7] A "rule" is defined "broadly to include 'statements of general or particular applicability and future effect' that are designed to 'implement, interpret, or prescribe law or policy," and the Court held that this case does not qualify under the statutory definition of a "rule," so rulemaking procedures are not required.[8]

---

* J.D. candidate, The George Washington University, May 2018. Editor-In-Chief, *Federal Communications Law Journal*, 2017–18.

1. *Neustar v. FCC*, 857 F.3d 886 (D.C. Cir. 2017)
2. 47 U.S.C. § 251(b)(2).
3. 11 FCC Rcd. 8352, 8399 (1996).
4. 30 FCC Rcd. 3082, 3086 (2015).
5. *See, id.* at 3092-3115.
6. *Id.* at 3093.
7. *Id.* at 3092.
8. *See Perez v. Mortgage Bankers Ass'n*, 135 S.Ct. 1199, 1199, 1203 (2015).

Neustar argues that the FCC's selection of Telcordia was contrary to law or arbitrary and capricious, based on an improper understanding and application of the neutrality regulations.[9] The FCC responded that although both Neustar and Telcordia are both qualified to serve as the LNPA, a legitimate cost analysis warranted recommendation of Telcordia as the next LNPA.[10]

Neustar argued that Telcordia cannot be neutral because Telcordia's parent company is Ericsson, which is an equipment manufacturer and service provider.[11] Rejecting this argument, the FCC supported its neutrality determination by emphasizing that such telecommunications sector connections were with Ericsson, not Telcordia.[12] Upon the analysis of the relationship between Ericsson and Telcordia, which is a wholly owned subsidiary of Ericsson, the FCC looked at the corporate structure and related business arrangements to confirm Telcordia's neutrality.[13] Finding that Telcordia is a "separate company with a separate independent board of directors, each of whom owes fiduciary duties to Telcordia," the FCC argued that even if Ericsson is aligned with the wireless industry, it does not necessarily follow that Telcordia is likewise aligned.[14]

In this case, it is important to distinguish what *must* be achieved through rulemaking under the statute and what *may* be achieved through informal adjudication.[15] The decision of this case largely relies on the fact that the FCC has "very broad discretion to decide whether to proceed by adjudication or rulemaking."[16] In fact, the Court rules that the text of Section 251 is broad enough to encompass process to implement the statutory requirements through rulemaking, even if the outcomes are achieved through informal adjudication.[17] The Court also held the FCC's hand in that since the FCC has not incorporated a specific LNPA by rule, the selection of a new LNPA also would not need to follow rulemaking procedures.[18]

Under the APA, a "reviewing court shall ... hold unlawful and set aside agency action, findings, and conclusions found to be ... arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law."[19] Courts will defer to the Commission's reading of its own regulations unless that reading is plainly erroneous or inconsistent with the regulations.[20] Therefore, the

9. *Neustar* at 891.
10. *Id.* at 901.
11. *Id.* at 890.
12. *Id.*
13. *Neustar* at 898.
14. *Id.* at 890.
15. *Id.* at 892–93.
16. *Conference Grp., L.L.C. v. FCC*, 720 F.3d 957, 965 (D.C. Cir. 2013).
17. *Neustar* at 892.
18. *Id.*
19. 5 U.S.C. § 706(2)(A).
20. *Auer v. Robbins*, 519 U.S. 452, 461 (1997) (quoting *Robertson v. Methow Valley Citizens Council*, 490 U.S. 332, 359 (1989).

FCC's determination that Telcordia satisfied the Act's requirements and the FCC's regulations was decided not to be arbitrary and capricious.[21]

Significantly, although the FCC briefly referenced *Chevron*'s deferential standard in its standard of review, it did not invoke this standard with respect to rulemaking. Accordingly, the Court held that the FCC's interpretation of the statutory mandate would not be entitled to deference in this case.[22]

Analyzing the overall context and benefits of the bids led the FCC to conclude that the benefits "outweigh the costs and potential adjustments associated with the transition to a new LNPA."[23] The FCC reiterated that Telcordia's bid had merit that "outweigh[ed] the costs and potential adjustments associated with the transition to a new LNPA," and thus Court could not conclude that the cost analysis was arbitrary and capricious.[24]

21. *Neustar* at 891.
22. *Id.* at 893.
23. *Id.* at 902.
24. *Id.*

Tennessee v. FCC

832 F.3d 597 (8th Cir. 2016).

Ryan Farrell *

In *Tennessee v. FCC*,[1] the Sixth Circuit Court of Appeals invalidated the FCC's 2015 order preempting laws in Tennessee and North Carolina restricting the expansion of municipal broadband.[2] The court found that Section 706 of Telecommunications Act of 1996 fell short of the clear statement that is required to preempt the allocation of power between the states and its subdivisions.[3]

I. BACKGROUND

This case concerns municipal broadband—specifically, whether, contrary to state law, municipalities that provide broadband internet service can expand to cover underserved areas that lie outside of their coverage area.[4] The state legislatures of Tennessee and North Carolina thought statute answered this question when they enacted laws that restricted the expansion of municipal broadband to these underserved areas.[5]

Tennessee enacted a law in 1999 which authorized municipalities operating an electric plant to offer internet services.[6] Sec. 601 of the law limited the area in which municipalities may provide internet services to only "within its service area."[7] This prevented a municipality from offering broadband services to surrounding areas not within its service area.[8] At the time, there was no FCC rule or regulation that required municipalities to offer broadband services outside of its coverage area.[9]

Eventually, developments in technology led to municipalities providing high speed, reliable broadband service.[10] The city of Chattanooga, Tennessee began offering high-speed broadband internet services through its' municipal electric provider.[11] Chattanooga developed a fiber-optic communication

* J.D. candidate, The George Washington University, May 2018. Managing Editor, *Federal Communications Law Journal*, 2017–18.

1. *Tennessee v. FCC*, 832 F.3d 597 (8th Cir. 2016).
2. *Id.* at 614
3. *Id* at 600.
4. *See Id.*
5. *Id.* at 600–01.
6. *Id.* at 600 (citing Tenn. Code Ann. 7-52-601).
7. *Id.*
8. *See Id.*
9. *See Id.*
10. *Id.*
11. *Id.*

infrastructure, and became the first broadband provider in the nation to offer Gigabit services to all of its customers.[12] According to the FCC's findings, Chattanooga's municipal broadband service is a success, providing added revenue to the city, leading to job growth, and lowering rates and increasing services among broadband providers.[13] Despite this, Sec. 601 of Tennessee's municipal broadband law prevented Chattanooga from expanding the service beyond its service area to underserved areas.[14]

North Carolina enacted its own municipal broadband restrictions in 2011, limiting city-owned communications service providers to provide service only within their municipal boundaries.[15] The law also places additional restrictions on municipal broadband providers by forcing them to make payments in lieu of taxes and opening their facilities up to private actors.[16] The law also contained three provisions that exempted municipalities from the restrictions, including "grandfather" exemptions which exempt municipalities "providing communications services as of January 1, 2011" from the restrictions, so long as they abide by limitations.[17] Like the Tennessee law, the North Carolina law did not conflict with any FCC rules or regulations at the time of enactment.[18]

Like Chattanooga, Tennessee, Wilson, North Carolina constructed a highly rated municipal broadband service named "Greenlight".[19] Also like Chattanooga, Wilson faced demand from surrounding communities.[20] However, if Wilson attempted to expand into these surrounding communities, they would no longer be grandfathered from North Carolina's municipal broadband restrictions.[21] As a result, Wilson had been unable to expand beyond its municipal borders.[22]

Chattanooga and Wilson separately petitioned the FCC to preempt the restrictions that prevented them from expanding beyond their borders.[23] The FCC responded by finding that preempting the two laws would increase competition and broadband investment.[24] The FCC found that both the Tennessee and North Carolina laws constituted barriers to broadband investment and competition.[25] The FCC issued an order preempting both statutes.[26]

---

12. City of Wilson, North Carolina Petition for Preemption of North Carolina eneral Statute Sections 160A-340 Et Seq., *Memorandum Opinion and Order*, 30 FCC Rcd 2408 (2015) at *10 [hereinafter *2015 Wilson Order*].
13. *Id.* at *7–8.
14. *Id.* at *9.
15. N.C. Gen. Stat. Ann Sec. 160A-340.1(a)(3).
16. *Tennessee*, 832 F.3d at 601.
17. *See id.* at 601–02.
18. *Id.* at 602.
19. *2015 Wilson Order*.
20. *Tennessee*, 832 F.3d at 602.
21. *Id.*
22. *Id.*
23. *Id.*
24. *Id.* at 602–03.
25. *Id.* at 603–04.
26. *Id.* at 605.

The FCC found that Congress granted the FCC the authority to pre-empt the laws through Sections 706(a)-(b) of the Telecommunications Act of 1996.[27] The FCC cited the preamble of the law, which stated the express goal of promoting competition in the marketplace, and noted Section 706 is the part of the law that gives the FCC the authorization to achieve this goal.[28] Addressing criticism that focused on the point that only Congress can grant the FCC power to preempt state law through explicit statutory language, the FCC argued the statutory language of Section 706 is not exhaustive and includes "the rule common throughout communications law"—that the FCC may preempt state laws.[29]

The FCC proceeded to preempt several parts of both the Tennessee and North Carolina laws.[30] In his dissent, Commissioner Ajit Pai, citing *Nixon v. Missouri Municipal League*, argued that the FCC could not preempt the state laws without an express statement from Congress.[31] Indeed, Commissioner Pai argued that Section 706 did not grant FCC any preemptive power at all.[32]

DISCUSSION

The Court began its analysis by noting that in its order the FCC was attempting to insert its authority into matters between a State and its municipal subdivisions.[33] The court also noted that the FCC could not do this absent a clear directive from Congress granting this authority.[34] As stated before, at the time these state laws were enacted no FCC rules or regulations, or directive from Congress, existed preventing states from placing restrictions on municipal broadband providers.

The Sixth Circuit Court rejected the FCC's arguments that Section 706 of the Communications Act gave them the authority to preempt the Tennessee and North Carolina laws. The FCC had attempted to distinguish their pre-emption here from the holding in *Nixon*, which struck down a Missouri state statute that forbade municipalities from entering the Telecommunications market.[35] The FCC argued that there is a difference between pre-empting a state ban on telecommunications providers and pre-empting state laws regulating an industry that the state has already authorized.[36] The FCC also argued that pre-empting state laws on municipal broadband did not implicate the core state sovereignty that was at stake in *Nixon*. The Sixth Circuit Court disagreed, noting that the issues invoked in this case are similar to those in

27. *Id.*
28. *See Id.* at 606.
29. *Id.* at 607.
30. *Id.* at 608.
31. *Id.* at 609 (citing *Nixon v. Missouri Municipal League*, 541 U.S. 125 (2004)).
32. *Id.*
33. *Id.* at 610.
34. *See id.* (citing *Nixon*).
35. *Nixon*, 541 U.S. at 129/
36. *Tennessee*, 832 F.3d at 611.

Nixon in that they involve state sovereignty *and* the regulation of interstate communications services.[37]

The Court also further held that Section 706 lacks a clear statement from Congress authorizing the FCC to engage in pre-empting the state laws.[38] The court noted that although Section 706 authorizes the FCC to achieve the goal of promoting competition, it does not authorize it to do so by preempting state law.[39]

The Court declined to address the assertion advanced by Commissioner Pai of whether or not Section 706 provides the FCC preemptive power at all.[40] The court also declined to say whether or not Congress could actually give the FCC the power to preempt as it did here.[41]

Judge Helene N. White wrote concurring in part and dissenting in part. Judge White agreed that the holding in *Nixon* compelled the reversal of the FCC's order.[42] Judge White, however, articulated a more relaxed view of the Clear Statement rule, stating that it should not require a clear statement whenever the regulation or statute preempted affects local government.[43]

CONCLUSION

The 6th Circuit's decision was a blow to the FCC's efforts to advance its municipal broadband effort. The 6th Circuit handed down a clear message: if the FCC wishes to promote marketplace competition as they see it, they cannot do it by interfering with a state's regulation of municipal affairs absent a clear direction from Congress.

37. *Id.*
38. *Id.* at 613.
39. *See Id.*
40. *Id.*
41. *Id.*
42. *Id.* at 614
43. *Id.* at 615