UNIVERSITY OF PITTSBURGH LAW REVIEW
Vol. 80 ● Summer 2019

NET NEUTRALITY REPEAL RIPS HOLES IN THE PUBLIC SAFETY NET

Catherine J.K. Sandoval

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

NET NEUTRALITY REPEAL RIPS HOLES IN THE PUBLIC SAFETY NET

Catherine J.K. Sandoval*

I. PUBLIC SAFETY PARADIGMS IN THE INTERNET AGE

A. The Public's Role in Public Safety

This Article contends that the Federal Communications Commission's ("FCC") failure to address the public safety risks of repealing net neutrality rules in its January 2018 "*Internet Freedom Order*" ignores the FCC's statutory mission to promote public safety and violates the Administrative Procedures Act ("APA").[1] Net neutrality is "the principle that broadband providers must treat all internet traffic the same regardless of source."[2] The *Internet Freedom Order* fails to address the public safety rationale for the bright-line net neutrality rules previously adopted in the FCC's *2015 Open Internet Order* ("*2015 Order*").[3] In support of its ban on paid priority arrangements with Internet Service Providers (ISPs), the FCC's *2015 Order*

* Associate Professor, Santa Clara University School of Law (SCU Law). Former Commissioner, California Public Utilities Commission (Jan. 2011 to Jan. 2017). Appointed by the Federal Communications Commission to the Federal-State Joint Conference on Advanced Telecommunications Services, 2013–Jan. 2017; State Chair 2014–2015, State Policy Chair, 2013–2014. Thanks to SCU Law, its faculty and students for their support for this research and an open Internet. Special thanks to my top-notch research assistant, Luke Batty, SCU Law Class of 2019, for his research work and contributions to drafting this Article, including his detailed review of the *Mozilla v. FCC* oral arguments. Special thanks to my husband, Steve Smith, for his kindness and boundless support.

[1] Restoring Internet Freedom, 83 Fed. Reg. 7852, 7852 (Feb. 22, 2018) (repealing FCC rules adopted in 2015 that prohibited ISPs from blocking, throttling, or engaging in paid prioritization of Internet traffic except for limited reasonable network management justifications); In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311 (2018); APA, 5 U.S.C. § 551 (2012); 5 U.S.C.A § 706 (West) (Scope of Judicial Review); Mozilla v. FCC, ___ F.3d ___, 95, 97, 100 (2019) (citing comments of Catherine Sandoval to support decision to remand the *Internet Freedom Order* to the FCC for failure to analyze public safety).

[2] U.S. Telecom Ass'n v. FCC, 825 F.3d 674, 689 (D.C. Cir. 2016).

[3] In the Matter of Protecting & Promoting the Open Internet, 30 FCC Rcd. 5601, 5604 (2015).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

cited the comments that I filed while serving as a Commissioner of the California Public Utilities Commission ("CPUC"). My comments expressed concern that Internet "paid prioritization undermines public safety and universal service."[4] The *Internet Freedom Order* fails to recognize the public's role in public safety enabled through the Internet's bilateral and multilateral communications channels.[5] This Article unmasks the "Cat Video" paradigm that the FCC's *Internet Freedom Order* employs to diminish the importance of public Internet communications. It concludes that an open Internet safeguarded from ISP interference protects the public's role in public safety and democracy.

This Article fills a gap in the net neutrality academic literature by conceptualizing the Internet's technological and regulatory evolution in the context of the public's role in public safety. It views people as content creators and public safety co-creators, who depend on open and neutral access to the Internet to share public safety information through video, text, Geographical Information System ("GIS") and other formats. The academic literature on net neutrality and public safety published to date has largely focused on institutional public safety roles and government Internet access for public safety.[6] This Article, along with my Article

---

[4] *Id.* at 5654–55 n.91 (citing Catherine J.K. Sandoval, Commissioner, Cal. Pub. Util. Commission, Comment Letter on Protecting and Promoting the Open Internet (Oct. 14, 2014)) [hereinafter Commissioner Sandoval, *Ex Parte Letter*].

[5] *See* Brief for Professors of Administrative, Communications, Energy, Antitrust, Contract Law, and Policy as *Amici Curiae* Supporting Petitioner at 4, Mozilla, Corp. v. FCC, No. 18-1051 (Aug. 27, 2018) [hereinafter *Amici Brief, Professors of Administrative, Communications, Energy, Contract Law, and Policy*] (citing Nuvio Corp. v. FCC, 473 F.3d 302, 307 (D.C. Cir. 2006)) (discussing the FCC's statutory duty to promote public safety). This amicus brief was prepared and submitted by Professor Catherine J.K. Sandoval, Professor Allen S. Hammond, IV, Professor Anthony Chase, and Dr. Carolyn Byerly, with the assistance of SCU Law student Luke Batty, Professor Sandoval's research assistant. *See also* Catherine Sandoval, Reply Comments, *In the Matter of Restoring Internet Freedom*, WC Docket No. 17-108, at 25, 41, 49, 50 (Aug. 30, 2017) [hereinafter Sandoval, *Reply Comments*] (regarding the public safety role of the open Internet).

[6] *See, e.g.*, Ajit Pai, *The Story of The FCC's Net Neutrality Decision and Why It Won't Stand Up in Court*, 67 FED. COMM. L.J. 147, 189 (2015).

> In the Spectrum Act of 2012, for example, Congress assigned the First Responder Network Authority certain responsibilities, including developing for public safety users a "core network" that "provides connectivity" to "the public Internet or the public switched network, or both." FCC Chairman Pai argues in this article that this "provision makes clear that Congress knows the difference between 'the public switched network' and the 'public Internet.'"

Id. See also id. n.64 (citing Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

Net Neutrality Powers Energy and Forestalls Climate Change,[7] are the two academic articles that put public safety, and the public's role in the use of Internet services, at the center of the net neutrality debate and analysis.

This Article theorizes that an open and neutral Internet improves public safety. Telecommunications theory recognizes that communications networks, whether the telephone system or the Internet, are more valuable when everyone can communicate with everyone.[8] Public safety, like the Internet and telephone networks, rests on a distributed model of universal service that recognizes that society is better off when everyone has access to communications networks. This Article advocates net neutrality regulation that facilitates a "Whole Community" approach to public safety, consistent with Federal Emergency Management Administration's ("FEMA")

2010; Establishment of Rules and Requirements for Priority Access Service, Second Report and Order, 15 FCC Rcd. 16720 (2000)) (finding "Priority Access Service, a wireless priority service for both governmental and non-government public safety personnel, 'prima facie lawful' under section 202"); Bryan N. Tramont & Russell P. Hanser, *Facing Tomorrow's Challenges: Looking Forward, Looking Back*, 16 COMMLAW CONSPECTUS, at i, viii (2007) ("Just like the task of ensuring law enforcement's ability to intercept communications when authorized by warrant, the task of creating a true next-generation public safety network will likely require appropriate government involvement."); Brooke Ericson, "*Möbius-Strip Reasoning": The Evolution of the FCC's Net Neutrality Nondiscrimination Principle for Broadband Internet Services and its Necessary Demise*, 62 ADMIN. L. REV. 1217, 1253 (2010) (analyzing the FCC's 2010 Open Internet Order that crafted net neutrality nondiscrimination principle under Title I of the Communications Act, "subject to reasonable network management and other enumerated exceptions for law enforcement, public safety, and homeland and national security.").

[7] *See* Catherine J.K. Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, 9 SAN DIEGO J. CLIMATE & ENERGY 1, 4, 16–18, 30–31, 33–34, 36–39, 45–48, 53, 56–57, 60–61, 79–81 (2018) [hereinafter Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*]. *See also* Amie Alexander, *Utility Law—All Hands on Deck: Bringing Broadband Home to Rural Arkansas*, 40 U. ARK. LITTLE ROCK L. REV. 401, 409 (2018).

> [T]wenty-two states and the District of Columbia, representing more than half the United States population, have asked a U.S. Appeals Court to reinstate the *2015 Open Internet Order* and strike down the FCC's efforts to preempt states from imposing their own open internet rules. These states contend that the FCC's actions could harm public safety, arguing that the absence of open internet rules jeopardizes the regulation of the electric grid.

Id.

[8] *See* Tex. Alarm & Signal Ass'n v. Pub. Util. Comm'n, 603 S.W.2d 766, 770 (Tex. 1980) (The "universal service objective is founded on the concept that all subscribers to a telephone company's basic service network benefit when another person joins that network. Therefore, the entire network is more valuable because of the addition of the new subscriber."); Pub. Util. Comm'n of Tex. v. AT&T Communications of the Sw., 777 S.W.2d 363, 372–73 (Tex. 1989).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

community-based model for disaster preparation and response.[9] Open and neutral Internet access is critical for disaster preparation and response, overall public safety, and for every member of society in everyday life.

The Internet supports community-enabled public safety, which is improved through information exchange. For example, public sharing of videos of a fire when it first breaks out helps first responders identify the fire's location, risks, and characteristics, and can guide neighbors to evacuation routes. Public use of an open and neutral Internet facilitates the public's role in public safety, and complements the work of government agencies and firms with statutory and regulatory public safety duties. Net neutrality enables people to send and receive information free of ISP interference, enhancing our collective well-being and public safety.

The FCC has a statutory duty to promote public safety.[10] The FCC's enabling act, the Communications Act of 1934, and the Wireless Communication and Public Safety Act of 1999, require the FCC to promote public safety through its regulatory actions.[11] The Amicus Brief for the appeal of the *Internet Freedom Order* to the D.C. Circuit that I authored with Professors Hammond, Byerly, and Chase, and the yeoman's work of my research assistant, SCU Law third-year law student Luke Batty, argued that the "FCC's disregard for the facts, circumstances, and statutory duties that supported its prior [net neutrality] policy violates the APA" and its statutory mission to promote the safety of the American public.[12]

Six months before the FCC adopted the *Internet Freedom Order*, the Supreme Court's June 2017 *Packingham v. North Carolina* decision recognized the Internet's

[9] FED. EMERGENCY MGMT. AGENCY, FDOC 104-00801, WHOLE COMMUNITY APPROACH TO EMERGENCY MANAGEMENT; PRINCIPLES, THEMES, AND PATHWAYS FOR ACTION (2011) [hereinafter FEMA, WHOLE COMMUNITY APPROACH]; Presentation Slide Deck, Pat Lanthier, From Chaos to Synergy via a Whole of Society Approach, Presentation to the Federal-State Joint 706 Conference (Nov. 20, 2014). Thanks to Pat Lanthier for his work and insights into the Whole Community approach to public safety and disaster response that influenced the development of this analysis on the importance of net neutrality to public safety.

[10] Communications Act of 1934, 47 U.S.C. § 151 (2018); Wireless Communication and Public Safety Act of 1999, 47 U.S.C. § 615 (2018); Nuvio Corp. v. FCC, 473 F.3d 302, 307–08 (D.C. Cir. 2006) (discussing the FCC's statutory duty to promote public safety); *see* FCC, STRATEGIC PLAN 2018–2022, at 2 (2018).

[11] Communications Act of 1934, 47 U.S.C. § 151; Wireless Communication and Public Safety Act of 1999, 47 U.S.C. § 615; Nuvio Corp. v. FCC, 473 F.3d 302, 307–08.

[12] *See Amici Brief, Professors of Administrative, Communications, Energy and Contract Law and Policy*, *supra* note 5, at 3–4.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

pivotal role in American society and democracy.[13] "While in the past, there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace—the 'vast democratic forums of the Internet' in general, and social media in particular."[14] *Packingham* recognizes that the Internet facilitates a variety of speech and participation by a multitude of speakers in the modern public square.[15] *Packingham* also recognizes that the Internet facilitates two-way and many-to-many dialogue, not just one-way downloads or information distribution from officials or institutions to "consumers." The FCC's *Internet Freedom Order* failed to address or even mention *Packingham*, despite record comments highlighting the *Packingham* Court's reframing of the role of public Internet access.[16]

The *Internet Freedom Order* also did not analyze the Internet's pivotal role in almost every sector of American life. The *Internet Freedom Order* focuses on the FCC's conclusion that repealing net neutrality rules and the Communications Act Title II (common carrier) classification of ISP services adopted in the *2015 Order* will promote ISP investment incentives.[17] The *Internet Freedom Order* gives short shrift to investments by the range of Internet "edge providers" such as individuals, families, non-profits, businesses, and government including public safety agencies in open and neutral Internet access. The *Internet Freedom Order* concludes without explaining its analysis as the APA requires that "the record does not suggest a correlation between edge provider investment and Title II regulation, nor does it

[13] *See* Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (2017) (citing Reno v. American Civil Liberties Union, 521 U.S. 844, 868 (1997)).

[14] *Id.*

[15] *Id.* at 1737.

[16] *See, e.g.*, John Bergmayer, Public Knowledge, Comment Letter for Notice of *Ex Parte* Presentation in Restoring Internet Freedom 9 (Nov. 3, 2017), https://ecfsapi.fcc.gov/file/110361479428/PK_Aiken_ExParte_11-3.pdf; Electronic Frontier Foundation, Comment Letter on In the Matter of Restoring Internet Freedom 28 (July 17, 2017), https://ecfsapi.fcc.gov/file/10717276427999/Dkt.%2017-108%20EFF%20Comments%20FCC%20NN%202017.07.17.pdf [hereinafter EFF Comments]; Free Press Comment Letter on In the Matter of Restoring Internet Freedom 28 (July 17, 2017), https://ecfsapi.fcc.gov/file/1071818465092/Free%20Press%20Title%20II%20Comments.pdf [hereinafter Free Press Comments]; American Civil Liberties Union, Comments Letter on In the Matter of Restoring Internet Freedom 4 (July 14, 2017), https://ecfsapi.fcc.gov/file/107142322321780/2017-07-14_ACLU_Comments_FCC_Net%20Neutrality.pdf [hereinafter ACLU Comments].

[17] In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311, ¶¶ 86–87 (2018).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

suggest a causal relationship that edge providers have increased their investments as a result of the *Title II Order*."[18]

Santa Clara County's *Internet Freedom ex parte* discussed the County's extensive investments in Internet-based systems to provide two-way and multi-party access to the public to protect public safety, public health, warn crime victims of inmate releases, fight fires, and carry out various functions.[19] "All of these systems could be undermined by a reversal of the Net Neutrality Rules, as could development of additional systems to serve public safety and welfare," Santa Clara County warned.[20]

The FCC's conclusory consideration of the relationship between Title II regulation and edge provider investment dismissed record comments such as those by Santa Clara County, the CPUC, and my comments about the importance of Title II protection to CPUC investment decisions. "As a CPUC Commissioner, the FCC's *2015 Open Internet Decision's* adoption of enforceable Open Internet rules through Title II classification gave my colleagues and me confidence in the rules for regulatory oversight over ISPs," my *Internet Freedom* Reply comments stated.[21] "Enforceable rules that prohibited ISPs from blocking, throttling, or engaging in paid prioritization encouraged our [CPUC] decisions to authorize Internet-enabled investments by energy and water ratepayers."[22] The CPUC's *Internet Freedom* comments emphasized that "a free and open Internet is critical to areas such as energy, education, medicine, and public safety. Given the importance of an open Internet in our society, strong non-discriminatory net neutrality rules are necessary to ensure consumers can enjoy unfettered access to the Internet."[23]

---

[18] *Id.* ¶ 107.

[19] Santa Clara County & Santa Clara County Central Fire Protection District, Comment Letter on Restoring Internet Freedom 6–7, 11–12 (Dec. 6, 2017), https://ecfsapi.fcc.gov/file/1207942320842/2017.12.06%20-%20Comment%20of%20County%20of%20Santa%20Clara%20and%20Santa%20Clara%20County%20Central%20Fire%20Protection%20District.pdf [hereinafter Santa Clara County, *Comment Letter*].

[20] *Id.* at 13.

[21] Sandoval, *Reply Comments*, *supra* note 5, at 51.

[22] *Id.*

[23] Cal. Pub. Util. Comm'n, Comment Letter on In the Matter of Restoring Internet Freedom 7 (July 17, 2017), https://ecfsapi.fcc.gov/file/107172199528427/WC%20Docket%20No.%2017-108%20CPUC%20Comments%20on%20Restoring%20Internet%20Freedom.pdf [hereinafter *CPUC, Comments*].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

The FCC's *Internet Freedom Order* consigns Internet users to limited disclosure and antitrust laws without recognizing that antitrust remedies only harm competition, which leaves public safety harms without remedy.[24] The FCC failed to consider antitrust law's limited remedies that address only harms to competition, despite record comments, including mine, underscoring the remedy limitations of antitrust, unfair competition, and consumer protection laws.[25] Those laws provide no remedy for non-competition harms such as harms to public safety, democracy, energy or water reliability, or critical infrastructure.[26]

This Article concludes that the D.C. Circuit Court of Appeals should vacate the FCC's *Internet Freedom Order* and remand it to the FCC for consideration of public safety and other vital issues the FCC ignored. As this Article was going to press, the D.C. Circuit's *Mozilla v. FCC* decision remanded the *Internet Freedom Order* to require the FCC to analyze the impact of net neutrality repeal proposals on public safety, a remand that requires examination of public safety paradigms and the Internet's role in facilitating bilateral and multilateral communication that empowers public safety.[27]

---

[24] *See* In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311, ¶ 116 (2018) ("To the extent that our approach relying on transparency requirements, consumer protection laws, and antitrust laws does not address all concerns, we find that any remaining unaddressed harms are small relative to the costs of implementing more heavy handed regulation."); *see, e.g.*, Sandoval *Reply Comments*, *supra* note 5, at 45 (emphasizing that antitrust and unfair competition laws remedy only harms to competition); *CPUC, Comments*, *supra* note 23, at 27 (citing *2015 Internet Freedom Order*, *supra* note 4, at 5655) (citing Commissioner Sandoval, *Ex Parte Letter*, *supra* note 4).

[25] Sandoval, *Reply Comments*, *supra* note 5, at n.236 (citing Atl. Richfield Co. v. USA Petroleum Co., 495 U.S. 328, 334 (1990) (holding that antitrust laws were intended to prevent and protect against "antitrust injury," "attributable to an anti-competitive aspect of the practice under scrutiny.")); Reply Brief of Internet Association et al., in Support of Petitioners at 12, Mozilla v. FCC, No. 18-1051 (D.C. Cir. 2018) (citing *Amici Brief, Professors of Administrative, Communications, Energy and Contract Law and Policy*, *supra* note 5, at 7–8) ("Consequently, antitrust laws are ill-suited to address harms to consumers, free speech, investment, and innovation in the net neutrality context.").

[26] *See Atl. Richfield Co.*, 495 U.S. at 334 ("antitrust injury" claims and remedies are limited anti-competitive injury); Sandoval, *Reply Comments*, *supra* note 5, at 45.

[27] *Mozilla*, ___ F.3d at 100; *see* Christine B. Williams, Jane Fedorowicz, Andrea Kavanaugh, Kevin Mentzer, Jason Bennett Thatcher & Jennifer Xu, *Leveraging Social Media to Achieve A Community Policing Agenda*, 35 GOV'T INFO. Q. 210, 210 (2018) (analyzing "communication behavior and engagement strategies in the bilateral use of social media between law enforcement agencies and the communities they serve.").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

B. Article Organization

This Article reframes the public safety paradigm embedded in Internet regulation to focus on public use of the open Internet; not only commercial and institutional public safety uses. Section II provides a brief overview of key threads in the debate over Internet regulation in the United States, starting with the Computer Inquiries that began in 1966. Much of the net neutrality litigation and debate has centered on regulatory classification of ISPs and its consequences for FCC jurisdiction.[28] The purpose of this Section is not to review these issues in an encyclopedic fashion, but to unmask themes relevant to public safety such as the function of ISPs as gatekeepers in the Internet ecosystem, enabled by technological increases in capacity and regulatory permission. This Section analyzes the relationship between the Internet's technological and social evolution and the construction of regulatory paradigms that govern ISP conduct.

Section III argues that the FCC frames its view of public Internet use through a "Cat Video paradigm" that assumes the public is not distributing or accessing material important to public safety and well-being. The FCC's limited public safety frame focuses on government and commercial Internet use and the role of institutional actors in public safety. This section examines the "Whole Community" approach to public safety reflected in FEMA's disaster preparedness and response paradigm. The Whole Community model emphasizes the legal, moral, and practical imperative of including everyone in disaster preparation and response. Recognizing the needs and abilities of all community members and vulnerable communities protects public safety and improves our collective well-being. As scientists warn that climate change makes flooding, hurricanes, and wildfires more intense,[29] Whole Community preparation and response is imperative. This Section argues for

[28] *See, e.g.*, Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 975 (2005) ("At issue in these cases is the proper regulatory classification under the Communications Act of broadband cable Internet service."); Verizon v. FCC, 740 F.3d 623, 650–51 (D.C. Cir. 2014) ("Thus, we must determine whether the requirements imposed by the Open Internet Order subject broadband providers to common carrier treatment. If they do, then given the manner in which the Commission has chosen to classify broadband providers [as information service providers under Title I], the regulations cannot stand."); U.S. Telecom Ass'n v. FCC, 825 F.3d 674, 713 (D.C. Cir. 2016) ("Although Verizon does recognize that broadband providers' delivery of broadband to end users also provides a service to edge providers, *id.*, it does not hold that the Commission must classify broadband as a telecommunications service in both directions before it can regulate the interconnection arrangements under Title II. The problem in Verizon was not that the Commission had misclassified the service between carriers and edge providers but that the Commission had failed to classify broadband service as a Title II service at all. The Commission overcame this problem in the Order by reclassifying broadband service—and the interconnection arrangements necessary to provide it—as a telecommunications service.").

[29] U.S. GLOBAL CHANGE RESEARCH PROGRAM, FOURTH NATIONAL CLIMATE ASSESSMENT (2017).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

recognition of the public's role in public safety, empowered by the open Internet, in the analysis and development of Internet regulation.

Section IV argues that the FCC's failure to address public safety in its *2018 Internet Freedom Order* violates the FCC's statutory mission and the APA. It examines the FCC's failure to consider the *Internet Freedom* docket's record that highlighted the ways in which government agencies rely on public access to mass-market Internet services to carry out public safety duties. It analyzes the FCC's failure to discuss the record evidence of public safety risks from net neutrality repeal to critical infrastructure, energy, and water management. It examines the oral arguments in the *Mozilla v. FCC* appeal of the *Internet Freedom Order*, unmasking the FCC's institutional-focused public safety frame, which obscures the public's role in public safety. It also analyzes the FCC's distortions of the record at the oral argument, such as the FCC lawyer's statement that to mitigate paid priority's effects, "[t]here would be network management tools. . . . For example if congestion would otherwise result there would be for latency, for applications that don't require a lot of latency sensitivity, such as you're getting an email that you get 10 milliseconds late or something like that, that is the traffic that would be deprioritized in a way to make this service work."[30] The *Internet Freedom Order* makes no finding that emails or any other Internet content would only arrive 10 milliseconds later if paid priority were allowed. The APA allows a court to uphold agency action only based on rationale articulated when the agency made the decision.[31] These omissions violate the FCC's statutory mission and the APA.

Section V recommends that the D.C. Circuit vacate and remand the FCC's *Internet Freedom Order* in light of the FCC's failure to address issues in its record or to justify its reversal. The D.C. Circuit's February 2019 decision in *National Lifeline Ass'n v. FCC* vacated and remanded the FCC's decision in the tribal Lifeline program for failure to address the relevant record or proffer justifications for departing from its previous decisions.[32] To carry out its statutory mission to promote public safety, the FCC must reframe its public safety paradigm to put the public at the center of public safety. Distributed public safety tools and roles protect the community in an era faced by restrained government resources and growing frequency and range of public safety risks. Upon remand of the *Internet Freedom*

[30] Oral Argument, Mozilla Corp. v. FCC, Case No. 18-1051 (2018) [hereinafter Mozilla v. FCC Oral Argument], at 3:29:50–3:30:35.

[31] Michigan v. EPA, 135 S. Ct. 2699, 2710 (2015) (stating "a court may uphold agency action only on the grounds that the agency invoked when it took the action") (citing SEC v. Chenery Corp., 318 U.S. 80, 87 (1943)); *see* Perez v. Mortg. Bankers Ass'n, 35 S. Ct. 1199, 1209 (2015) (quoting Fox TV Stations, Inc. v. FCC, 556 U.S. 502, 515 (2009)).

[32] Nat'l Lifeline Ass'n v. FCC, 915 F.3d 19, 22–23 (D.C. Cir. 2019).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

Order, commenters and the FCC must put the public at the center of public safety, and recognize the role of an open and neutral Internet in safeguarding our collective public safety, well-being, economy, and sustainability.

II. REGULATORY FRAMES OF PUBLIC SAFETY USES OF THE INTERNET

A. Public Safety Conceptualizations in the Net Neutrality Debate

This Section provides a brief overview of the evolution of public safety uses of the Internet as seen through landmark FCC cases and proceedings reviewing Internet regulation. This overview is not intended as an exegesis of the FCC's more than half-century record of reviewing telecommunications and information services. This Section highlights the relationship between the technical evolution of communications, computer, and Internet services and conceptualizations of the role of public safety in Internet regulation.

B. The "Computer Inquiries," From the Computer as Boundary Object to Computer Processing as a Boundary Function

Professor Roberta Lentz observed that the FCC's "Computer Inquiries" began under the Nixon Administration in 1966 and continued through the administrations of Presidents Carter and Reagan.[33] Through the Computer Inquiries, the FCC crafted a distinction between "basic" and "enhanced" services.[34] Three decades later, Congress adopted this regulatory classification framework in the Telecom Act of 1996, codifying the distinction between common carrier and information services

[33] Roberta Lentz, *Regulation as Linguistic Engineering*, *in* HANDBOOK OF GLOBAL MEDIA AND COMMUNICATIONS POLICY 432, 435, 439 (Robin Mansell & Marc Raboy eds., 2011).

[34] *See, e.g.*, Notice of Inquiry & Proposed Rulemaking, In the Matter of Regulatory & Policy Problems Presented by the Interdependence of Computer & Commc'n Servs. & Facilities, 7 F.C.C.2d 11 (1966); In the Matter of Regulatory & Policy Problems Presented by the Interdependence of Computer & Commc'n Servs. & Facilities, 28 F.C.C.2d 267 (1971) (Final Decision and Order); Notice of Inquiry & Proposed Rulemaking, In the Matter of Amendment of Section 64.702 of the Commission's Rules & Regulations, 61 F.C.C.2d 103 (1976); In the Matter of Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry), 77 F.C.C.2d 384, 386 (1980) (Final Decision); In the Matter of Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry), FCC 84-190 (1984) (Memorandum Opinion and Order); In the Matter of Amendment of Sections 64.702 of the Commission's Rules & Regulations (Third Computer Inquiry), 4 FCC Rcd. 5927 (1989) (Memorandum Opinion and Order on Further Reconsideration and Second Further Reconsideration).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

that drives the regulatory classification issues in the net neutrality debate.[35] The FCC launched the Computer Inquiries in 1966 "as the telecommunication environment shifted from one in which large centralized computers transmitted data to 'dumb' terminals at remote locations, to one in which computing capacity became embedded in devices at either end of the transmission path, as well as in the network itself."[36] Lentz observed that the Computer Inquiries "were also engaged in the evolution of the computing industry as well as the early stages of the Internet."[37]

The 1966 initiation of the Computer Inquiries preceded ARPANET's launch in 1969, the forerunner to the modern Internet. ARPANET's distributed architecture promoted resiliency.[38] ARPANET "was designed to enable computers operated by the military, defense contractors, and universities conducting defense-related research to communicate with one another by redundant channels even if some portions of the network were damaged in a war."[39] The Court in *Reno v. American Civil Liberties Union* observed that ARPANET "provided an example for the development of a number of civilian networks that, eventually linking with each other, now enable tens of millions of people to communicate with one another and to access vast amounts of information from around the world."[40]

Concomitant with the Computer Inquiries, the FCC's 1968 Carterfone decision recognized users' right to attach devices to the telephone network as long as they did not harm the network.[41] As the Computer Inquires progressed from *Computer I* to *Computer II*, the FCC in 1975 adopted standards through the "Part 68" proceeding that allowed devices such as computer modems to interconnect to the telephone network.[42] The Part 68 proceeding stated: "[e]quipment containing the appropriate FCC registered protective circuitry, or FCC registered terminal equipment, may,

[35] Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified at 47 U.S.C. §§ 157, 230(b) (2006)).

[36] Lentz, *supra* note 33, at 436.

[37] *Id.*

[38] *See* Reno v. American Civil Liberties Union, 521 U.S. 844, 849–50 (1997).

[39] *See id.*

[40] *Id.*

[41] In the Matter of Use of the Carterfone Device in Message Toll Telephone Service, 13 F.C.C.2d 420, 423–26, *recons. denied*, 14 F.C.C.2d 571, 575 (1968).

[42] In the Matter of Proposals for New or Revised Classes of Interstate & Foreign Message Toll Tel. Serv. (MTS) & Wide Area Tel. Serv. (WATS), 56 F.C.C.2d 593, 597–99 (1975).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

following the effective date of this Order, be connected directly with the telephone network pursuant to the procedures set forth in these rules, without benefit of carrier-supplied connecting arrangements."[43]

The Part 68 standards "were designed to promote access to a dominant telephone system governed by common-carrier regulation."[44] Professor Kevin Werbach observed that freedom to connect modems and run Internet applications would not be possible without the Part 68 rules.[45] Carterfone and the Part 68 proceedings were crucial to the Internet's development as they allowed users to access the Internet through telephone networks already built in their neighborhoods under common carrier regulation and universal service policies.

"The FCC in 1980, through its Computer II proceeding, affirmed that facilities-based telecommunications providers would continue to be subject to common-carrier obligations for the data traffic passing through their network."[46] "Common carriage regulations forbade discrimination by the voice network against traffic passing through the telephone network, including nascent Internet traffic."[47]

The Court in *NCTA v. Brand X Internet Services* recounted the role of the Computer Inquiries in the Internet's development. As the telephone network evolved and telephone companies offered Internet access through digital subscriber lines (DSL), the FCC also required the telephone companies "to make the telephone lines used to transmit DSL service available to competing ISPs on nondiscriminatory, common-carrier terms."[48] The *Brand X* Court observed that through the *Computer II* rules, the FCC "subjected facilities-based providers to common-carrier duties not because of the nature of the 'offering' made by those carriers, but rather because of

[43] *Id.* at 599.

[44] Catherine T.K. Sandoval, *Disclosure, Deception, and Deep-Packet Inspection: The Role of the Federal Trade Commission Act's Deceptive Conduct Prohibitions in the Net Neutrality Debate*, 78 FORDHAM L. REV. 641 n.419 (2009) [hereinafter Sandoval, *Disclosure, Deception, and Deep-Packet Inspection*].

[45] Kevin Werbach, *The Federal Computer Commission*, 84 N.C. L. REV. 1, 21 (2005).

[46] Sandoval, *Disclosure, Deception, and Deep-Packet Inspection*, *supra* note 44, at 652 (citing In the Matter of Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry), 77 F.C.C.2d 384, 417–23 (1980)).

[47] *Id.*; Nat'l Cable & Telecomm. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 1000–01 (2005).

[48] *Brand X*, 545 U.S. at 1000.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

the concern that local telephone companies would abuse the monopoly power they possessed by virtue of the 'bottleneck' local telephone facilities they owned."[49]

Lentz analyzes the Computer Inquiries as an example of "linguistic engineering," which she characterizes as a "form of information infrastructure."[50] Lentz observes the FCC's 1971 final decision in "Computer I," the first set of Computer Inquiries, deemed the computer to be the "boundary object" between regulated and unregulated services.[51] The FCC determined which side of the regulatory boundary the service fell on by examining whether computing was "incidental to" the communication or the data processing aspect of a service deemed to be in that category.[52] Lentz observes that by 1979 in the Second Computer Inquiry, the FCC shifted the boundary from the computer to "computer processing."[53] The FCC's "definitional changes" in the Computer Inquiries, Lentz argues, illustrate "the malleability of regulatory categories in the service of specific policy goals."[54]

Professor Susan P. Crawford described the creation of categorical and regulatory distinctions for computing services and common carriage communications as "designed to protect the computing industry from the depredations of the carriers."[55] She describes these distinctions as "premised on the continued existence of basic, general-purpose, non-discriminatory access and transport."[56]

The distinctions developed in the Computer Inquiries became the basis for the "common carrier" and "information service provider" classifications codified in the Telecommunications Act of 1996 ('96 Act).[57] "Common-carrier regulations fostered competition for independent ISPs, and prohibited those who controlled access to the

[49] *Id.* at 996.

[50] Lentz, *supra* note 33, at 443.

[51] *Id.* at 439.

[52] *Id.* at 440.

[53] *Id.* at 441.

[54] *Id.* at 437.

[55] Susan P. Crawford, *Transporting Communications*, 89 B.U. L. REV. 871, 887, 891–98 (2009) (The FCC's Computer Inquiries required common carriage to constrain telephone company conduct that might restrict the computer marketplace.).

[56] *Id.*

[57] Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified at 47 U.S.C. §§ 157, 230(b) (2006)).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

Internet's physical layer from discriminating against nascent Internet content or applications."[58] "In its 1986 Computer III order, the FCC required local telephone companies that provided enhanced services to offer their wires on a common-carrier basis to competing enhanced-service providers."[59] This order effectively mandated telephone companies to make their lines available to competing ISPs on "nondiscriminatory, common-carrier terms."[60]

C. The Telecommunications Act of 1996, Codifying Common Carrier and Information Services and Requiring Steps to Promote Internet Access and Deployment

As explained in *U.S. Telecom Ass'n v. FCC*, which upheld the FCC's *2015 Order*, Congress:

> Borrowing heavily from the Computer II framework, enacted the Telecommunications Act of 1996, which amended the Communications Act. The Telecommunications Act subjects a "telecommunications service," the successor to basic service, to common carrier regulation under Title II.[61] In contrast, an "information service," the successor to an enhanced service, is not subject to Title II. The Telecommunications Act defines a "telecommunications service" as the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.[62]

The 1996 Act defines telecommunications as "the transmission, between or among points specified by the user, of information of the user's choosing without change in the form or content of the information as sent and received."[63] "An information service is an 'offering of a capability for generating, acquiring, storing, transforming,

[58] Sandoval, *Disclosure, Deception, and Deep-Packet Inspection*, *supra* note 44, at 653.

[59] *Id.* at 652 (citing Nat'l Cable & Telecomm. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 995 (citing In the Matter of Amendments of Sections 64.702 of the Commission's Rules and Regulations (Third Computer Inquiry), 104 F.C.C.2d 958, 964 (1986))).

[60] *Id.*

[61] U.S. Telecom Ass'n v. FCC, 825 F.3d 674, 691 (D.C. Cir. 2016) (citing 47 U.S.C. § 153).

[62] *Id.* (citing 47 U.S.C. § 153(53)).

[63] *Id.* (citing 47 U.S.C. § 153(50)).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

processing, retrieving, utilizing, or making available information via telecommunications.'"[64]

In 1997, the Supreme Court in *Reno v. American Civil Liberties Union* described the Internet as a vast forum accessed through "hosts" or "entities with a host affiliation."[65] "Hosts" included colleges or universities, some businesses, local libraries, and "computer coffee shops" that provided Internet access for a fee.[66] At the time of the 1996 trial at issue in *Reno*, proprietary networks that linked to the Internet "America Online, CompuServe, the Microsoft Network, and Prodigy . . . had almost 12 million individual subscribers."[67] The Court described the primary communications and retrieval methods for the Internet at that time as "electronic mail ('e-mail'), automatic mailing list services ('mail exploders,' sometimes referred to as 'listservs'), 'newsgroups,' 'chat rooms,' and the 'World Wide Web.'"[68] "All of these methods," which the *Reno* Court characterized as part of "the vast democratic forums of the Internet,"[69] could then be "used to transmit text; most can transmit sound, pictures, and moving video images."[70] As described by the Court "[t]aken together, these tools constitute a unique medium—known to its users as 'cyberspace'—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet."[71]

The regulations stemming from the Computer Inquiries, and the FCC's Carterfone and Part 68 decisions, led to a proliferation of independent ISPs that competed to offer dial-up Internet service through telephone facilities.[72] "In 1999 over 6000 ISPs offered dial-up service to the Internet and 95% of Americans had access to four local ISPs," Jason Oxman reported for the FCC Office of Plans and Policy.[73] Common-carrier regulations fostered competition for independent ISPs,

[64] *Id.* (citing 47 U.S.C. § 153(24)).

[65] Reno v. American Civil Liberties Union, 521 U.S. 844, 850 (1997).

[66] *Id.*

[67] *Id.* at 850–51.

[68] *Id.* at 851.

[69] *Id.* at 868.

[70] *Id.* at 851.

[71] *Id.*

[72] Jason Oxman, *The FCC and the Unregulation of the Internet* 3, 14, 16 (FCC Office of Plans & Policy, Working Paper No. 31, 1999).

[73] *Id.* at 17.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

and prohibited those who controlled access to the Internet's physical layer from discriminating against nascent Internet content or applications.

D. *The Four Principles of Internet Freedom and* NCTA v. Brand X *at the Dawn of the Social Media Age*

The FCC's *2018 Internet Freedom Order* extols the virtues of the unenforceable four principles of Internet Openness announced on February 8, 2004 by then FCC Chairman Powell.[74] These four principles were suggested as voluntary guidance for ISPs:

> *Freedom to Access Content*. First, consumers should have access to their choice of legal content.
>
> *Freedom to Use Applications*. Second, consumers should be able to run applications of their choice.
>
> *Freedom to Attach Personal Devices*. Third, consumers should be permitted to attach any devices they choose to the connection in their homes.
>
> *Freedom to Obtain Service Plan Information*. Fourth, consumers should receive meaningful information regarding their service plans.[75]

Chairman Powell urged "consumers to challenge their broadband providers to live up to these standards and to let the Commission know how the industry is doing."[76] In 2005, the Commission unanimously approved the *Internet Policy Statement*, which adopted four voluntary principles designed "to encourage broadband deployment" and "preserve and promote the open and interconnected nature of the Internet."[77]

When Chairman Powell gave his speech encouraging Internet providers to adopt four voluntary principles to ensure Internet Freedom, the Internet's characteristics were very different than they were nearly fourteen years later when the FCC repealed net neutrality rules in 2018. *TIME* ranked the camera phone as one

---

[74] In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311, 315, 351, 434 (2018) (citing Michael K. Powell, Chairman, Fed. Commc'n Comm'n, The Digital Broadband Migration: Toward a Regulatory Regime for the Internet Age, Speech at the University of Colorado Law Symposium (Feb. 8, 2004) [hereinafter *Powell Speech*]).

[75] *Powell Speech*, *supra* note 74, at 5.

[76] *Id.* at 6.

[77] In the Matters of Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, 20 FCC Rcd. 14986, 14988 (2005).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

of the top inventions of 2003 at a time when flip phones still reigned among those who had cell phones.[78] One megapixel camera phones took grainy pictures in early 2004.[79] It was not until July 2004 that Sprint released a camera that could share pictures wirelessly.[80] "Facebook launched in February 2004, the same month that then FCC Chairman Powell announced his voluntary Internet Freedom principles."[81] *Merriam-Webster* named "Blog" the word of the year in 2004.[82]

In 2004, the FCC defined advanced Internet services as those providing Internet connections at speeds exceeding 200 kbps in both directions.[83] Subscribership to 200 kbps symmetrical "advanced services increased from 5.9 million lines in June 2001 to 20.3 million lines in December 2003."[84] The FCC defined "high-speed lines" as those providing 200 kbps in at least one direction, subscribership to which almost tripled from June 2001 to December 2003, "from 9.6 million lines to 28.2 million lines."[85] This speed level would not run many modern Internet applications popular in 2019 including mapping, GIS-based services, and streaming video.[86]

In *United States v. American Library Assn.*, the Supreme Court in 2003 recalled Congress' vision of the Internet in 1999 as "simply another method for making information available in a school or library," "no more than a technological extension of the book stack."[87] This characterization of the Internet was inaccurate. Even in the

---

[78] *See* Anita Hamilton, *Camera Phones, Best Inventions of 2003*, TIME (Nov. 16, 2003), http://content.time.com/time/specials/packages/article/0,28804,1935038_1935082_1935257,00.html.

[79] Jordan Minor, *A Look Back at the Technology from 10 Years Ago*, PASTE MAG. (Dec. 11, 2014), https://www.pastemagazine.com/articles/2014/12/tech-from-10-years-ago-blogging-bluetooth-and-the.html.

[80] *See* Simon Hill, *From J-Phone to Lumia 1020, A Complete History of the Camera Phone*, DIGITAL TRENDS (Aug. 11, 2013), https://www.digitaltrends.com/mobile/camera-phone-history/.

[81] Mark Hall, *Facebook*, ENCYCLOPEDIA BRITANNICA (Feb. 7, 2019), https://www.britannica.com/topic/Facebook.

[82] *Word of the Year Retrospective, The Way We Word*, MERRIAM WEBSTER, https://www.merriam-webster.com/words-at-play/2014-word-of-the-year-retrospective/2004-blog (last visited Apr. 9, 2019).

[83] FED. COMMC'N COMM'N, FOURTH BROADBAND PROGRESS REPORT (2004).

[84] *Id.*

[85] *Id.*

[86] *See* In the Matter of AT&T Mobility, LLC, 30 FCC Rcd. 6613, 6616 (2015) (noting that slow speeds AT&T imposed on consumers who used "too much" of their "unlimited" service would not run many popular applications including mapping, teleconferencing, and streaming video).

[87] United States v. Am. Library Ass'n, 539 U.S. 194, 207 (2003).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

dial-up days of 1999, the Internet was much more than a book stack, a means for accessing information published by others. The Internet enabled new means of communication, new industries, and created new opportunities. Internet use grew after the World Wide Web's public release in 1991 and Google's launch in 1998.

In 2005, when the Supreme Court in *NCTA v. Brand X Internet Services* upheld the FCC's decision to classify cable modem Internet as an information service, Americans predominantly accessed the Internet through dial-up connections via local telephone facilities.[88] *Brand X* observed that at the time the case was decided, the "traditional means by which consumers in the United States access the network of interconnected computers that make up the Internet is through 'dial-up' connections provided over local telephone facilities."[89] Cable Modem and telephone-based Digital Subscriber Line ("DSL") service provided "Broadband" Internet that transmitted data at higher speeds.[90] As of 2008, the FCC still defined "high-speed Internet lines" as those providing over 200 kbps in one direction.[91]

E. Comcast Corp. v. FCC*; Judicial Limits to Regulating by Unenforceable Principles as ISP Technical Capacity Grows, 2007 to 2010*

In 2007, several Comcast customers complained to the FCC that Comcast interfered with their ability to access certain applications, including peer to peer ("P2P") Internet protocols.[92] After an investigation, Comcast agreed to change its network management policies and disclose "the details of its new approach and the company's progress toward implementing it."[93] The FCC warned of enforcement

[88] Nat'l Cable & Telecomm. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 974–75 (2005).

[89] *Id.* (citing Brand X Internet Servs. v. FCC, 345 F.3d 1120, 1123–24 (9th Cir. 2003); In the Matter of Inquiry Concerning High–Speed Access to the Internet Over Cable and Other Facilities, 17 FCC Rcd. 4798, 4802–03 (2002)).

[90] *Brand X*, 545 U.S. at 975.

[91] FED. COMMC'N COMM'N, FIFTH BROADBAND PROGRESS REPORT, app. B at 2 (2008).

[92] *See* In the Matter of Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications, 23 FCC Rcd. 13,028, 13,030–32 (2008) (concluding that Comcast's interference with P2P and other applications did not constitute reasonable network management). Free Press sought, among other remedies, a permanent injunction because such a remedy would redress society's "loss of unpredictable innovation" and would "encourage innovation in Internet applications and content, as well [as] promot[e] the deployment and uptake of high-speed Internet access." Formal Complaint of Free Press and Public Knowledge against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications, File No. EB-08-IH-1518 (Nov. 1, 2007).

[93] In the Matter of Formal Complaint of Free Press and Public Knowledge, 23 FCC Rcd. at 13,060.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

action if Comcast did not timely submit the disclosures required by its Order closing the investigation into these complaints.[94]

The D.C. Circuit, in 2010 in *Comcast Corp. v. FCC*, rejected the FCC's 2008 decision on the grounds that it had not established the jurisdictional basis for such regulatory action that effectively imposed common carrier regulations on Internet-based services.[95] Comcast observed that the FCC's Order relied on "section 4(i) of the Communications Act of 1934," which authorizes the FCC to exercise ancillary jurisdiction to "perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions."[96] The D.C. Circuit held that the FCC can exercise that authority "only if it demonstrates that its action—here barring Comcast from interfering with its customers' use of peer-to-peer networking applications—is 'reasonably ancillary to the . . . effective performance of its statutorily mandated responsibilities.'"[97] The D.C. Circuit determined that the FCC failed to make that showing to support its Comcast decision. Nor could it rely on policy statements such as that adopted in 2005 incorporating the Internet Freedom principles.[98]

When the FCC adopted the 2008 Comcast Order in response to the Free Press complaint, it had not yet conducted a proceeding to analyze whether to adopt rules limiting ISPs to "reasonable network management," or other net neutrality principles. Neither had the FCC squarely addressed the jurisdictional basis for the consideration of any such rules.

The FCC's 2008 *Comcast Order* is an important marker that recognizes the Internet's evolution to include more services involving one-to-many sharing, and increased video use.[99] The FCC's *Comcast* decision observed that Bit Torrent, which used the P2P protocol Comcast allegedly slowed, "harnesses the numerous individual Internet connections maintained by its users, rather than relying on a single, central pipeline, to distribute large files 'cheaply and quickly.'"[100] The FCC

[94] *Id.*

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

[96] *Id.* at 644 (citing 47 U.S.C § 154(i)).

[97] *Id.* (citing Am. Library Ass'n v. FCC, 406 F.3d 689, 692 (D.C. Cir. 2005)).

[98] *Id.*

[99] In the Matter of Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications, 23 FCC Rcd. 13,028, 13,0329–30 (2008).

[100] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

found that P2P network efficiency depends on Internet users' ability to establish TCP connections for both downloading and uploading content.[101]

Uploads were increasing as more people had tools to share content they created, in addition to accessing or receiving content and applications.[102] The FCC observed that "BitTorrent and other peer-to-peer technologies, such as Gnutella, have entered the mainstream. New online content distributors, such as Vuze, Inc., rely on BitTorrent to distribute video programming to millions of online viewers legally, as do several established distributors such as CBS, Twentieth Century Fox, and Sports Illustrated."[103]

The Comcast Order recognized the increasing technical ability of ISPs to limit or interfere with certain types of Internet traffic.[104] While scholars had earlier debated about ISP technical capability and financial incentives to favor certain traffic at the expense of others, the Comcast case highlighted ISPs' technical ability to slow or limit certain types of traffic, and their incentives to do so.[105]

The FCC found that Comcast "deployed equipment across its networks that monitors its customers' TCP connections using deep packet inspection to determine how many connections are peer-to-peer uploads. When Comcast judges that there are too many peer-to-peer uploads in a given area, Comcast's equipment terminates

---

[101] *Id.* at 13,030.

[102] *See id.* at 13,029.

[103] *Id.* at 13,030.

[104] *Id.* at 13,078 (Commissioner Michael J. Copps noting that "broadband providers amassed the power and technical ability to dictate where we can go and what we can do on the internet.").

[105] Sandoval, *Disclosure, Deception, and Deep-Packet Inspection*, *supra* note 44, at 648 (citing Joseph Farrell & Philip J. Weiser, *Modularity, Vertical Integration, and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age*, 17 HARV. J.L. & TECH. 85, 101 (2003) (identifying incentives to undermine an application that can compete with the ISP's core platform as an exception to the principle that ISPs will tend to "internalize complementary efficiencies"); Brett Frischmann & Barbara van Schewick, *Network Neutrality and the Economics of an Information Superhighway: A Reply to Professor Yoo*, 47 JURIMETRICS J. 383, 411 (2007) (arguing that limited competition and incentives to keep secondary market revenues create incentives for ISPs to discriminate); James B. Speta, *Handicapping the Race for the Last Mile?: A Critique of Open Access Rules for Broadband Platforms*, 17 YALE J. REG. 39, 84 (2000) (asserting that where network effects are strong as in the broadband market, "even a monopolist will have the incentive to encourage a wide variety of information services in order to increase subscribership."); Christopher S. Yoo, *Network Neutrality and the Economics of Congestion*, 94 GEO. L.J. 1847, 1888 (2006) (contending that network owners have an incentive to support complementary innovation that would increase the value of their networks).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

some of those connections by sending RST packets."[106] RST, or "reset" packets, "will generally cause ordinary networking software to close its side of the connection in response."[107] Through reset messages, "[e]ach PC gets a message invisible to the user that looks like it comes from the other computer, telling it to stop communicating. But neither message originated from the other computer—it comes from Comcast."[108] "In response to the FCC's order to reveal Comcast's network management practices, Comcast revealed in September 2008 that it used Sandvine to examine the headers of TCP/IP packets to distinguish whether traffic is VoIP, P2P, or e-mail."[109]

The FCC emphasized that Comcast determines "how it will route some connections based not on their destinations but on their contents; in laymen's terms, Comcast opens its customers' mail because it wants to deliver mail not based on the address or type of stamp on the envelope but on the type of letter contained therein."[110] The FCC expressed its concern about use of this technique as "Comcast's method, sending RST packets to both sides of a TCP connection, is the same method computers connected via TCP use to communicate with each other, a customer has no way of knowing when Comcast (rather than its peer) terminates a connection."[111]

The Comcast case reflects both regulatory and technical shifts after the Supreme Court's 2005 decision in *NCTA v. Brand X Internet Services* upheld the FCC's classification of cable-modem-based Internet as an Information Service Provider and not a common carrier.[112] Following that decision, the FCC also relieved ISPs who used DSL or telephone-based technologies from common-carrier

---

[106] In the Matter of Formal Complaint of Free Press and Public Knowledge, 23 FCC Rcd. at 13,050–51.

[107] *Id.* at 13,029 n.3 (citing Electronic Frontier Foundation Reply Comments, attach. at 1 ("When received, RST packets will generally cause ordinary networking software to close its side of the connection in response.")).

[108] Sandoval, *Disclosure, Deception, and Deep-Packet Inspection*, *supra* note 44, at 674 n.199 (citing Associated Press, *How the AP Tested Comcast's File-Sharing Filter*, SAN JOSE MERCURY NEWS (Oct. 19, 2007), https://www.mercurynews.com/2007/10/19/how-the-ap-tested-comcasts-file-sharing-filter/, http://www.newsvine.com/_news/2007/10/19/1035713-ap-tests-comcasts-file-sharing-filter); Peter Svensson, *Comcast Blocks Some Internet Traffic*, ASSOCIATED PRESS (Oct. 19, 2007), http://.nbcnews.com/id/21376597/ns/technology_and_science-internet/t/comcast-blocks-some-internet-traffic/.

[109] Sandoval, *Disclosure, Deception, and Deep-Packet Inspection*, *supra* note 44, at 673 n.197 (citing Letter from Comcast to the FCC, 7 (Sept. 25, 2008)).

[110] In the Matter of Formal Complaint of Free Press and Public Knowledge, 23 FCC Rcd. at 13,051.

[111] *Id.*

[112] Nat'l Cable & Telecomm. Ass'n v. Brand X Internet Services, 545 U.S. 967, 975 (2005).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

obligations.[113] My Article, *Disclosure, Deception, and Deep-Packet Inspection: The Role of the Federal Trade Commission Act's Deceptive Conduct Prohibitions in the Net Neutrality Debate*, argued that since *Brand X*, "ISPs have used both technology and contract to constrain subscriber use of Internet applications."[114] "Deep-packet inspection software examines Internet packets attempting to pass through an ISP network and allows the ISP to 'distinguish peer-to-peer traffic [or any other Internet application they choose to track] . . . and either block it or reduce its available bandwidth.'"[115] Using deep-packet inspection, ISPs have the technical power to cut off Internet applications "with a mere flick of the switch."[116]

The technical and social shift to more widespread Internet content creation and distribution challenges Internet Network designs that dedicate a small percentage of Internet bandwidth to uploads. At the time of the Comcast decision, ISP network bandwidth was "divided to provide more capacity for downstream uses (downloading) than upstream uses (sending). That network design reified the paradigm of Internet users as content consumers, rather than content creators or people who share content."[117] Comcast's "network design contributed to network congestion as Internet applications evolved to facilitate more user-generated data, as well as browsing, downloading, and uploading larger data files."[118]

The Comcast complaint was submitted in 2007, as social media platforms were beginning to proliferate, allowing more uploading and content sharing. Twitter was founded in March 2006, initially as an SMS platform.[119] The 140-character limit was tailored to SMS texting protocol.[120] As Twitter use grew, its servers occasionally

---

[113] *See id.* at 1000.

[114] Sandoval, *Disclosure, Deception, and Deep-Packet Inspection*, *supra* note 44, at 646.

[115] *Id.* (citing PeerApp, PEERAPP WHITE PAPER: ACCELERATING THE VIDEO INTERNET 6 (2008) (stating ISPs use deep-packet inspection products to "sort out what applications are running over their networks, so ISPs can fully understand the traffic demands of each application, and then manage or 'shape' the traffic accordingly").

[116] *Id.* (citing Turner Broad. Sys. v. FCC, 512 U.S. 622, 656 (1994) (upholding regulations that require cable companies to carry the signals of over-the-air broadcasters to preserve competition in light of cable's bottleneck control that enables them to exclude broadcasters)).

[117] *Id.* at 672.

[118] Sandoval, *Disclosure, Deception, and Deep-Packet Inspection*, *supra* note 44, at 672.

[119] Amanda McArthur, *The Real History of Twitter, In Brief*, LIFEWIRE (Nov. 2, 2018), https://www.lifewire.com/history-of-twitter-3288854.

[120] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

became overloaded.[121] Several years later in 2011 Twitter allowed users to share photos through its platform, increasing network resource demand.[122] Twitter video sharing would not begin until 2012, followed by six-second looping videos in 2013.[123]

YouTube was founded in 2005 and sold to Google in 2006.[124] In 2007, YouTube utilized large amounts of bandwidth and would continue to do so for several years.[125] Netflix was launched as a video rental service in 1997, primarily using the U.S. mail to distribute videos.[126] In 2007, Netflix launched streaming videos through subscription service.[127] Sandvine estimated that by 2016, Netflix was "responsible for 35.2% of all peak-time fixed broadband traffic [in North America], with YouTube claiming another 17.5%."[128] ISP network management techniques to address the changing nature and volume of consumer Internet use were at the heart of the Comcast case.

The FCC's definition of high-speed Internet as of 2018 is still calibrated to an asymmetrical connection that provides more upload than download speed.[129] P2P,

---

[121] *Id.*

[122] Benn Parr, *Twitter Rolls Out Photo Sharing to All Users*, MASHABLE (Aug. 9, 2011), https://mashable.com/2011/08/09/twitter-photo-sharing-all/#h2SPD_GrySqA.

[123] *The Evolution of Twitter Since the Dawn of the First Tweet*, INTERACTIVESCHOOLS.COM: THE CREATIVE UX AGENCY (Sept. 20, 2018), http://blog.interactiveschools.com/blog/the-evolution-of-twitter.

[124] Mary Bellis, *The Creation of YouTube*, THOUGHTCO (Apr. 3, 2018), https://www.thoughtco.com/who-invented-youtube-1992691.

[125] Kendra Leghart, *The FCC's New Network Semi-Neutrality Order Maintains Inconsistency in the Broadband World*, 12 N.C. J.L. & TECH. ONLINE 199, 227 n.142 (2011) (citing Bret Swanson, *The Coming Exaflood*, WALL ST. J. (Jan. 20, 2007), http://online.wsj.com/article/SB116925820512582318.html ("YouTube streams 75 petabytes (a petabyte is one quadrillion bytes) every three months, which is roughly the same amount as all the world's radios, cable and broadcast televisions stream in one year.").

[126] Annie Carter, *How Did Netflix Start*, ITSTILLWORKS (Jan. 9, 2018), https://itstillworks.com/facts-6757161-did-netflix-start-.html.

[127] Ashley Rodriguez, *Ten years ago, Netflix launched streaming video and changed the way we watch everything*, QUARTZ (Jan. 17, 2017), https://qz.com/887010/netflix-nflx-launched-streaming-video-10-years-ago-and-changed-the-way-we-watch-everything.

[128] Daniel A. Lyons, *An Antitrust-Informed Approach to Regulating Internet Interconnection* 24 B.U. J. SCI. & TECH. L. 229, 239 (2018) (citing Sandvine, 2016 GLOBAL INTERNET PHENOMENA, LATIN AMERICA AND NORTH AMERICA 2, 4 (2016)).

[129] *See* In the Matter of Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, 30 FCC Rcd. 1,375, 1,377 (2015) (determining

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

video creation and sharing, GIS, and other protocols challenge the characterization of an asymmetrical connection as "high-speed." More applications Americans commonly use to facilitate content publication and sharing defy the construct of high speed as requiring less upload speed than download. As video services became a larger portion of Internet traffic, the FCC must analyze its asymmetrical regulatory paradigm for Internet regulation.

F. The FCC's 2010 Open Internet Order*, Vacated in Part in* Verizon v. FCC*, 2014, Internet Regulation and the Virtuous Cycle of Innovation in the Instagram Age*

1. Protecting the Virtuous Circle of Innovation the Open Internet Engenders

The Internet's technical and functional evolution contributed to the debates over which regulatory category common carrier or information service to apply to broadband Internet services. The FCC's *2010 Open Internet Order* found that an open Internet creates "a virtuous circle of innovation in which new uses of the network—including new content, applications, services, and devices—lead to increased end-user demand for broadband, which drives network improvements, which in turn lead to further innovative network uses."[130] "Novel, improved, or lower-cost offerings introduced by content, application, service, and device providers spur end-user demand and encourage broadband providers to expand their networks and invest in new broadband technologies," the FCC observed.[131]

As examples of the innovations an open Internet engenders, the FCC cited "[s]treaming video and e-commerce applications," which "have led to major network improvements such as fiber to the premises, VDSL, and DOCSIS 3.0."[132] "Local

---

that "advanced telecommunications capability" requires access to actual download speeds of at least 25 Mbps and actual upload speeds of at least 3 Mbps); *see also* In the Matter of Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, 33 FCC Rcd. 1660, 1,668–69 (2018) (finding that fixed services provide "high-speed, switched, broadband telecommunications capability" as long as they meet the Commission's current speed benchmark of 25 Mbps download/3 Mbps upload (25 Mbps/3 Mbps)). The report also evaluates the availability of mobile Internet at 4G LTE as speeds of 5 Mbps/1 Mbps, and speeds of 10 Mbps/3 Mbps or higher but does not adopt a new standard for served speed for mobile services. *Id.* at 1,670.

[130] In the Matter of Preserving the Open Internet, 25 FCC Rcd. 17,905, 17,910–11 (WC Docket No. 07-52) (2010).

[131] *Id.* at 17,911.

[132] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

broadcasters are experimenting with new approaches to delivering original content, for example by creating neighborhood-focused websites; delivering news clips via online video programming aggregators, including AOL and Google's YouTube; and offering news from citizen journalists," the FCC noted.[133] "Unimpeded access to Internet distribution likewise has allowed new video content creators to create and disseminate programs without first securing distribution from broadcasters and multichannel video programming distributors (MVPDs) such as cable and satellite television companies. Online viewing of video programming content is growing rapidly."[134]

In 2014, the D.C. Circuit in *Verizon v. FCC* upheld the Commission's finding in the *2010 Open Internet Order* that "Internet openness drives a 'virtuous cycle' in which innovations at the edges of the network enhance consumer demand, leading to expanded investments in broadband infrastructure that, in turn, spark new innovations at the edge."[135] *Verizon v. FCC* also recognized that broadband providers' position in the Internet's architecture gave it the technical ability and financial incentive to exert control over the flow of Internet traffic.[136] "Broadband providers also have powerful incentives to accept fees from edge providers, either in return for excluding their competitors or for granting them prioritized access to end users."[137] "In fact, there appears little dispute that broadband providers have the technological ability to distinguish between, and discriminate against, certain types of Internet traffic,"[138] the D.C. Circuit emphasized.

2. ISPs as Internet Gatekeepers

The FCC's *2010 Open Internet Order* found "broadband providers potentially face at least three types of incentives to reduce the current openness of the Internet."[139] "*First*, broadband providers may have economic incentives to block or otherwise disadvantage specific edge providers or classes of edge providers, for

[133] *Id.* at 17,912–13.

[134] *Id.* at 17,914.

[135] Verizon v. FCC, 740 F.3d 623, 659 (D.C. Cir. 2014) (upholding the FCC's *2015 Open Internet Order* transparency rules and reversing the rules against blocking and throttling as common carrier-type restrictions, not supported by the FCC's classification of ISPs as information service providers).

[136] *Id.* at 645–46.

[137] *Id.*

[138] *Id.* at 646.

[139] In the Matter of Preserving the Open Internet, 25 F.C.C.R. 17905, 17915 (2010) (emphasis added).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

example by controlling the transmission of network traffic over a broadband connection, including the price and quality of access to end users."[140] "*Second*, broadband providers may have incentives to increase revenues by charging edge providers, who already pay for their own connections to the Internet, for access or prioritized access to end users."[141] "*Third*, if broadband providers can profitably charge edge providers for prioritized access to end users, they will have an incentive to degrade or decline to increase the quality of the service they provide to non-prioritized traffic."[142]

The technical ability of ISPs to limit Internet openness was not in question in the *2010 Open Internet Order* as the FCC observed instances where it had found or there were allegations of ISP actions that limited Internet openness. The FCC cited the 2005 *Madison River* case, where the Commission investigated allegations that "a broadband provider that was a subsidiary of a telephone company . . . had blocked Internet ports used for competitive VoIP [Voice over Internet Protocol] applications."[143] In addition to the 2008 Comcast complaint that investigated allegations that Comcast "disrupted certain peer-to-peer (P2P) uploads of its subscribers, without a reasonable network management justification and without disclosing its actions," the FCC highlighted complaints about certain mobile broadband services practices that limited Internet openness.[144] For example, the FCC found that "[a]fter entering into a contract with a company to handle online payment services, a mobile wireless provider allegedly blocked customers' attempts to use competing services to make purchases using their mobile phones."[145] "A nationwide mobile provider restricted the types of lawful applications that could be accessed over its 3G mobile wireless network."[146]

---

[140] *Id.*

[141] *Id.* at 17919.

[142] *Id.* at 17922.

[143] *Id.* at 17925 (*see* Madison River Communications, LLC and Affiliated Companies, 20 FCC Rcd. 4295 (2005)).

[144] *Id.* (citing In the Matter of Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications, 23 FCC Rcd. 13,028, 13055-56, paras. 1, 47–48 (2008); *see also* WCB Letter 12/13/10, Attach. at 1–15; Attachment A: Comcast Corporation Description of Current Network Management Practices, COMCAST, downloads.comcast.net/docs/Attachment_A_Current_Practices.pdf (last visited March 31, 2019)).

[145] *Id.*

[146] *Id.* (*see, e.g.*, Letter from James W. Cicconi, AT&T Services, Inc., to Ruth Milkman, Chief, Wireless Telecommunications Bureau, FCC, RM-11361, RM-11497 at 6–9 (filed Aug. 21, 2009) ("AT&T

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

3. Disclosure Alone Is Not Enough to Protect the Open Internet

My comments submitted for the record of the FCC's *2010 Open Internet Order* proceeding highlighted ISP contract terms that limited types of Internet content or protocols such as video and P2P.[147] These comments compared "wireless, cable and wireline-based Internet Service Provider ("ISP") descriptions on their web sites of the scope and breadth of Internet service advertised—whether touted as 'Unlimited,' sold based on set bandwidth consumption limits, or undefined" and compared those representations to "the restrictions set forth in the ISP's Terms of Service ("TOS") and Acceptable Use Policy ("AUP")."[148] My 2010 analysis found that most wireless ISPs advertised "Unlimited" Internet or data access, but in separate documents, displayed in fine print, accessible only through cyber-savvy searches, limit service to an undefined level bounded by "excessive use."[149] Wireless ISPs commonly "banned the legal use of Peer-to-Peer, while some barred Voice Over Internet Protocol."[150] Some wireless ISPs proscribed "downloading or uploading certain types of content such as movies or games."[151]

My comments emphasized that ISPs often made it difficult for consumers to find these restrictions.[152] Limiting terms were "often communicated through separate documents, displayed in fine print, many of which are accessible only through trails and clues worthy of a cyber-savvy Indiana Jones."[153] Tech-savvy consumers who could find the descriptions of ISP restrictions often could not understand what they meant because they were written in vague language that gave the ISP unbridled

indicated to Apple that it does not object to Apple enabling VoIP applications for the iPhone that use Wi-Fi connectivity . . . rather than AT&T's 2G or 3G wireless data services."); Sling Comments at 4–11; DISH PN Reply at 7 ("In reality, it took nine months of regulatory scrutiny and pressure from the public and DISH for AT&T to 'work with' DISH so that AT&T subscribers could access their Slingbox offerings over the wireless network. Other third-party application providers have experienced similar restrictions. VoIP operators such as Skype have faced significant difficulty in gaining access across wireless Internet connections.").

[147] Catherine J.K. Sandoval, *Reply Comments on Preserving the Open Internet* 2, 4 (WC Docket No. 07-52) (Apr. 26, 2010), https://ecfsapi.fcc.gov/file/7020442044.pdf.

[148] *Id.* at 4.

[149] *Id.* at 2.

[150] *Id.*

[151] *Id.* at 4.

[152] *Id.* at 2.

[153] *Id.* at 4.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

discretion to determine what level of use was permitted.[154] My study of ISP contract terms in 2010 found that many "wireless ISPs now advertise their Internet service as 'Unlimited,' but ban legal applications and erect invisible fences around 'excessive use.'"[155]

For example, Sprint's "Everything data with any Mobile," advertised in 2010 "Unlimited data: Web surfing, email, BlackBerry Internet Services, GPS Navigation, Sprint TV and Radio."[156] Sprint's "Acceptable Use Policy and Visitor Agreement," limited "excessive use" of its "Unlimited data" plan as ". . . determined by resource consumption relative to that of a typical individual user of the Service and not by the use of any particular application."[157] "While this policy does not target any specific application . . . it is impossible for an individual subscriber to know what a 'typical individual user of the Service' consumes without more information from the network operator who guards that data."[158]

Full and comprehensible disclosure "is important to make sure that consumers clearly understand what they are paying for, and that they receive what they paid for."[159] Yet, disclosure alone will not create an open Internet. Neither does disclosure remove incentives to discriminate against Internet content or applications that may compete with vertically integrated ISPs who also offer voice or video services or content through the Internet.[160] ISPs have a unique role and "power to control Internet use," a role the FCC emphasized in its determination that ISPs have "gatekeeper" power over Internet access.[161] The FCC's *2010 Open Internet Order* found that broadband providers' arguments that they should be allowed to charge

[154] *Id.* ("Those restrictions are often communicated through separate documents, displayed in fine print, many of which are accessible only through trails and clues worthy of a cyber-savvy Indiana Jones.")

[155] *Id.* at 16.

[156] *Id.* at 25.

[157] *Id.* at 26–27.

[158] *Id.* at 27.

[159] *Id.* at 6.

[160] *Id.* at 6–7.

[161] *Id.* at 7 (citing Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1420 (2009) ("[A]n ISP [is] . . . the only point on the network that sits between a user and the rest of the Internet.")).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

"edge" or content providers fees for Internet access, apart from subscription fees, illustrated that ISPs have the incentive and "ability to act as gatekeepers."[162]

The D.C. Circuit in *Verizon v. FCC* found in 2014 that ISPs who provide "last-mile" access that connects Internet users to the Internet serve as gatekeepers for subscribers who use the ISP to send traffic through the Internet.[163] *Verizon v. FCC* described the ISP gatekeeper role based on their position between Internet users and transmission of user data to and from the Internet. "Because all end users generally access the Internet through a single broadband provider, that provider functions as a 'terminating monopolist,' with power to act as a 'gatekeeper' with respect to edge providers that might seek to reach its end-user subscribers," the D.C. Circuit observed.[164] This "gatekeeper" capacity "distinguishes broadband providers from other participants in the Internet marketplace—including prominent and potentially powerful edge providers such as Google and Apple—who have no similar 'control [over] access to the Internet for their subscribers and for anyone wishing to reach those subscribers.'"[165]

4. The Open Internet Protects Public Safety

The FCC's *2010 Open Internet Order* for the first time in the net neutrality debate discusses the relationship between the Open Internet rules and public safety. "Open Internet rules are not intended to expand or contract broadband providers' rights or obligations with respect to other laws or safety and security considerations, including the needs of emergency communications and law enforcement, public safety, and national security authorities," the FCC concluded.[166] The FCC's construction of these limits makes it unclear whether "authorities" was meant to modify "public safety" needs so that this language only applied to public safety use of the Internet by "authorities." "*Nothing in this part supersedes any obligation or authorization a provider of broadband Internet access service may have to address the needs of emergency communications or law enforcement, public safety, or national security authorities, consistent with or as permitted by applicable law, or limits the provider's ability to do so*," the FCC's *2010 Open Internet Order*

[162] In the Matter of Preserving the Open Internet, 25 FCC Rcd. 17,905, 17,919 (2010).

[163] Verizon v. FCC, 740 F.3d 623, 628–29 (D.C. Cir. 2014).

[164] *Id.* at 646.

[165] *Id.*

[166] *Preserving the Open Internet*, 25 FCC at 17,962–63.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

concluded.[167] The FCC underscored that its open Internet rules "do not supersede any obligation a broadband provider may have—or limit its ability—to address the needs of emergency communications or law enforcement, public safety, or homeland or national security authorities (together, 'safety and security authorities')."[168]

The FCC's conceptualization of the Internet's role in public safety in 2010 focused on the ISP's roles and responsibilities with regard to public "safety and security authorities," not with regard to public safety generally. The *2010 Open Internet Order* highlighted ISP duties under the Communications Assistance for Law Enforcement Act, the Foreign Intelligence Surveillance Act, and the Electronic Communications Privacy Act.[169] The FCC also recognized that "there may be federal, state, tribal, and local public safety entities; homeland security personnel; and other authorities that need guaranteed or prioritized access to the Internet in order to coordinate disaster relief and other emergency response efforts, or for other emergency communications."[170]

The FCC agreed with commenters in the *2010 Open Internet Order* docket that the "safety and security rule should be tailored to avoid the possibility of broadband providers using their discretion to mask improper practices."[171] The FCC concluded that "it would be a mistake to limit the rule to situations in which broadband providers have an obligation to assist safety and security personnel."[172] The FCC recognized ". . . time may be of the essence in meeting safety and security needs."[173]

While the FCC's *2010 Open Internet Order* focused on institutional constructions of "public safety," the FCC acknowledged the importance of public safety in adopting net neutrality regulations. Danielle Goldstein, attorney for Santa Clara County, who represented Government Petitioners in the February 1, 2019, *Mozilla v. FCC* oral argument, highlighted the importance of the *2010 Order*'s recognition of the public safety role of the open Internet.[174] "We understood . . . the

[167] *Id.* at 17,963 (emphasis in original).

[168] *Id.*

[169] *Id.*

[170] *Id.*

[171] *Id.* at 17,964.

[172] *Id.*

[173] *Id.*

[174] Mozilla v. FCC Oral Argument, *supra* note 30, at 1:44:22.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

Commission to be policing Internet openness for a long time before the *2015 Order*. It's also true that the use of broadband in public safety has been on a rapid increase and we anticipate that that it will increase further still."[175] She emphasized that "both the *2010 Order* and the *2015 Order* specifically address public safety, which the [Internet Freedom] Order here didn't."[176] Goldstein argued that the *Internet Freedom Order*'s failure to address public safety use of the Internet is "opening up the doors both to having no regulator in the space that we can turn to and specifically allowing practices that allow public safety communications to be moved to the back of the line without any reason for doing so."[177]

The FCC's *2010 Open Internet Order* did not consider public use of nascent social media tools to foster public safety in America and abroad. Twitter and Flickr were important means of communication by victims of and witnesses to the November 2008 terrorist attack in Mumbai, India.[178] "A group of terrorists killed 165 and injured 304 people at the heart of India's financial capital, Mumbai, by using a combination of improvised explosive devices, grenades, and hand-held guns."[179] Presaging what is by 2019 an all too common use of social media, people in or near the hotel attacked in Mumbai in 2008 used Twitter to communicate what was happening or that they were safe, as well as to echo other messages.[180] Flickr was used to send photos of the incident as it was happening.[181] A decade later photos or live video would frequently emerge from inside disasters, terrorist, or dangerous incidents.

---

[175] *Id.*; *see also* Luke Batty, Mozilla Corp. v FCC, *Net Neutrality Oral Arguments*, YOUTUBE (Feb. 11, 2019), https://www.youtube.com/watch?v=vK7exbi9dnA. Many thanks to my research assistant, Luke Batty, for his assistance with this article, particularly his detailed review of the oral argument in *Mozilla Corp. v. FCC.* The posting of the oral argument on YouTube is an important public service as that platform makes it readily accessible to the public and easy to stop and start the file to review the oral argument.

[176] *Id.* at 1:44:38.

[177] *Id.* at 1:44:48.

[178] Charles Arthur, *How Twitter and Flickr Recorded the Mumbai Terrorist Attack*, GUARDIAN (Nov. 27, 2008), https://www.theguardian.com/technology/2008/nov/27/mumbai-terror-attacks-twitter-flickr.

[179] Onook Oh, Manish Agrawal & H. Raghav Rao, *Community Intelligence and Social Media Services: A Rumor Theoretic Analysis of Tweets During Social Crises*, 37 MIS Q. 407, 412 (2013); *see also* GOV'T OF INDIA, MUMBAI TERROR ATTACK: DOSSIER OF EVIDENCE 1 (2008).

[180] Claudine Beaumont, *Mumbai Attacks: Twitter and Flickr Used to Break News*, TELEGRAPH (Nov. 27, 2008), https://www.telegraph.co.uk/news/worldnews/asia/india/3530640/Mumbai-attacks-Twitter-and-Flickr-used-to-break-news-Bombay-India.html.

[181] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

Protecting public safety is core to the FCC's purpose and work. The FCC recognized its statutory public safety mission in analyzing the jurisdictional basis for the rule it adopted in 2010 to protect the open Internet.[182] The FCC was founded in 1934:

> For the purpose of regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all people of the United States without discrimination on the basis of race, color, religion, national origin, or sex, a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of the national defense, [and] for the purpose of promoting safety of life and property through the use of wire and radio communication. . . ."[183]

In 2016, the D.C. Circuit recognized in *Nuvio Corp. v. FCC* that Congress required the FCC to consider public safety in weighing regulation, including the economic cost of regulation.[184] "Congress has given an agency the responsibility to regulate a market such as the telecommunications industry that it has repeatedly deemed important to protecting public safety, the agency's judgments about the economic cost of its regulations must take into account its duty to protect the public," *Nuvio* emphasized.[185]

The D.C. Circuit in *Nuvio* underscored two statutory mandates through which Congress required the FCC to consider public safety in its rulemakings. The Communications Act of 1934, § 151 established the FCC "'[] to make available, so far as possible . . . [a] world-wide wire and radio communication service with adequate facilities at reasonable charges . . . *for the purpose of promoting safety of life and property through the use of wire and radio communications*.'"[186] The Wireless Communication and Public Safety Act of 1999, § 3, 47 U.S.C. § 615, requires the FCC to "'[] encourage and support efforts by States to deploy comprehensive end-to-end emergency communications infrastructure and programs, based on coordinated statewide plans, including seamless, ubiquitous, reliable

[182] In the Matter of Preserving the Open Internet, 25 FCC Rcd. 17,905, 17,966–67 (2010).

[183] 47 U.S.C. § 151 (2018).

[184] Nuvio Corp. v. FCC, 473 F.3d 302, 307 (2016).

[185] *Id.*

[186] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

wireless telecommunications networks and enhanced wireless 9-1-1 service.'"[187] Both statutes mandate analysis of public safety consideration in FCC decision-making.[188]

Nuvio found that the FCC's explicit consideration of public safety against objections to its rule ordering VoIP providers to transmit 9-1-1 calls within 120 days of its Order satisfied the statutory requirements that the FCC consider public safety and the APA.[189] *Nuvio* emphasized the FCC's analysis that recognized "'[w]hile 120 days is an aggressively short amount of time in which to comply with these requirements, *the threat to public safety if we delay further is too great* and demands near immediate action.'"[190]

Then Judge Kavanaugh's concurrence in *Nuvio* emphasized the FCC's statutory mission "of promoting safety of life and property through the use of wire and radio communications."[191] The Wireless Communications Act instructs the FCC to "'. . . designate 9-1-1 as the universal emergency telephone number within the United States for reporting an emergency to appropriate authorities and requesting assistance.'"[192] The ENHANCE 911 Act ("E-911 Act") adopted in 2005 found that "'for the sake of our Nation's homeland security and public safety, a universal emergency telephone number ("911") that is enhanced with the most modern and state-of-the-art telecommunications capabilities possible should be available to all citizens in all regions of the Nation.'"[193] Through the E-911 Act, "Congress made clear that 'enhanced 911 is a high national priority.'"[194]

Judge Kavanaugh's *Nuvio* concurrence emphasized these congressional mandates to consider public safety in evaluating the FCC's decision-making. "In my judgment, the FCC possesses the statutory authority, which the Commission may reasonably choose to exercise, to address the public safety threat by banning providers from selling voice service until the providers can ensure adequate 911

[187] *Id.* at 308.

[188] *Id.* at 307–08.

[189] *Id.* at 308.

[190] *Id.* (emphasis in the original).

[191] *Id.* at 311 (Kavanaugh, J., concurring).

[192] *Id.* (citing 47 U.S.C. § 251(e)(3) (2012)).

[193] *Id.* (citing Pub L. No. 108-494, 118 Stat. 3986 (2004) (codified at 47 U.S.C. § 942)).

[194] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

connections," Judge Kavanaugh wrote.[195] He observed that this authority ". . . necessarily includes the lesser power to ban such sales beginning in 120 days."[196]

The FCC timetable for wireless carriers to offer 911 access at issue in *Nuvio* focuses on carriers' public safety obligations but does not limit the FCC's consideration of the public safety implication of communication by wire or radio. In carrying out its statutory mission "of promoting safety of life and property through the use of wire and radio communications," the FCC must take into account the evolution of technological use and capabilities.[197] The FCC's *2010 Open Internet Order* emphasized that as the Supreme Court explained in the radio context in 1943, "Congress charged the Commission with 'regulating a field of enterprise the dominant characteristic of which was the rapid pace of its unfolding' and therefore intended to give the Commission sufficiently 'broad' authority to address new issues that arise with respect to 'fluid and dynamic' communications technologies."[198] These longstanding Supreme Court precedents recognize the FCC's mission to consider the evolving nature of communications technologies that use radio or wire to serve the public.

The FCC's analysis of the evolution of communications technologies including the Internet requires the Commission to consider the shifting use of the Internet for public safety. The *2010 Open Internet Order* considered public safety through an institution-focused lens that emphasized public safety authorities but did not limit public safety consideration or rules to institutional users or agencies charged with public safety duties. The *2015 Order* was the first to explicitly consider the public's use of the Internet for public safety. As a basis for adopting bright-line rules to protect the Internet's openness, the *2015 Order* cited my comments filed as a CPUC Commissioner that analyzed a range of public safety Internet uses including E-911

[195] *Id.*

[196] *Id.*

[197] *Id.* (citing 47 U.S.C. § 151 (1996)).

[198] In the Matter of Preserving the Open Internet, 25 FCC Rcd. 17,905, 17,967 (2010) (citing Nat'l Broad. Co., Inc. v. United States, 319 U.S. 190, 219–20 (1943) (Congress did not "attempt[] an itemized catalogue of the specific manifestations of the general problems" that it entrusted to the Commission); *see also* FCC v. Pottsville Broad. Co., 309 U.S. 134, 137, 138 (1940) (the Commission's statutory responsibilities and authority amount to "a unified and comprehensive regulatory system" for the communications industry that allows a single agency to "maintain, through appropriate administrative control, a grip on the dynamic aspects" of that ever-changing industry)).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

access, energy, water, and critical infrastructure management, fire and disaster prevention, preparation, and response.[199]

Verizon v. FCC emphasized the legal importance of regulatory classification, and vacated the net neutrality rules that the FCC's *2010 Open Internet Order* adopted based on Title I, but left in place the transparency rules.[200] In *Verizon v. FCC*, the D.C. Circuit ruled that the FCC could not impose common-carrier restrictions, such as non-discrimination rules against blocking and throttling with an exception for reasonable network management, unless it classified Internet service as a common carrier service.[201] Verizon upheld the FCC's rationale that its *2010 Open Internet Order* protected the virtuous circle of innovation the open Internet supports.[202] It also upheld the Commission's findings about ISP gatekeeper roles in the Internet architecture.[203] Verizon did not discuss the FCC's public safety analysis regarding its open Internet rules, nor did it disturb the FCC's public safety findings and determinations.

G. *The* 2015 Open Internet Order *and* U.S. Telecom Ass'n v. FCC*; Net Neutrality Regulation as the Internet Goes Social and Video Goes Viral*

1. Technological Evolution of the Internet's Function and ISP Gatekeeper Abilities and Incentives

By 2015 the Internet's technology, use, adoption, and deployment bore no resemblance to the technological extension of the book stack the Supreme Court described in 2003.[204] In less than eleven years, this outdated characterization of the Internet as a receptacle for passive audiences, who merely consume and do not create and disseminate information, was turned on its head. Readily available applications and services enabled publication and distribution of text, video, images, GIS files, and other content. By 2015, the Internet had become a lively two-way, multi-party platform for communication, allowing speech to flourish and ideas to proliferate. The lack of Internet gatekeepers makes it an open platform to diverse voices and

[199] In the Matter of Protecting & Promoting the Open Internet, 30 FCC Rcd. 5601, 5654–55 n.291 (2015) (citing Commissioner Sandoval, *Ex Parte Letter*, *supra* note 4, at 2).

[200] Verizon v. FCC, 740 F.3d 623, 659 (D.C. Cir. 2014).

[201] *Id.*

[202] *Id.* at 644–66.

[203] *Id.*

[204] United States v. Am. Library Ass'n, 539 U.S. 194, 207 (2003).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

viewpoints, in contrast to closed studios and centrally controlled media systems. The Internet's platform for speakers and multi-sided communication makes it an unrivaled mechanism for democratic engagement and an important platform for public safety.[205]

The FCC's *2015 Order* recognized "that broadband providers have both the incentive and the ability to act as gatekeepers standing between edge providers and consumers" and can undermine the "virtuous cycle" of innovation the Internet drives.[206] "Broadband providers can exploit this role by acting in ways that may harm the open Internet, such as preferring their own or affiliated content, demanding fees from edge providers, or placing technical barriers to reaching end users,"[207] the *2015 Order* concluded. "As gatekeepers . . . [ISPs] can block access altogether; they can target competitors, including competitors to their own video services; and they can extract unfair tolls."[208]

By the time the *2015 Order* was adopted, ISP technical capacity to restrict Internet access had also evolved. The FCC fined AT&T $100 million in 2015 for inadequate disclosure to "unlimited plan" customers that their Internet speeds would be dramatically slowed if they used more than an undisclosed amount of data.[209] AT&T reduced deprioritized customer speeds to "256 kbps or 512 kbps [kilobits per second,] . . . for an average of 12 days per billing cycle," the FCC determined.[210] Those speeds made it "impossible to use AT&T's data service" for common uses such as "mapping applications . . . streaming online video to catch up on television or news, or using video chat applications to stay connected with friends and family," the FCC found.[211]

In 2016, the D.C. Circuit in *USTA v. FCC* upheld the FCC's *2015 Order*, citing the FCC's analysis that "convincingly detailed how broadband providers' [gatekeeper] position in the market gives them the economic power to restrict edge-

[205] Commissioner Sandoval, *Ex Parte Letter*, *supra* note 4, at 86.

[206] In the Matter of Protecting & Promoting the Open Internet, 30 FCC Rcd. 5601, 5608 (2015) (citing *Verizon*, 740 F.3d at 659).

[207] *Id.* at 5629.

[208] *Id.* at 5608.

[209] In the Matter of AT&T Mobility, LLC., 30 FCC Rcd. 6613, 6613 (2015).

[210] *Id.* at 6616.

[211] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

provider traffic and charge for the services they furnish edge providers."[212] ISP deliberate slowing of customers on unlimited plans to speeds where they cannot use a map demonstrates ISP technical capability and willingness to disable Internet functionality through their network practices.

2. Recognizing the Public's Role in Public Safety Supported by the Open Internet

The FCC's *2015 Order* was the first to consider the public's role in public safety uses of the Internet. The *2015 Order* construed public safety broadly, not just as an issue affecting institutional public safety agencies. The FCC cited to my comments, submitted in my individual capacity as a CPUC Commissioner, that emphasized public safety issues in the open Internet ranging from E-911 access and call completion, to water, energy, and critical infrastructure use of the Internet by the public to promote safety and reliability.[213]

The FCC's 2014 Notice of Proposed Rulemaking ("NPRM") for the Open Internet proceeding proposed to establish a minimum level of access standard for broadband Internet, and to allow Internet "content" or "edge providers," to negotiate with ISPs for fast access to the Internet above that level.[214] After considering the record, the FCC rejected its minimum Internet speed proposal put forward in the NPRM. "Broadband providers, edge providers, public interest organizations, and other parties note the practical and technical difficulties associated with setting any such minimum level of access," the FCC concluded.[215] The FCC cited my comments that emphasized "any of the minimum level of access standards the FCC proposes

[212] U.S. Telecom Ass'n, 825 F.3d 674, 694 (citing Verizon v. FCC, 740 F.3d 623, 646 (D.C. Cir. 2014)).

[213] *Protecting & Promoting the Open Internet*, 30 FCC Rcd. at 5663 n.254, 5670 n.254, 5679 n.355, 5707 nn.501 & 503.

[214] In the Matter of Protecting & Promoting the Open Internet, 29 FCC Rcd. 5561, 5596 (2014).

[215] *Protecting & Promoting the Open Internet*, 30 FCC Rcd. at 5663 n.254. *See, e.g.*, Mozilla Comments at 15 (warning that defining a no-blocking rule in terms of establishing a minimum level of service is not likely "to prove effective and workable in practice"); USTelecom Comments at 50 ("the Commission should not impose a minimum level of service for free obligation"); Letter from Catherine J.K. Sandoval, Commissioner, California Public Utilities Commission, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 14-28, 10-127, Attach. at 14 (filed Oct. 14, 2014) [hereinafter *Sandoval Ex Parte Letter*] ("[A]ny of the minimum level of access standards the FCC proposes would be insufficient to support the needs of a diversity of Internet users including Critical Infrastructure.")").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

would be insufficient to support the needs of a diversity of Internet users including Critical Infrastructure."[216]

To support the adoption of a ban on paid Internet priority, the *2015 Order*, citing my comments, recognized several values net neutrality rules would safeguard, including public safety and universal service.[217] The Order also cited protecting free expression, eliminating artificial barriers to entry, distorting the market, harming competition, harming consumers, and discouraging innovation as reasons that supported its paid priority ban.[218]

The *2015 Order* declined, based on the record, to adopt a "a legal standard prohibiting commercially unreasonable practices" without imposing bright-line net neutrality rules. It concluded that such a commercial reasonableness standard "is not the most effective or appropriate approach for protecting and promoting an open Internet."[219] The FCC rested this conclusion on record comments including mine regarding the importance of the open Internet to public safety such as disaster response and treatment of burn victims.[220]

In evaluating the FCC's role in Internet traffic exchange disputes between ISPs and content providers, the FCC cited my comments that discussed the effect of congestion on service, including E-911 access. "When links are congested and capacity is not augmented, the networks—and applications, large and small, running over the congested links into and out of those networks—experience degraded quality of service due to reduced throughput, increased packet loss, increased delay, and increased jitter," the FCC observed.[221] The FCC based its concern on record comments, such as those of Level 3, then a Competitive Local Exchange Carrier and

[216] *Id.*

[217] *Id.* at 5670 n.291.

[218] *Id.* at 5654.

[219] *Id.* at 5665.

[220] *Id.* at 5679 n.355 ("CDT Comments at 19; Free Press Comments at 8–9; Public Knowledge Comments at 31; MLB Advanced Media Comments at 2–3; Microsoft Comments at 13–4; Internet Association Comments at 16; *Sandoval Ex Parte Letter*, *supra* note 215, at 2 (asserting that the commercial reasonableness rule would "deter investment and Internet applications, such as Internet-enabled 'Smart beds,' which read a patient's vital signs and send aggregated data on available beds to mass casualty and disaster planners who use this information to determine which hospital has an available bed in a burn unit)").

[221] *Id.* at 5689.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

Internet core transport facilitator, which explained "that congested interconnection points result in dropped packets and a degraded consumer experience."[222]

The FCC also cited my comment's report of "slow connection speeds during the Comcast-Cogent traffic exchange dispute," and observation that the dispute affected other applications including "gaming, VPN, and VoIP (including compliance with 911 standards)."[223] The FCC concluded, that "at the end of the day, consumers bear the harm when they experience degraded access to the applications and services of their choosing due to a dispute between a large broadband provider and an interconnecting party."[224] My comments cautioned that "difficulties in using interconnected VoIP service amidst a broadband provider dispute with a server host or content provider raise grave concerns about public safety and network reliability."[225]

The FCC's *2015 Order* considered the public's use of and interest in the open Internet, free of ISP blocking, throttling, and paid priority, and unreasonable network management. The *Internet Freedom Order*'s public safety analysis fulfills the FCC's statutory duty recognized in *Nuvio* to consider public safety in rulemakings.[226] In addition, the APA imposes a heightened standard on subsequent agency consideration of issues previously considered in a rulemaking on that topic.[227] The FCC also had a duty to consider record evidence before it in the *Internet Freedom* docket regarding the public's interest in the open Internet and public role in public safety. The FCC failed to comply with its statutory duties and the APA by omitting consideration of public safety issues central to its statutory mission in its *Internet Freedom Order*. "An 'arbitrary and capricious' regulation of this sort is itself unlawful and receives no *Chevron* deference" to an administrative agency's

[222] *Id.* at 5707 n.501.

[223] *Id.* (citing Commissioner Sandoval, *Ex Parte Letter*, *supra* note 4, attach. at 22–24).

[224] *Id.* at 5689.

[225] *Id.* at 5707 n.503 (citing Commissioner Sandoval, *Ex Parte Letter*, *supra* note 4, attach. at 24).

[226] Nuvio Corp. v. FCC, 473 F.3d 302, 307 (D.C. Cir. 2006).

[227] Perez v. Mortg. Bankers Ass'n, 135 S. Ct. 1199, 1209 (2015).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

interpretation of an ambiguous statute.[228] As described below, these failures mandate the *Internet Freedom Order*'s remand, and would support vacatur.[229]

III. THE "CAT VIDEO PARADIGM"—POLICY FRAMES AND THE INTERNET'S EVOLUTION AS A PUBLIC SAFETY PLATFORM

A. Framing Analysis: Policy Discourse Shaped by Prescriptive Frames

The sociology and communications theory fields have long used "framing analysis" to uncover perspectives that shape discourse or media portrayals. "Erving Goffman's *Frame Analysis* developed in 1974 maintains that we all actively classify, organize, and interpret our life experiences to make sense of them. The 'schemata of interpretation,' which are labeled 'frames,' enable individuals 'to locate, perceive, identify, and label' occurrences or information."[230]

W.A. Gamson and A. Modigliani describe a frame as "the core of a larger unit of public discourse, called a 'package,' that also contains various policy positions that may be derived from the frame as well as a set of 'symbolic devices' that signify the presence of frames and policy positions."[231] Gamson and Lasch, and Gamson and Modigliani identify five "devices that signify the uses of frames: metaphors, exemplars, catchphrases, depictions, and visual images."[232]

Zhongdang Pan and Gerald M. Kosicki contend that framing can also be "viewed as placing information in a unique context so that certain elements of the issue get a greater allocation of an individual's cognitive resources" and, as a result,

---

[228] Encino Motorcars, LLC v. Navarro, 136 S. Ct. 2117, 2126 (2016) (citing United States v. Mead Corp., 533 U.S. 218, 227 (2001)).

[229] U.S. Telecom Ass'n v. FCC, 825 F.3d 674, 708–09 (D.C. Cir. 2016) (quoting Fox Television Stations, Inc. v. FCC, 556 U.S 502, 515–16 (2009)). *Mozilla*, ___ F.3d at 95, 97, 100 (remanding the Internet Freedom Order for failure to analyze the public safety issues raised in the record by former CPUC Commissioner Sandoval, the CPUC, Santa Clara County, and others, but declining to vacate the Order).

[230] Zhongdang Pan & Gerald M. Kosicki, *Framing Analysis: An Approach to News Discourse*, 10 POL. COMM. 55, 56 (1993) (citing ERVING GOFFMAN, FRAME ANALYSIS: AN ESSAY ON THE ORGANIZATION OF EXPERIENCE 21 (1974)).

[231] *Id.* (citing W.A. Gamson & A. Modigliani, *The Changing Culture of Affirmative Action*, *in* 3 RESEARCH IN POLITICAL SOCIOLOGY 137–77 (1987)) [hereinafter Gamson & A. Modigliani]).

[232] *Id.* (citing Gamson & A. Modigliani, *supra* note 231; W.A. Gamson & K.E. Lasch, *The Political Culture of Social Welfare Policy*, EVALUATING THE WELFARE STATE: SOCIAL AND POLITICAL PERSPECTIVES 397–415 (1983); W.A. Gamson & A. Modigliani, *Media Discourse and Public Opinion: A Constructionist Approach*, 95 AM. J. SOC. 1, 1–37 (1989)).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

"selected elements become important in influencing individuals' judgments or inference making."[233] Robert Entman described this priority-making function by observing that "to frame a communicating text or message is to promote certain facets of a 'perceived reality' and make them more salient in such a way that endorses a specific problem definition, causal interpretation, moral evaluation, and/or a treatment recommendation."[234]

Merlijn Van Hulst and Dvora Yanow offer a "policy analytic approach" that "shifts the focus to 'framing,' the interactive, intersubjective processes through which frames are constructed."[235] Hulst and Yanow "contend that 'frames' are often treated as objects people possess in their heads and develop for explicitly strategic purposes."[236] Hulst and Yanow describe frames as a "taxonomizing approach to the subject," and classify "framing" as more dynamic.[237] The taxonomizing function of frames captures the FCC's focus on regulatory classification. Framing reflects FCC perspectives in decision-making, views often shrouded in regulatory process.

B. The FCC's Internet Freedom Order *Rips the Public Safety Frame Off the Wall*

The FCC's *Internet Freedom Order* views the proceeding's issues and record through frames like out-of-date prescription glasses. The *Internet Freedom Order*'s first paragraph extols the "light-touch framework under which a free and open Internet underwent rapid and unprecedented growth for almost two decades."[238] This frame and the FCC's framing of the Internet led the FCC to ignore the Internet's technological evolution and changing public use.

As an example of the application of the FCC's pre-conceived frame, the FCC determined that "[c]onsumers purchase mobile broadband Internet access service to

---

[233] Pan & Kosicki, *supra* note 230, at 57 (citing D. Kahneman & A. Tversky, *Choices, Values, and Frames*, 39 AM. PSYCHOLOGIST 341, 341 (1984)).

[234] Margaret Cissel, *Media Framing: A Comparative Content Analysis on Mainstream and Alternative News Coverage of Occupy Wall Street*, 3 ELON J. UNDERGRADUATE RES. COMM. 67 (2012) (citing R.M. Entman, *Framing: Towards Clarification of a Fractured Paradigm*, 4 J. COMM. 43, 51 (1993)).

[235] Merlijn Van Hulst & Dvora Yanow, *From Policy "Frames" to "Framing": Theorizing a More Dynamic, Political Approach*, 46 AM. REV. PUB. ADMIN. 92, 93 (2016) (citing K. WEICK, THE SOCIAL PSYCHOLOGY OF ORGANIZING (2d ed. 1979)).

[236] *Id.*

[237] *Id.*

[238] In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311, 312 (2018).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

access the Internet, on-line video, games, search engines, websites, and various other applications, while they purchase mobile voice service solely to make calls to other users using NANP [North American numbering plan] numbers."[239] The FCC used these distinctions to support its determination that "mobile broadband Internet access today is not the functional equivalent of commercial mobile service."[240]

The FCC frames public use of mobile broadband Internet by emphasizing online video, games, and entertainment uses. The FCC's frame ignores the role of interconnected mobile broadband providers in supporting 9-1-1 access, the service at issue in *Nuvio* in 2006, voice, video, GIS, and other uses of the Internet to promote public safety.

The FCC's *2015 Order* recognized that a "broadband provider dispute with a server host or content provider raise[s] grave concerns about public safety and network reliability."[241] The FCC's *2018 Internet Freedom Order* failed to acknowledge the public safety functions of mobile broadband Internet. The D.C. Circuit's *Mozilla v. FCC decision* agreed with Government Petitioners and with the arguments in the amicus brief I authored and co-signed that absence of consideration of public safety, a statutory mandate in the FCC's mission and regulation of mobile broadband, constitutes arbitrary and capricious decision-making under the APA.[242]

The *Internet Freedom Order* shares with the Computer Inquires the absence of substantive discussion about the impact of these proceedings on democracy. Lentz's study of each rulemaking for the Computer Inquires noted the absence in "the Computer Inquiry dockets of terms like 'First Amendment,' 'democracy,' or 'speech.'"[243] Lentz cites my Article, *Disclosure, Deception, and Deep-Packet Inspection*, that argued for FCC and Federal Trade Commission action to "safeguard the Internet itself as a source for innovation and a wide range of speech."[244] Lentz

[239] *Id.* at 361–62.

[240] *Id.*

[241] In the Matter of Protecting & Promoting the Open Internet, 30 FCC Rcd. 5601, 5707 n.503 (2015) (citing Commissioner Sandoval, *Ex Parte Letter*, *supra* note 4, attach. at 24).

[242] Nuvio Corp. v. FCC, 473 F.3d 302, 307 (D.C. Cir. 2006); *Amici Brief, Professors of Administrative, Communications, Energy and Contract Law and Policy*, *supra* note 5, at 2; Reply Brief for Government Petitioners at 3, Mozilla Corp. v. FCC, No. 18-1051 (Nov. 16, 2018) [hereinafter Government Petitioners Reply Brief]; *Mozilla*, ___ F.3d at 94–100.

[243] Lentz, *supra* note 33, at 443.

[244] *Id.* (citing Sandoval, *Disclosure, Deception, and Deep-Packet Inspection*, *supra* note 44, at 651).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

expressed concern that "putting ISPs into the enhanced services category means they are allowed to censor or limit access to content, free from First Amendment scrutiny."[245] The APA requires the FCC to address the impact of regulatory classification and net neutrality rule repeal on democracy and free expression, as they were among the values that the *2015 Internet Freedom Order* was adopted to protect.[246]

The FCC's *Internet Freedom Order* rips the public safety frame off the wall without acknowledging that its Order does so. "The Supreme Court in *Encino Motorcars, LLC v. Navarro* held that the APA requires that the agency must at least 'display awareness that it is changing position' and 'show that there are good reasons for the new policy.'"[247] "An agency rescinding a rule 'is obligated to supply a reasoned analysis for the change beyond that which may be required when an agency does not act in the first instance.'"[248] "'Put another way,' the D.C. Circuit stated in *USTA v. FCC*, '[i]t would be arbitrary and capricious to ignore such matters.'"[249] The FCC abrogates its statutory duties to protect public safety and fails the APA through the absence of discussion of the importance of net neutrality rules to public safety and democracy.

C. Open Internet Access Empowers Democracy and Public Safety for the Whole Community

Democracy is intertwined with public safety. Participatory democracy allows everyone to speak, values every person, and protects their rights to liberty.[250]

---

[245] *Id.*

[246] *Protecting & Promoting the Open Internet*, 30 FCC Rcd. at 5670 n.292 (citing Illinois and NY Comments at 6 (asserting that "[i]f broadband providers can discriminate among content, they can effectively pick winners and losers, interfering with the public's ability to freely educate itself about political, cultural, and social issues—education that is critical to our democracy"); Ad Hoc Comments at 20 (asserting that paid prioritization would distort consumers' choices among content and edge providers); Church World Service et al. Reply at 1; Independent Filmmaker Organizations Reply at 3–6; City of Los Angeles Comments at 5).

[247] *Amici Brief, Professors of Administrative, Communications, Energy and Contract Law and Policy*, *supra* note 5, at 5 (citing Encino Motorcars, LLC v. Navarro, 136 S. Ct. 2117, 2126 (2016)).

[248] *Id.* (citing Motor Veh. Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto Ins. Co., 463 U.S. 29, 42 (1983)).

[249] *Id.* (citing U.S. Telecom Ass'n v. FCC, 825 F.3d 674, 708–09 (D.C. Cir. 2016) (quoting Fox Television Stations, Inc. v. FCC, 556 U.S 502, 515–16 (2009))).

[250] *See* David Alan Sklansky, *Police and Democracy*, 103 MICH. L. REV. 1699, 1769 (2005) (arguing that "participatory democracy tends to highlight the importance of order and public safety").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

Community policing is a philosophy that promotes "the systematic use of partnerships and problem-solving techniques, to proactively address the immediate conditions that give rise to public safety issues, such as crime, social disorder, and fear of crime."[251] Community-based policing reforms focus on "legitimacy theory," fostering decision-making inclusivity "to build trust and develop a law-abiding citizenry."[252] The philosophy of community policing is based on the theory that "the police cannot successfully prevent or investigate crime without the willing participation of the public, therefore police should transform communities from being passive consumers of police protection to active co-producers of public safety."[253] "Community policing transforms police from being an emergency squad in the fight against crime to becoming primary diagnosticians and treatment coordinators," David H. Bayley and Clifford D. Shearing observed.[254]

Similarly, FEMA's "Whole Community Approach to Emergency Management" emphasizes the need to include the public in disaster planning and response and address the diverse needs of community members.[255] "Government can and will continue to serve disaster survivors," Craig Fugate, FEMA Administrator in 2011, testified to Congress, "[h]owever, we fully recognize that a government-centric approach to disaster management will not be enough to meet the challenges posed by a catastrophic incident."[256] "That is why we must fully engage our entire societal capacity," Fugate emphasized.[257] FEMA's Whole Community approach to disaster preparation and response rests on the proposition that "[a] community-centric approach for emergency management that focuses on strengthening and

[251] Williams et al., *supra* note 27, at 211 n.4.

[252] Sunita Patel, *Toward Democratic Police Reform: A Vision for "Community Engagement" Provisions in DOJ Consent Decrees*, 51 WAKE FOREST L. REV. 793, 794 (2016).

[253] David H. Bayley & Clifford D. Shearing, *The Future of Policing*, 30 L. & SOC'Y REV. 585, 588 (1996).

[254] *Id.*

[255] *FEMA, Whole Community Approach*, *supra* note 9, at 2.

[256] *Improving the Nation's Response to Catastrophic Disasters: How to Minimize Costs and Streamline our Emergency Management Programs*, U.S. DEP'T HOMELAND SECURITY (Mar. 30, 2011), https://www.dhs.gov/news/2011/03/30/administrator-craig-fugate-federal-emergency-management-agency-transportation-and.

[257] *FEMA, Whole Community Approach*, *supra* note 9, at 2.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

leveraging what works well in communities on a daily basis offers a more effective path to building societal security and resilience."[258]

FEMA describes its Whole Community approach as "a means by which residents, emergency management practitioners, organizational and community leaders, and government officials can collectively understand and assess the needs of their respective communities and determine the best ways to organize and strengthen their assets, capacities, and interests."[259] "A Whole Community approach attempts to engage the full capacity of the private and nonprofit sectors, including businesses, faith-based and disability organizations, and the general public, in conjunction with the participation of local, tribal, state, territorial, and Federal governmental partners."[260] FEMA emphasized the need for emergency managers "to understand how to work with the diversity of groups and organizations and the policies and practices that emerge from them in an effort to improve the ability of local residents to prevent, protect against, mitigate, respond to, and recover from any type of threat or hazard effectively."[261]

A New Jersey court described the Whole Community approach embraced by a local Office of Emergency Management ("OEM") as "emergency planning that involves entire communities and not just government agencies. By including the full spectrum of people and organizations represented in a community, emergency planning will account for the needs of all communities' members, regardless of their personal circumstances or abilities."[262] "We include individuals with functional needs, advocates and human service providers in all phases of the emergency management process—mitigation, preparedness, response and recover," the OEM explains.[263] "There is nothing 'special' about insuring everyone can access mass care shelters, understand emergency information, evacuate safely or receive recovery

[258] *Id.* at 22.

[259] *Id.* at 3.

[260] *Id.*

[261] *Id.*

[262] Smith v. Twp. of Warren, No. CV 14-7178-BRM-LHG, 2016 WL 7409952, at *2 (D.N.J., Dec. 22, 2016).

[263] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

information. Whole-community planning is something we practice as a normal course of business, because every life matters."[264]

"FEMA's Whole Community approach seeks to involve individuals and families, including people with 'access and functional needs,' businesses, community organizations and all other sectors of society to prepare for disasters."[265] "The Whole Community approach emphasizes the necessity of non-traditional resources and their application in innovative ways 'to save lives and sustain communities after catastrophic disasters.'"[266] The Whole Community concept includes participation by and response to "the full spectrum of community residents and members (including but not limited to people speaking diverse languages or from diverse cultures or economic backgrounds, all ages from children and youth to seniors, people with disabilities, others with access and functional needs, and populations traditionally underrepresented in civic government)."[267]

The Whole Community approach to disaster preparation and response reflects concepts embedded in communications policy including commitments to universal service and public safety. The "universal service objective is founded on the concept that all subscribers to a telephone company's basic service network benefit when another person joins that network. Therefore, the entire network is more valuable because of the addition of the new subscriber."[268] Making communications networks including the Internet accessible and open to the whole community promotes universal service and increases community resiliency and resources.

Jennifer Prah Ruger argues that "informal, personal risk management instruments are ineffective in the face of larger natural or social disasters, which impact a whole community."[269] "Social risk management [SRM]," she explains,

---

[264] *Id. See also NJOEM and NJ Statewide Independent Living Council Promote Emergency Preparedness for People with Disabilities*, N.J. OFF. ATT'Y GEN. (May 24, 2011), http://ready.nj.gov/media/pr052411.html.

[265] Emily Naser-Hall, *The Disposable Class: Ensuring Poverty Consciousness in Natural Disaster Preparedness*, 7 DEPAUL J. SOC. JUST. 55, 66 (2013).

[266] *Id.*

[267] Angelyn Spaulding Flowers, *Emergency Management and Vulnerable Populations*, 48 URB. LAW. 563, 563–64 (2016).

[268] Tex. Alarm & Signal Ass'n v. Pub. Util. Comm'n, 603 S.W.2d 766, 770 (Tex. 1980); Pub. Util. Comm'n v. AT&T Comm'ns, 777 S.W.2d 363, 372 (Tex. 1989).

[269] Jennifer Prah Ruger, *Social Risk Management—Reducing Disparities in Risk, Vulnerability and Poverty Equitably*, 27 MED. & L. 109, 113 (2008).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

"aims at providing instruments for the poor (and non-poor as well) to minimize risk exposure's impact, making them less vulnerable and eventually able to rise out of poverty. Three main welfare enhancing goals of SRM include: reduced vulnerability, enhanced consumption smoothing and improved equity."[270]

"Social justice demands more than fair distribution of resources in circumstances of extreme health emergency," Lawrence O. Gostin and David P. Fidler argue.[271] "A failure to act expeditiously and with equal concern for all citizens, including the poor and less powerful, predictably harms the whole community by eroding public trust and undermining social cohesion."[272] "It signals to those affected and to everyone else that the basic human needs of some matter less than those of others, and it thereby fails to show the respect due to all members of the community," they contend.[273] "Social justice thus encompasses not only a core commitment to a fair distribution of resources, but it also calls for policies of action that are consistent with the preservation of human dignity and the showing of equal respect for the interests of all members of the community," Gostin and Fidler underscore.[274]

Infrastructure access including Internet governance is a subject of great public interest, as evidenced by the millions of public comments filed in the 2018 net neutrality proceeding.[275] Infrastructure failures, including Internet governance, require concerted government-public-and private collaboration. My book chapter on the Native American reservation electricity gap, *Energy Access is Energy Justice: The Yurok Tribe's Trailblazing Work to Close the Native American Reservation Electricity Gap*, argues that "[e]nergy infrastructure poverty is community poverty stemming from federal, state, and private sector decisions that excluded many Native

[270] *Id.*

[271] Lawrence O. Gostin & David P. Fidler, *Biosecurity Under the Rule of Law*, 38 CASE W. RES. J. INT'L L. 437, 469 (2007).

[272] *Id.*

[273] *Id.*

[274] *Id.*

[275] Brian Naylor, *As FCC Prepares Net-Neutrality Vote, Study Finds Millions of Fake Comments*, NPR (Dec. 14, 2017), https://www.npr.org/2017/12/14/570262688/as-fcc-prepares-net-neutrality-vote-study-finds-millions-of-fake-comments. *See also* Sandoval, *Reply Comments*, *supra* note 5, at 57–58; *Amici Brief, Professors of Administrative, Communications, Energy and Contract Law and Policy*, *supra* note 5, at 20 (citing Sandoval, *Reply Comments*, *supra* note 5, at 13 ("False filings based on identity theft hack the tools of democratic decision-making for an ulterior motive.")).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

American reservations from 'universal service' policies."[276] "Strategies focused on individual rights, or on alleviating individual or family poverty, are insufficient to provide the resources needed to build the electric grid to households and institutions that lack such access," my book chapter argued.[277] Similarly, public access to the Internet depends on infrastructure and governance decisions such as the FCC's proceedings analyzing rules that govern net neutrality. These proceedings must take into account the changing nature of the Internet and its use as diverse communities face fires, floods, and other conflagrations.

FEMA and humanitarian assistance organizations increasingly recognize communications as humanitarian and disaster aid.[278] "When disaster strikes, communications networks are often lost, at a time when humanitarian workers and community members need them most."[279] The Internet, mobile devices, GIS-based and other apps that use video, photos, and text, each can collect disaster or public safety data through citizen volunteers, which helps facilitate emergency response.[280]

In the deadly 2018 "Camp Fire" centered in Paradise, California in Butte County, 86 people died and more than 18,800 structures were destroyed.[281] The 911 system quickly became overwhelmed and communications systems failed as lines

[276] Catherine J.K. Sandoval, *Energy Access Is Energy Justice: The Yurok Tribe's Trailblazing Work to Close the Native American Reservation Electricity*, *in* ENERGY JUSTICE, INTERNATIONAL AND U.S. PERSPECTIVES 7 (Raya Salter et al. eds., 2018).

[277] *Id.*

[278] Catherine Cheney, *Communications as Aid: Key Takeaways from the Humanitarian ICT Forum*, DEVEX (Mar. 2017), http://www.devex.com/news/communication-as-aid-key-takeaways-from-the-humanitarian-ict-forum-89898/amp.

[279] *Id.*

[280] *See* Michael Erskine & Dawn Gregg, *Utilizing Volunteered Geographic Information to Develop a Real-Time Disaster Mapping Tool: A Protype and Research Framework, Association for Information Systems*, AIS ELECTRONIC LIBRARY (AISEL), CONF-IRM 2012 PROCEEDINGS (May 1, 2012), https://pdfs.semanticscholar.org/1d69/d352ef3aba070f7202161faeac20a67a3e06.pdf.

[281] Ashley McBride, *Camp Fire: Death Toll Rises to 86 After Hospitalized Man Dies from Burn Injuries*, SAN FRANCISCO CHRON. (Dec. 11, 2018), https://www.sfchronicle.com/california-wildfires/article/Camp-Fire-Death-toll-rises-to-86-after-13458956.php; J.D. Morris, *California Wildfire Losses, Mostly from Camp Fire, Total $9 Billion So Far*, SAN FRANCISCO CHRON. (Dec. 12, 2018), https://www.sfchronicle.com/business/article/California-wildfire-losses-mostly-from-Camp-13461876.php.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

burned.[282] The nature and scale of this wildfire challenged traditional public safety resources and paradigms that rely on institutional response during a disaster. Police and fire officials were overwhelmed, lacked accurate information, infrastructure failed, and traffic jams clogged escape routes as fire roared.[283] Survivors fended for themselves and struggled to help family members and neighbors.[284]

During several California fires, communications failures led public safety officials to resort to old-school methods (*i.e.*, bullhorns) as lines burned, the power went out, and power-dependent communications systems failed.[285] The CPUC found in 2016:

> During a fire, loss of communications facilities and/or services requires the incident commander to determine whether to deploy public safety personnel to drive through neighborhoods and use their loudspeakers or bullhorns to announce evacuations. Officials must decide during an outage whether to activate sirens or the local Ham radio community, and "go old-school" when phones and the Internet don't work.[286]

As fires raged Camp Fire and other wildfire survivors reported trying to get out a video, text, or call as they made life or death decisions to escape or seek shelter. Social media facilitated communications to loved ones as survivors reached places where networks still functioned.

During and in the aftermath of the Camp Fire, Facebook activated its crisis response mode that allows a user to mark themselves "safe" or inquire into the safety of another Facebook member.[287] Several Paradise residents filmed their evacuation

---

[282] Lisa Krieger, *Camp Fire Created a Blackhole of Communication, In Disasters our High-Tech Communities Are Reduced to 1940s Responses*, SAN JOSE MERCURY NEWS (Dec. 16, 2018), https://www.mercurynews.com/2018/12/16/camp-fire-created-a-black-hole-of-communication/.

[283] *Id.*

[284] *Id.*

[285] *Id.* (citing interview with Professor Catherine Sandoval, "communications failures force communities to rely on 1940s methods such as bullhorns for evacuation warnings"); *see also* CAL. PUB. UTIL. COMM'N, 16-12-066, DECISION ON RURAL CALL COMPLETION ISSUES, OTHER CALL COMPLETION ISSUES AND CALL INITIATION ISSUES INCLUDING LACK OF 911 ACCESS AND DIAL TONE 73 (2016) [hereinafter *CPUC Rural Call Completion Decision D. 16-12-066*].

[286] *CPUC Rural Call Completion Decision D. 16-12-066*, *supra* note 285, at 73.

[287] *See* Crisis Response, *The Camp Fire in Butte County, California, USA*, FACEBOOK (Nov. 2018), https://www.facebook.com/crisisresponse/the-camp-fire-2018/support/; *see also How do I Mark Myself*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

as they fled the Camp Fire.[288] Video posted on the Internet was important as people sought evacuation routes while the Camp Fire raged. The *New York Times* reported, "In the age of the cellphone, another important investigative tool will be video. Many people turned on their phone cameras as they were escaping or as the fire was approaching their homes, and posted the video to social media."[289] "Investigators will be searching for the video, hoping to create a kind of composite from multiple sources, showing how the fire spread and which way smoke was moving at any given moment."[290]

D. The Social Internet as a Public Safety Platform

Onnok Oh, Manish Agrawal, and H. Raghav Rao observed that "[d]uring large-scale crises (e.g., natural disasters and terrorist attacks), it has become the norm that the incident is initially reported by a local eyewitness with a mobile communication device, the report is rapidly distributed through social media services, and mainstream media involvement follows."[291] They note that "online citizens have shown the potential of being first responders who can improvise an effective emergency response by leveraging their local knowledge, typically not available to professional emergency responders who are not familiar with the local community."[292] Locally-based first-responders may have community familiarity, but may face challenges in reaching people, as resources are overwhelmed and infrastructure fails in disasters, major fires, floods, hurricanes, and similar incidents.

Terrorism and mass shootings have also been accompanied by changing Internet use, including accounts from people trapped inside or near these crime scenes. Students at Marjorie Stoneman Douglas High School in Parkland, Florida

---

Safe or Ask if Someone Else Is Safe During a Disaster?, FACEBOOK, https://www.facebook.com/help/516656825135759?helpref=faq_content (last visited Feb. 11, 2019); *Crisis Response*, FACEBOOK, https://www.facebook.com/about/crisisresponse/ (last visited Feb. 10, 2019); Eric Ravenscraft, *How to Mark Yourself "Safe" On Facebook During an Emergency*, HOW TO GEEK (Sept. 7, 2017), https://www.howtogeek.com/324945/how-to-mark-yourself-safe-on-facebook-during-an-emergency/.

[288] *See Former Firefighter Films [as] He Evacuates Burning Paradise During Camp Fire*, ABC NEWS (Dec. 7, 2018), https://abc7news.com/video-former-firefighter-films-he-evacuates-burning-paradise-during-camp-fire/4853479/.

[289] Kirk Johnson, *What Started the California Fires? Experts Track the Blazes' Origins*, N.Y. TIMES (Nov. 15, 2018), https://www.nytimes.com/2018/11/15/us/camp-fire-paradise-cause.html.

[290] *Id.*

[291] Oh, Agrawal & Rao, *supra* note 179, at 408.

[292] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

posted photos, videos, and texts from inside their school during the 2018 shooting, and subsequently used the Internet as a means to organize and support each other as well as other shooting victims.[293]

The Internet has also facilitated the broadcast of criminal activity, as well as corrosive or fabricated comment and rumor. The mass shooter in New Zealand, who killed at least fifty people and wounded another fifty while they worshipped at two different Mosques, live-streamed his crime, and posted his manifesto on Twitter.[294] Social media platforms, already struggling to moderate content, floundered in dealing with monstrous uses of the Internet to broadcast crimes and massacres.

Such incidents require that we consider the possibility that a malicious actor will seek paid priority access to the Internet. My comments for the FCC *Internet Freedom* docket warned that some "people or organizations, whether domestic or foreign, may seek to buy or hack paid prioritization for nefarious, even criminal purposes."[295] If students inside Marjorie Stoneman Douglas High School faced delays due to ISP sale of Internet priority to others prior to the school shooting, they could have faced increased dangers.

ISPs paid priority sales in pursuit of new revenue streams makes public safety subject to ISP self-interested incentives. Government Petitioners' reply brief points out that the FCC had previously rejected reliance on the market to protect public safety. "The Commission has rejected analyses that risk the "subordination of important public policy objectives to market forces" because "public safety interests are not driven solely by economic considerations."[296] ISPs should not determine who

---

[293] *See* Abby Ohlheiser & Kayla Epstein, *Just Try to Keep Calm, How One Parkland Student's Phone became his Lifeline and his Voice*, WASH. POST (Mar. 3, 2018), https://www.washingtonpost.com/graphics/2018/lifestyle/parkland-shooting-in-social-media/?utm_term=.07ddba89af90; *see also* Brandon Griggs, *Hiding Under a Desk as a Gunman Roamed the Halls, a Terrified Student Live-Tweeted a School Shooting*, CNN (Feb. 15, 2018), https://www.cnn.com/2018/02/15/us/student-live-tweeting-florida-school-shooting-trnd/index.html.

[294] *See* Nelma Jahromi, *The New Zealand Shooting and the Challenges of Governing Live-Streamed Video*, NEW YORKER (Mar. 16, 2019), https://www.newyorker.com/tech/annals-of-technology/the-new-zealand-shooting-and-the-challenges-of-governing-live-streamed-video; *see also* Steve George, Joshua Berlinger, Hilary Whiteman, Harmeet Kaur, Ben Westcott & Meg Wagner, *New Zealand Mosque Terror Attacks*, CNN (Mar. 18, 2018), https://www.cnn.com/asia/live-news/live-updates-new-zealand-shooting-christchurch-terror-attack-intl/h_d3291a80387aac2a68b8f15b81930cb3.

[295] Sandoval, *Reply Comments*, *supra* note 5, at 26.

[296] Government Petitioners Reply Brief, *supra* note 242, at 5 (citing Facilitating the Deployment of Text-to-911, 29 FCC Rcd. 9846, ¶ 22 (2014)).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

has access to the Internet during crisis moments or everyday based on the ISP's revenue objectives and private deals.

The Internet has become an important means for people to share life-saving public safety information. The CPUC found in the 2016 Water-Energy Nexus proceeding I led as Assigned Commissioner that: "[v]oice communication is critical among first responders, communities, and during and after emergencies. Internet communication, maps, and video can be used to coordinate with first responders, fire teams including utilities, to protect people, property, infrastructure, watershed, and communities."[297]

The Internet provides a critical platform for public safety, democratic engagement, and accountability. Public safety Internet access is critical for the public using mass-market Internet access, as well as for public safety officials who may use commercial or enterprise plans, or mass market plans. Santa Clara County's Internet Freedom *ex parte* describes the extensive use of the Internet by its County Sheriff Department, Fire Protection District, and the public they serve.[298]

Santa Clara County informed the FCC that "County law enforcement also uses the internet to communicate critical inmate-release information to vulnerable victim populations through VineLink.com which provides victims with 'automated notifications about changes in custody status.'"[299] The system's efficacy "would be undermined if victims are unable to access this information due to blocking, throttling, or other interference with ready access," Santa Clara County warned.[300] California Penal Code 679.02 establishes the statutory rights of victims and witnesses to crimes to notification of inmate status and release. An ISP's Internet priority deal that delays crime victims' timely access to information undermines victims' statutory rights and the state's exercise of its police power to protect public safety and welfare.[301]

---

[297] CAL. PUB. UTIL. COMM'N, 16-12-047, DECISION UPDATING THE WATER ENERGY NEXUS COST CALCULATOR, PROPOSING FURTHER INQUIRY, AND NEXT STEPS 31 (2016).

[298] Santa Clara County, *Comment Letter*, *supra* note 19, at 6–7.

[299] *Id.* at 13.

[300] *Id.*

[301] *See* McKay Jewelers v. Bowron, 19 Cal. 2d 595 (1942) (noting the "police power" is an attribute of state sovereignty founded on the duty of the state to protect its citizens and provide for the safety and general welfare); *see also* Gonzales v. Oregon, 546 U.S. 243 (2006) (States have authority under the police power to "legislate with regard to protection of the lives, limbs health, comfort, and quiet of all persons.").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

Santa Clara County also relies on public access to the Internet to protect public health. To increase the efficacy and efficiency of its health-emergency alert system, "the County is transitioning to a web- and internet-based system . . . using the cloud-based MailChimp platform, including to individuals accessing the internet through home and small-business internet service plans."[302] The County has historically relied on "fax-based solutions" which "can take a day and a half to alert all providers of a developing situation."[303] Faxes are not well-suited to reach the general public, many of whom lack access to fax machines. The 2019 measles outbreak in Washington State led to a state declaration of emergency, while Oregon, New York, and other states also reported high numbers of measles cases.[304] Mass-market Internet resources are an important means to access and distribute information about contagions and other public health issues and emergencies. Santa Clara County warned that "[a]ll of these systems could be undermined by a reversal of the Net Neutrality Rules, as could development of additional systems to serve public safety and welfare."[305]

Rather than recognize the evolving nature of public Internet access to promote public safety, the *Internet Freedom Order* clung to its 2004 frame of the Internet and its then-existing regulatory system. The FCC ignored the Internet's evolution and the FCC's public safety duties, as well as state, tribal, and city and county duties to protect public safety. Some private sector companies such as the alarm industry also have public safety duties that could be hindered by ISP paid priority delays.[306] State and local laws impose legal duties on the alarm industry through service standards,

---

[302] Santa Clara County, *Comment Letter*, *supra* note 19, at 8.

[303] *Id.*

[304] *See* Julia Belluz, *Washington Declared a Public Health Emergency over Measles. Thank Vaccine-Refusing Parents*, VOX.COM (Jan. 29, 2019), https://www.vox.com/2019/1/27/18199514/measles-outbreak-2018-clark-county-washington; *see also* Ken Alltucker, *A Quarter of All Kindergartners in This County in Washington Aren't Immunized. Now There's a Measles Crisis*, USA TODAY (Feb. 11, 2019), https://www.usatoday.com/story/news/health/2019/02/11/measles-spread-anti-vaccination-communities-new-york-clar-county-washington/2812667002/.

[305] Santa Clara County, *Comment Letter*, *supra* note 19, at 13.

[306] Alarm Industry Communications Committee, Reply Comments on Restoring Internet Freedom 1, 5 (Aug. 30, 2017), https://ecfsapi.fcc.gov/file/108300232601598/AICC.NN%20Reply%20Comments.v6-FINAL.pdf [hereinafter Alarm Industry Communications, Reply Comments]; *see also* ADT Corp., Reply Comments on Restoring Internet Freedom 1, 3–4 (Aug. 30, 2017), https://www.fcc.gov/ecfs/filing/10830125808530.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

including maximum transmission time for an alarm signal to travel from the premises to the central monitoring station.[307]

The FCC's *Internet Freedom Order* concludes "that the light-touch approach that we adopt today, in combination with existing antitrust and consumer protection laws, more than adequately addresses concerns about Internet openness, particularly as compared to the rigidity of Title II."[308] The *Internet Freedom Order* fails to discuss the lessons of the Supreme Court's June 2017 decision in *Packingham v. North Carolina*, adopted six months before the FCC adopted its *2018 Order*.[309] In *Packingham*, the Court concluded that "[w]hile in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace—the 'vast democratic forums of the Internet' in general, and social media in particular."[310] "Seven in ten American adults use at least one Internet social networking service. One of the most popular of these sites is Facebook, the site used by petitioner leading to his conviction in this case."[311] The Court noted that "Facebook has 1.79 billion active users," measuring "three times the population of North America."[312]

John Bergmayer, counsel for the public interest organization Public Knowledge, commented in the Internet Freedom docket that "*Packingham* signals that the Court is likely to continue to protect the First Amendment rights of internet users."[313] The Electronic Frontier Foundation (EFF) cited *Packingham* for the proposition that the "meaningful exercise of our constitutional rights—including the

[307] *See* Alarm Industry Communications, Reply Comments, *supra* note 306, at 5.

[308] Restoring Internet Freedom, 83 Fed. Reg. 7852, 7880 (2018).

[309] *See* Packingham v. North Carolina, 137 S. Ct. 1730 (2017); *see also* Sandoval, *Reply Comments*, *supra* note 5, at 45 n.236 (citing Atlantic Richfield Co. v. USA Petroleum Co., 495 U.S. 328, 334 (1990) (holding that antitrust laws were intended to prevent and protect against "antitrust injury" "attributable to an anti-competitive aspect of the practice under scrutiny")); *see also* Reply Brief, Internet Association, *supra* note 25, at 12 (citing Br. of Professors of Admin., Commc'ns, Energy, Antitrust, and Contract Law and Policy 7–8) ("Consequently, antitrust laws are ill-suited to address harms to consumers, free speech, investment, and innovation in the net neutrality context.").

[310] *Packingham*, 137 S. Ct. at 1735 (citing Reno v. American Civil Liberties Union, 521 U.S. 844, 868 (1997)).

[311] *Id.* (citing Brief for Electronic Frontier Foundation et al. as *Amici Curiae* 5–6).

[312] *Id.* at 1735.

[313] John Bergmayer, Comment Letter, *supra* note 16, at 9.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

freedoms of speech, assembly, and press—has become dependent on broadband Internet access."[314]

Free Press cited *Packingham* to underscore the Supreme Court's recognition of the importance of the Internet to the First Amendment, and of its broadening role in American life. The *Packingham* court wrote, "[i]n the 21st century, access to the internet and particularly social media is the principle source for 'current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge.'"[315] The ACLU highlighted the Supreme Court's affirmation in *Packingham* that the Internet is the world's most important place for the exchange of viewpoints.[316] Twenty years earlier, the court in *Blumenthal v. Drudge* found that the Internet "enables people to communicate with one another with unprecedented speed and efficiency and has revolutionized how people share and receive information."[317]

While not specifically addressing public safety uses of the Internet by the public, *Packingham* recognizes a variety of speech in the modern public square facilitated through the Internet. *Packingham* comprehends that the Internet facilitates two-way and many-to-many dialogue, not just one-way downloads or information distribution from officials or institutions to consumers. Christine B. Williams, Jane Fedorowicz, Andrea Kavanaugh, Kevin Mentzer, Jason Bennett Thatcher, Jennifer Xu studied police use of the Internet using "agenda setting theory" to examine how police use horizontal media, such as social media, and vertical media, such as traditional mass media, to influence the public.[318] Their study found that "when using social media, public sector agencies generally and police departments in particular primarily disseminate information about their organizations and their activities, but rarely offer opportunities for engagement or what is also known as dialogic communication."[319]

Social media offers the opportunity to transcend one-way, asymmetrical communications. Videos from Camp Fire victims as they fled the fire and from Marjorie Stoneman Douglas students demonstrate the power of platforms that enable

---

[314] EFF Comments, *supra* note 16 (citing *Packingham*, 137 S. Ct. at 1737).

[315] Free Press Comments, *supra* note 16 (citing *Packingham*, 137 S. Ct. at 1737).

[316] ACLU Comments, *supra* note 16 (citing *Packingham*, 137 S. Ct. at 1737).

[317] *Id.* (citing Blumenthal v. Drudge, 992 F. Supp. 44, 48 (D.D.C. 1998)).

[318] Williams et al., *supra* note 27, at 213.

[319] *Id.* at 212.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

many-to-many communications to promote public safety. Rumor can plague many social media platforms, including those traded during urgent incidents.[320] ISP paid priority does not reduce rumor-spread, and may degrade access to communications platforms as ISPs and intermediaries with funds to pay for priority delay other communications.

The FCC failed to address *Packingham*'s observations or lessons in its *Internet Freedom Order*. Also absent from any discussion of public safety in the *Internet Freedom Order*,[321] is a failure to consider public safety uses in the vast public square *Packingham* recognized. This omission violates the FCC's statutory duties and the APA. Consistent with this Article's recommendations and my record comments highlighting the Internet's public safety role, the D.C. Circuit remanded the *Internet Freedom Order* to the FCC to analyze public safety, utility pole access, and Lifeline program access issues. Upon remand, the Commission must consider the public's role in public safety as part of the review of net neutrality rules to protect Internet openness. Doing so will require the Commission to change its paradigm of the role of the public use of the Internet and its conceptions about public safety responsibility.

E. The "Cat Video Paradigm"

This Article contends that the "cat video paradigm" frames FCC perceptions of public Internet use, obscuring the Internet's importance to public safety, critical infrastructure, energy, and democracy. The public's recreational use of the Internet such as cat video watching is a woefully incomplete model upon which to base broadband regulation and security models. The FCC's failure to consider public use of the Internet for public safety purposes manifests the cat video paradigm's prevalence and consequences.[322]

The D.C. Circuit's 2014 description of how the Internet works captures the Cat Video paradigm. The D.C. Circuit observed in *Verizon v. FCC*, "Internet users generally connect to these networks [Internet 'backhaul' networks composed of long-haul fiber-optic links and high-speed routers capable of transmitting vast amounts of data]—and, ultimately, to one another—through local access providers

[320] *See* Oh, Agrawal & Rao, *supra* note 179, at 408.

[321] Government Petitioners Reply Brief, *supra* note 242, at 4 (citing Resp. Br. 95–96).

[322] Catherine Sandoval, *Cybersecurity Paradigm Shift: The Risks of Net Neutrality Repeal to Energy Reliability, Public Safety, and Climate Change Solutions*, 10 SAN DIEGO J. CLIMATE & ENERGY 101, 176 (2019).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

like petitioner Verizon, who operate the 'last-mile' transmission lines."[323] ISPs operate those "last-mile" networks that provide access to the Internet, a network of networks. "When you connect to your ISP, you become part of their network. The ISP may then connect to a larger network and become part of their network. The Internet is simply a network of networks."[324]

Verizon v. FCC described the Internet's process in this way:

> To pull the whole picture together with a slightly oversimplified example: when an edge provider such as YouTube transmits some sort of content—say, a video of a cat—to an end user, that content is broken down into packets of information, which are carried by the edge provider's local access provider to the backbone network, which transmits these packets to the end user's local access provider, which, in turn, transmits the information to the end user, who then views and hopefully enjoys the cat.[325]

This cat video example demonstrates how Internet communications travel. It uses the example of a cat video loading since millions of people watch and post cat videos, finding them relaxing, and mood or energy boosters.[326]

The cat video paradigm, as echoed by the courts, FCC, and some parties, frames perceptions of the public's Internet content consumption. This frame obscures the

---

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

[324] Jeff Tyson, *How Internet Infrastructure Works*, HOWSTUFF WORKS, http://web.stanford.edu/class/msande91si/www-spr04/readings/week1/Howstuffworks.htm (last visited Oct. 21, 2018).

> Every computer that is connected to the Internet is part of a network, even the one in your home. For example, you may use a modem and dial a local number to connect to an Internet Service Provider (ISP). At work, you may be part of a local area network (LAN), but you most likely still connect to the Internet using an ISP that your company has contracted with.

Id.

[325] *Verizon*, 740 F.3d at 629.

[326] *See* Stephanie Pappas, *Why #OddlySatisfying Videos Are So . . . Satisfying*, LIVE SCIENCE (Mar. 22, 2018), https://www.livescience.com/62091-oddlysatisfying-videos-satisfying.html; *see also* Yvette Brend, *Cuteness Power, Why Watching Videos is Good for Your Brain, 'It's Not a Real Medicine but Cute Heals You,'* CBC (Apr. 30, 2017), https://www.cbc.ca/news/canada/british-columbia/cuteness-cute-kawaii-power-krigolso-uvic-joshua-dale-japan-1.3984970 ("An emerging Japanese school of thought, which revolves around the study of Kawaii or the quality of being cute, has found evidence that staring at cute things can boost mood and concentration by tapping into the same chemical reward system in the brain that makes cocaine addictive.").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

Internet's importance to public safety, critical infrastructure, education, health, the economy, and democracy. It distorts recognition of the public's centrality to public safety, government functions, and democracy. Each of these values increasingly depends on an open and neutral Internet.

The "cat video paradigm" bridges all of the categories Gamson and Lasch, and Gamson and Modigliani described.[327] It employs a metaphor to signify fun Internet content the FCC does not perceive as important or meriting regulatory protection for the category of uses and users. It provides an exemplar of the type of Internet content that influences regulatory, ISP, and public perceptions. The "cat video paradigm" evokes depictions and visual images. Unmasking this paradigm reveals the FCC's assumptions in the FCC's *2018 Internet Freedom Order* about the absence of an important public safety role for public use of mass-market broadband Internet. This frame ignores the public's role in public safety, in contrast to the FCC's *2015 Order*, which cited public safety as a reason to prohibit paid priority.[328] The APA requires heightened analysis of this change, an analysis the FCC's *Internet Freedom Order* fails to provide.

The FCC's 2018 decision to remove the prohibitions on paid Internet priority did not consider public use of mass-market Internet services, Broadband Internet Access Service (BIAS), for uses that impact public safety. My Reply Comments submitted for the *Internet Freedom* docket argues that allowing paid priority "would leave Americans needing remote health monitoring, as well as the American government, military, business, and all Americans, at risk of being outbid by others for Internet priority."[329] Without safeguards to ensure that other Internet users are not harmed by prioritization, paid priority allows ISPs to "deprioritize" the signals of other Americans, including those used for public safety, to speed ahead those who pay the ISP more for Internet priority.

[327] *See* Gamson & A. Modigliani, *supra* note 231; *see also* Gamson & Lasch, *supra* note 232.

[328] In the Matter of Protecting & Promoting the Open Internet, 30 FCC Rcd. 5601, 5654–55 n.291 (2015).

[329] *See* Sandoval, *Reply Comments*, *supra* note 5, at 27.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

IV. THE FCC NET NEUTRALITY REPEAL ORDER'S FAILURE TO ANALYZE PUBLIC SAFETY

A. The APA and the FCC's Founding Statute Require the FCC to Analyze Public Safety

1. The APA and the FCC's Statutory Mission to Protect Public Safety

This Section analyzes the FCC's failure to address public safety issues in its *2018 Internet Freedom Order*. The APA requires the FCC and any federal administrative agency conducting a rulemaking process to analyze factors embedded in its statutory mission or statutory mandates.[330] This legal requirement ensures that the agency adheres to its statutory mission and relevant statutory guidance while considering administrative decisions. Protecting public safety is one of the reasons the FCC was founded in 1934 and is a statutory factor the FCC must consider in its rulemakings.[331]

In 2006, the D.C. Circuit in *Nuvio Corp. v. FCC* held that the FCC must consider public safety in its rulemakings.[332] The Commission's enabling act, the Communications Act of 1934, requires the FCC to consider and advance public safety.[333] Congress founded the FCC to

> make available, so far as possible to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or sex, a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of promoting safety of life and property through the use of wire and radio communications.[334]

The Wireless Communication and Public Safety Act of 1999 requires the FCC to "encourage and support efforts by States to deploy comprehensive end-to-end emergency communications infrastructure and programs, based on coordinated

---

[330] Nuvio Corp. v. FCC, 473 F.3d 302, 307–08 (D.C. Cir. 2006) ("The Commission is required to consider public safety by both its enabling act, see Communications Act of 1934 § 1, 47 U.S.C. § 151 . . . and the Wireless Communications and Public Safety Act of 1999 § 3, 47 U.S.C. § 615.").

[331] *Id.*

[332] *Id.*

[333] Communications Act of 1934 § 1, 47 U.S.C. § 151 (2018).

[334] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

statewide plans, including seamless, ubiquitous, reliable wireless telecommunications networks and enhanced wireless 9-1-1 service."[335] The FCC's *2015 Order* cites this statutory mission to anchor its discussion of whether to classify broadband Internet services as a common carrier or information provider service.[336]

My comments to the FCC for its *2018 Internet Freedom* docket emphasized the importance of the FCC's statutory public safety mission.[337] The FCC was founded when interference was rampant on the airwaves. Lack of centralized control or regulation lead to "confusion and chaos."[338] "With everybody on the air, nobody could be heard," the Supreme Court observed in *National Broadcasting Co. v. United States*[339] Discussing the rationale for regulation of broadcast spectrum the Supreme Court in 1969 *Red Lion Broadcasting Co. v. FCC*, observed "[w]ithout government control, the medium would be of little use because of the cacophony of competing voices, none of which could be clearly and predictably heard."[340]

My *Internet Freedom* Reply Comments warned that the "FCC's proposal to remove both its rules and jurisdiction over ISPs would create a cacophony on the Internet, allowing those who can pay for priority to push ahead of others so only those with priority can be heard."[341] The FCC proposed and adopted no rules to safeguard other Internet users from delays due to paid priority sold to others, or from blocking, throttling, or network management practices adopted in the ISP's business interest.[342] "This cyber-Mad Max version of the Internet would allow those with paid or hacked priority to push other Internet communications to the back of the line or make their connection attempts fail. This is the type of communications dystopia the FCC was founded to prevent," my Reply Comments observed.[343] The FCC *Internet Freedom Order*'s failure to analyze the implications of its proposals for public safety fails to execute its statutory charge and violates the APA.

---

[335] 47 U.S.C. § 615.

[336] In the Matter of Protecting & Promoting the Open Internet, 30 FCC Rcd. 5601, 5734–35 (2015).

[337] *See, e.g.*, Sandoval, *Reply Comments*, *supra* note 5, at 55, 57.

[338] *Id.* at 57.

[339] *Id.* (citing Nat'l Broadcasting Co. v. United States, 319 U.S. 190, 212 (1943)).

[340] *Id.* (citing Red Lion Broadcasting Co. v. FCC, 395 U.S. 367, 376 (1969)).

[341] *Id.*

[342] Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 7, at 4 n.7.

[343] *See, e.g.*, Sandoval, *Reply Comments*, *supra* note 5, at 57.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

"[C]omplete absen[c]e of any discussion of a statutorily mandated factor renders an agency decision arbitrary and capricious."[344] The Government Petitioners in the *Mozilla v. FCC* appeal of the *Internet Freedom Order* argued that the *Order* is "arbitrary and capricious because it failed to reconcile the Commission's abdication of regulatory authority with the inevitable harms that the *Order* will cause to consumers, public safety, and existing regulatory schemes."[345] Government Petitioners emphasize that the *Internet Freedom Order* "entirely ignored many of these issues, including public safety, in violation of the agency's statutory mandate."[346] Government Petitioners argue that the FCC fell short of its statutory duties to protect public safety and consider important issues under the APA. "In evaluating the impact of these changes, the Commission did not perform any analysis of the public safety risks that several parties (including Government Petitioners) had identified in the record, despite its statutory mandate to consider such safety concerns."[347]

"There's no real dispute that the FCC has a statutory mandate to consider public safety. 47 U.S.C. § 151 tells us this is one of the reasons that the agency exists," said Danielle Goldstein, counsel for Santa Clara County, who argued on behalf of the Government Petitioners in the February 1, 2019 *Mozilla v. FCC* oral argument.[348] "There's also no real dispute that commenters on this record raised the prospect of harms to public safety that if realized, could cause damage to property of loss of life. In the event that, for example, a person doesn't receive a timely evacuation order or shelter-in-place order."[349] "The FCC did not address this evidence—didn't even mention it. And so, the only real dispute here is whether an order that completely fails to mention the harms to public safety, much less include them in its analysis, can meet the FCC's statutory obligation to consider public safety."[350]

FCC Attorney Tom Johnson argued in the net neutrality oral argument that the FCC's permission for paid priority would, among other things, potentially benefit

[344] Pub. Citizen v. Fed. Motor Carrier Safety Admin., 374 F.3d 1209, 1216 (D.C. Cir. 2004) ("[T]he final rule is arbitrary and capricious because the agency neglected to consider a statutorily mandated factor.").

[345] Brief for Government Petitioners, Mozilla v. FCC, 18-1051 at 2.

[346] *Id.*

[347] *Id.* at 6.

[348] Mozilla v. FCC Oral Argument, *supra* note 30, at 1:42:51.

[349] *Id.*

[350] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

public safety officials who might want "dedicated networks."[351] This argument confuses the effects of the net neutrality repeal. The *2015 Order* rules did not apply to enterprise services which some public safety agencies, businesses, and governments use.[352] The 2015 net neutrality rules applied to mass-market broadband Internet access ("BIAS").[353] The *2018 Internet Freedom Order* allows ISPs to engage in paid priority that may prefer or degrade traffic using mass-market Internet.

Goldstein, arguing for Government Petitioners at the *Mozilla v. FCC* oral argument, underscored the importance of ensuring that those dependent on mass-market Internet access are not subject to blocking, throttling, or degraded access due to paid priority for others. She emphasized that those using mass-market services are either giving information to the public entity or getting public safety information, such as information about vaccines during a flu pandemic.[354] People in the path of a flood, fire, or danger, and those helping them including community responders, should be enabled to prepare for and respond to disaster and urgent incidents through a Whole Community approach, supported by an open Internet.

The examples of the San Jose flood and the Oroville dam's spillway failure in 2017, the evacuations required by these incidents, and the work to address their aftermath illustrate the importance of the open Internet and mass-market Internet services for public safety. The Anderson Dam above San Jose, California, the tenth largest city in America, overflowed after several heavy rainstorms, leading to flooding on February 21, 2017, as the Santa Clara Valley Water District diverted water into the Coyote Creek to prevent the dam from failing.[355] The ensuing flood inundated neighborhoods near the normally dry creek, causing more than 14,000 people to evacuate, some through boats sent by the San Jose fire department, and causing $100 million in damage.[356] A year after the flood, the City of San Jose "now has 2 alert systems available, including one similar to an amber alert, which can automatically be sent to cell phones in a specified area. The city also bought portable

[351] *Id.* at 3:24–3:25.

[352] In the Matter of Protecting & Promoting the Open Internet, 30 FCC Rcd. 5601, 5610 (2015).

[353] *Id.* at 5609–10.

[354] Mozilla v. FCC Oral Argument, *supra* note 30, at 4:17:10.

[355] Maureen Naylor, *Changes Made Since San Jose's Coyote Creek Flood*, FOX KTVU (Feb. 21, 2018), http://www.ktvu.com/news/changes-made-since-san-joses-coyote-creek-flood; *see also New Flood Evacuation Orders Issued in San Jose*, CBS KPIX (Feb. 21, 2017), https://sanfrancisco.cbslocal.com/2017/02/21/rescue-crews-pull-residents-from-flooded-homes-in-south-san-jose/.

[356] Naylor, *supra* note 355.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

speakers so crews could drive through neighborhoods and make announcements in several languages."[357] A week before the San Jose flood, damage to the Oroville Dam's spillway led to the evacuation of 188,000 residents near Oroville, California "after a hole in an emergency spillway in the Oroville Dam threatened to flood the surrounding area."[358]

In response to the Oroville and San Jose evacuations, I volunteered to assist state and local efforts to deal with these disasters, using my knowledge about telecommunications, regulation, water services, vulnerable, and diverse communities. During those two weeks, I used my personal mobile phone, which uses a mass-market plan that offers data and the ability to call phone numbers in the North American Numbering Plan. I was often away from Wi-Fi and wired networks during that time due to attending conferences and meetings. I relied on my phone's wireless connection for data access. I frequently monitored the river gauges in Coyote Creek, made accessible online by the National Weather Service and supported by the Santa Clara Valley Water District I was volunteering to assist.[359] I also watched video about these two flood incidents to formulate recommendations to public safety officials and water agencies dealing with these emergencies. My term as a CPUC Commissioner had ended the month before and I was teaching full-time as Law Professor at Santa Clara University, so I was using my personal phone that depends on a mass-market plan, and not any enterprise account. While I was glad to assist my community in addressing these public safety emergencies, I also ended up with a very high phone bill due to that month's data usage.

Had I been watching the ISP's favored content, instead of public safety information about floods, I would not have received a very high bill. Professor Tim Wu in 2007 identified "as examples of net neutrality violations having little, if any, public safety and welfare justifications" ISP conduct including "[c]reating 'walled

[357] *Id.*

[358] Samantha Schmidt, Derek Hawkins & Kristine Phillips, *188,000 Evacuated as California's Massive Oroville Dam Threatens Catastrophic Floods*, WASH. POST (Feb. 13, 2017), https://www.washingtonpost.com/news/morning-mix/wp/2017/02/13/not-a-drill-thousands-evacuated-in-calif-as-oroville-dam-threatens-to-flood/?utm_term=.0235239e708b.

[359] *See, e.g.*, *Coyote Creek at Edenvale*, NAT'L WEATHER SERV., https://water.weather.gov/ahps2/river.php?wfo=mtr&wfoid=18782&riverid=204570&pt%5B%5D=143421&allpoints=143421%2C152540%2C152541%2C152542%2C152546%2C152547%2C152548%2C153680%2C153688&data%5B%5D=hydrograph&data%5B%5D=impacts&data%5B%5D=stage&data%5B%5D=flow (last visited Feb. 20, 2019).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

garden' access to favored video content of affiliates and partners."[360] My use of data to watch river gauges during a flood, and video of two dams to assist public safety put me on the wrong side of the ISP's walled garden of favored content that would have been exempt from their data cap.

Recognizing the concern about ISP practices that disadvantage certain Internet content while favoring ISP-chosen content, the *2015 Order* "gave the FCC the jurisdiction and rules to consider a complaint that an ISP unreasonably interfered with and disadvantaged public safety data transmissions—whether GIS mapping or live video of a fire or flood's path."[361] The no unreasonable interference rule, also known as the "general conduct rules," addresses circumstances where the ISP would not have slowed a commensurate amount of data "had the user been watching an ISP's 'zero-rated' entertainment video exempt from ISP data caps."[362]

At the *Mozilla v. FCC* oral argument, the ISP coalition's attorney argued against the *2015 Order*'s "general conduct rule" that prohibited unreasonable interference with and disadvantage to broadband access, arguing that sponsored data plans should be permitted.[363] This argument does not take into account the effect of sponsored data caps on public safety uses of the Internet. Had users watched the ISP's favored entertainment programming instead of river gauges, video relevant to rising flood waters, and exigent public safety dangers, they would not have been subject to high ISP charges for exceeding data caps.

Some ISPs slow consumers who have high data usage during the course of a month. This practice can make mapping or other applications such as video

---

[360] Rob Frieden, *Hold the Phone: Assessing the Rights of Wireless Handset Owners and Carriers*, 69 U. PITT. L. REV. 675, 688–89 (2008) (citing Tim Wu, *Wireless Carterfone*, 1 INT'L J. COMM. 389 (2007) (identifying examples of net neutrality violations having little, if any, public safety and welfare justifications including handset locking; using firmware "upgrades" to "brick," *i.e.*, render inoperative, the handset or alternatively disable third party firmware and software; disabling handset functions; specifying formats for accessing memory, e.g., music, ringtones, and photos; creating "walled garden" access to favored video content of affiliates and partners; and using proprietary, non-standard interfaces making it difficult for third parties to develop compatible applications and content)).

[361] *Amici Brief, Professors of Administrative, Communications, Energy, Contract Law, and Policy*, *supra* note 5, at 12; *see also* In the Matter of Protecting & Promoting the Open Internet, 30 FCC Rcd. 5601, 5728–29, 5885 (2015) (imposing a no unreasonable interference/disadvantage standard to ensure that broadband providers do not engage in practices that threaten the open nature of the Internet in other or novel ways).

[362] *Amici Brief, Professors of Administrative, Communications, Energy, Contract Law, and Policy*, *supra* note 5, at 12.

[363] Mozilla v. FCC Oral Argument, *supra* note 30, at 4:02:00–4:02:25.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

conferencing unusable. In 2015, the FCC fined AT&T $100 million for violations of the 2010 transparency rules for slowing customers on "unlimited" data plans to speeds where mapping and other common applications would not work.[364]

In July 2017, Verizon slowed the Santa Clara Fire Protection District's data when the District was fighting the Mendocino Complex fire—California's largest fire.[365] During this slowdown, Fire District personnel appealed to Verizon to stop the severe data slowdown for a device in active use to help coordinate fire resources.[366]

"Throttling means that the device that can normally act like a modern broadband internet connection is slowed to the point of acting more like an AOL dial up modem from 1995," the Fire Chief Reported.[367] Verizon demanded that the Fire Department switch to a plan that costs $2.00 a month more to stop the throttling, an unfathomable demand to a fire department using the Internet during an active firefight. Fire Department personnel could not readily authorize additional payments for the requested $2.00 per month upcharge in light of government contracting rules. Verizon's service slowdown turned the Internet calendar back to the dial-up days in the midst of a public safety emergency. Throttling left firefighters unable to use data connections that require more than dial-up speeds to acquire information and coordinate their firefighting response. Verizon's demand for $2.00 a month more to restore modern Internet speeds and provide "unlimited" service that the plan advertised[368] pulled public servants off the front lines of crisis management to battle the ISP's demands for a higher-priced plan. The ISP's technical ability and willingness to slow down the fire department's Internet use during California's largest firefight highlight the ISP's gatekeeper role, and the need for regulation to constrain ISP abuse of that bottleneck position.

Verizon subsequently apologized for its conduct and promised not to throttle after declared disasters.[369] The disaster declaration trigger for cessation of throttling leaves people vulnerable to throttling during a disaster or exigent situation. Disaster declarations often take time to issue, ranging from days or weeks for a gubernatorial disaster declaration to months or longer for a presidential disaster declaration, neither

[364] In the Matter of AT&T Mobility, LLC., 30 FCC Rcd. 6613 (2015).

[365] Addendum to Brief for Government Petitioners, Mozilla Corp. v. FCC, No. 18-1051 (Aug. 20, 2018).

[366] *Id.* appx. A, 11.

[367] *Id.*

[368] *Id.*

[369] *See infra* notes 534–37 and accompanying text.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

of which is guaranteed.[370] Verizon's promise leaves the public vulnerable to throttling that may not end for days, weeks, or months after a declared disaster, and may not cease or pause if no government official declares a disaster.

The prospect of an ISP throttling or degrading mass-market Internet users in favor of paid priority raises concerns about the impact of such practices on public safety. The amicus brief of Professors of *Administrative, Communications, Energy and Contract Law and Policy* argues that the FCC had a duty to consider these public safety risks before lifting the ban on paid priority, blocking, and throttling, and removing the proscription of unreasonable interference with or disadvantage to Internet traffic.[371]

When drafting the *2015 Order*, the FCC was critical of ISP treatment of users with unlimited plans. The FCC noted that "significant concern has arisen when mobile providers have attempted to justify certain practices as reasonable network management practices, such as applying speed reductions to customers using 'unlimited data plans' in ways that effectively force them to switch to price plans with less generous data allowances."[372] If the D.C. Circuit vacates the *Internet Freedom Order*, on remand the FCC should examine the public safety risks of ISP slowdowns of Internet public safety use, including that by public safety agencies, first-responders, and the public.

The CPUC expressed concern regarding the FCC's proposals to remove net neutrality rules in its comments submitted for the *Internet Freedom* docket. The CPUC emphasized that "as the *2015 Order* discusses, the absence of strong anti-discriminatory rules could undermine critical infrastructure and public safety."[373] "For example, without non-discriminatory rules, providers of emergency services or public safety agencies might have to pay extra for their traffic to have priority."[374] "If states, cities, and counties were required to pay for priority access, their ability to

---

[370] *See* FEMA, The Disaster Declaration Process, Jan. 8, 2018, https://www.fema.gov/disaster-declaration-process (describing the presidential disaster declaration process under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. §§ 5121–5207 (the Stafford Act) § 401).

[371] *Amici Brief, Professors of Administrative, Communications, Energy, Contract Law, and Policy*, *supra* note 5, at 10–11.

[372] In the Matter of Protecting & Promoting the Open Internet, 30 FCC Rcd. 5601, 5639–40 (2015).

[373] *CPUC*, *Comments*, *supra* note 23, at 28–29.

[374] *Id.* at 29.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

provide comprehensive, timely information to the public in a crisis could be profoundly impaired."[375]

The CPUC emphasized that "a free and open Internet is critical to areas such as energy, education, medicine, and public safety. Given the importance of an open Internet in our society, strong non-discriminatory net neutrality rules are necessary to ensure consumers can enjoy unfettered access to the Internet."[376] The CPUC observed that "broadband transmission facilities present the most likely bottlenecks that could be used to effectively limit consumer choice among content, applications, services, and devices."[377]

Santa Clara County discussed in the *Internet Freedom* proceeding record several public safety risks raised by removing protections for the public Internet. Open access to mass-market Internet services is important to public receipt of the notices from Santa Clara County's Office of Emergency Services and its "AlertSCC" which requires broadband internet service to provide these potentially "life-saving warnings to residents of Santa Clara County."[378] Santa Clara County also relies on the Internet to provide patients served by its county health care centers to access their medical records, schedule appointments, and find health information. Access to personal health information and arranging "for medicine delivery or medical treatment depends on the availability of accessible and affordable broadband internet service."[379]

Santa Clara County fosters justice in its criminal adjudication system by permitting Internet-enabled "at-home electronic monitoring systems" that "allow individuals to live at home, maintain their family relationships, continue employment, attend school or vocational programs, and participate in treatment

[375] *Id.* (citing *Protecting & Promoting the Open Internet*, 30 FCC Rcd. at 5653–55 (noting commenters' concerns about paid prioritization and citing to an *ex parte* letter from then-CPUC Commissioner Catherine Sandoval, "asserting that paid prioritization undermines public safety and universal service. . . .")).

[376] *Id.* at 27.

[377] *Id.* (citing *CPUC*, *Comments*, *supra* note 23, at 5; In the Matter of Preserving the Open Internet et al., GN Docket No. 09-191, WC Docket No. 07-52, Notice of Proposed Rulemaking (filed Apr. 26, 2010)).

[378] Santa Clara County, Reply Comments on In the Matter of Restoring Internet Freedom (Aug. 30, 2017), https://ecfsapi.fcc.gov/file/1083040730347/Reply%20Comments%20of%20the%20County%20of%20Santa%20Clara%20with%20TOC.pdf.

[379] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

programs."[380] Santa Clara County emphasized that these "internet-based electronic monitoring programs allow the County to ensure public safety while also providing innovative options for at-home supervision."[381]

Several parties in the alarm industry raised concerns in the *Internet Freedom* record that repealing net neutrality rules would allow ISPs to compromise public safety by disfavoring the traffic of independent alarm companies. The Alarm Industry Association's Reply Comments emphasized the public safety duties of alarm companies, arguing that repealing net neutrality rules would put compliance with these duties and public safety at risk. "Alarm companies have an obligation to their customers to make sure that alarm signals are processed and delivered in a timely manner."[382] The Alarm Industry Association argued that "ADT is correct in its observation that, '[a]bsent protections, broadband providers would be free to block a particular alarm service provider's messaging content and to discriminate amongst competing alarm service providers.'"[383]

In addition to concerns about blocking, the Alarm Industry Association expressed concern that "[p]aid-prioritization schemes can result in similar harm, where alarm transmissions are de-prioritized, degraded, or interrupted, running contrary to the Commission's statutory obligation to promote network development to support public safety."[384] "In emergency situations, seconds could mean the difference between life and death. Allowing paid-prioritization schemes to de-prioritize non-affiliated alarm traffic in favor of other applications would flatly contradict the Commission's duty to the public interest."[385]

Notwithstanding the statutory "mandate to consider public safety and record evidence showing substantial public safety concerns associated with abusive BIAS [Broadband Internet Access Services] provider practices that violate open Internet principles but are permitted by the [2018 Internet Freedom] *Order*, the Commission did not consider public safety at all," Government Petitioners observed.[386] "[T]he

[380] *Id.* at 6–7.

[381] *Id.* at 7.

[382] Alarm Industry Communications, Reply Comments, *supra* note 306.

[383] *Id.*

[384] *Id.*

[385] *Id.*

[386] Brief for the Government Petitioner, *supra* note 345, at 22.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

complete absen[c]e of any discussion of a statutorily mandated factor" renders the *Order* arbitrary and capricious, Government Petitioners emphasized.[387]

A coalition of ISPs and industry associations in support of Respondents in the *Mozilla v. FCC* case argued that the *Internet Freedom Order* complied with the FCC's statutory duty to analyze the public safety implications of its rulemaking.[388] Intervenors patch together this argument by inserting words into the FCC's Order that do not exist.

Intervenor ISPs argue that the FCC "reasonably concluded that there was 'scant evidence' of threats to public safety."[389] Government Petitioners' Reply Brief retorts that the *Internet Freedom Order* does not support the parties' citation. "Intervenors insert the words 'public safety' into the *Order*'s discussion of 'scant evidence that end users, under different legal frameworks, have been prevented by blocking or throttling from accessing the content of their choosing,'" Government Petitioners report, a legal sleight of hand the D.C. Circuit recognized as not addressing the public safety consequences of net neutrality appeal.[390] The footnote associated with that sentence, note 980, does not even mention public safety, nor does the footnote the ISP intervenor's brief cited, footnote 978.[391] The FCC's Order as published by the

[387] *Id.* (citing Public Citizen v. Fed. Motor Carrier Safety Admin., 374 F.3d 1209, 1216 (D.C. Cir. 2014)); *see also id.* at 24 ("[T]he Order's total silence on the issue of public safety is arbitrary and capricious.").

[388] Joint Brief for Intervenors USTELECOM, CTIA, NCTA, ACA, and WISPA In Support of Respondents at 35–36, Mozilla v. FCC, No. 18-1051 (Oct. 18, 2018) [hereinafter ISP Intervenor Brief].

[389] *Id.* (citing In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311, 468 (2018)).

[390] Government Petitioners Reply Brief, *supra* note 242, at 5 (citing *Restoring Internet Freedom*, 33 FCC Rcd. at 468 (2018)); *Mozilla*, ___ F.3d at 99.

[391] As Judges Williams and Silberman have pointed out, proponents of utility-style regulation have pointed to "astonishing[ly]" few incidents that involved the blocking of content or applications. *USTelecom*, 825 F.3d at 762 (Williams, J., dissenting); Verizon v. Federal Commc'n Comm'n, 740 F.3d 623, 664–65 (D.C. Cir. 2014) (Silberman, J., dissenting). *See supra* paras. 110–15; TechFreedom Reply at 85–86 ("[E]xamples of an ISP actually blocking a competitive application/service from accessing its last-mile network are remarkably few."); Massillon Cable Comments at 7; AT&T Comments at 11; *infra* Part VI.B. We reject the argument that the blocking of alarm signals alleged by ADT justifies a no-blocking rule, because it is unclear if the blocking was intentional and the blocking was resolved informally. *See* Letter from Michael H. Pryor, Counsel for ADT, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 17-108, Attach. at 3 (filed Oct. 11, 2017). *Id. See also id.* n.978. *See, e.g.*, Letter from City of Santa Clara, CA & Santa Clara County Central Fire Protection District to Marlene H. Dortch, Secretary, FCC, WC Docket No. 17-108 (filed Dec. 6, 2017); Letter from Robb Davis, Mayor, City of Davis, CA to Ajit Pai, Chairman, FCC, WC Docket No. 17-108 (filed Dec. 6, 2017); Letter from Governor Jay Inslee, State of Washington, to Chairman Pai, FCC, WC Docket No. 17-108 (filed Dec. 6, 2017). *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

FCC in January 2018 belies ISP intervenor's attempts to shoehorn words into the Order that do not exist.

My first-year law students would recognize that asserting to a court-invented text nonexistent in the Government's Order is wholly inconsistent with the legal profession's standards. Neither does it fulfill a lawyer's duties or the APA to argue that invented text indicates that the Government complied with the rule requiring the government to articulate its analysis of that topic. It is shocking that lawyers of such caliber would proffer this insertion of imagined text. Those lawyers represent ISPs arguing that the D.C. Circuit should sustain the *Internet Freedom Order* and allow their clients to manage public Internet access without FCC rules prohibiting blocking, throttling, paid priority, and unreasonable interference with or disadvantage to Internet traffic. These lawyers do their clients, the American public, and the court a disservice in asserting facts absent from the FCC's Order. Analysis imagined by the ISPs or its lawyers does not substitute for the FCC's required analysis of public safety under the APA and the FCC's statutory charge.

ISP Intervenors then contend that the FCC concluded that as a result of its Order, "States could 'continue to play their vital role' in advancing public safety."[392] Governor Petitioners reply that "[i]ntervenors misrepresent the *Order* as permitting States to 'continue to play their vital role' in advancing public safety" by referencing a portion of the *Order* discussing state regulation of consumer protection and unfair business practices, topics the D.C. Circuit noted do not address public safety.[393]

Intervenors contend that the FCC adequately discussed public safety when through its dismissal in footnote 943 of the national security concerns about paid priority my reply comments raised. Footnote 943 states without analysis that "any national security concerns raised were vague and lack any substantiation whatsoever."[394] This Article discusses *infra* notes 461 through 466 the FCC's failure to analyze the record that substantiated the national security concerns my Reply Comments raised. Government Petitioners argue that this portion of the *Order* is irrelevant to Government Petitioners' public safety concerns, and the D.C. Circuit agreed that the FCC's cursory dismissal "says nothing about the multi-faceted public

---

[392] ISP Intervenor Brief, *supra* note 388, at 37 (citing *Restoring Internet Freedom*, 33 FCC Rcd. at 428–29 n.737).

[393] Government Petitioners Reply Brief, *supra* note 242, at 6 (citing ISP Intervenor Brief, *supra* note 388, at 37 (quoting *Restoring Internet Freedom*, 33 FCC Rcd. at 428–29)); *Mozilla*, ___ F.3d at 100.

[394] ISP Intervenor Brief, *supra* note 388, at 37 (citing *Restoring Internet Freedom*, 33 FCC Rcd. at 462–63 n.943).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

safety concerns associated with subjecting emergency services providers, other public health providers, and members of the public who depend on those services to paid prioritization and blocking and throttling."[395] The D.C. Circuit remanded the FCC's *Internet Freedom Order* in light of the Commission's failure to analyze "the direct and specific comments by Santa Clara County, former California Public Utility Commissioner Sandoval, and others" that "repeatedly raised substantial concerns about the Commission's failure to undertake the statutorily mandated analysis of the 2018 Order's effect on public safety."[396]

Intervenors cite the *Internet Freedom Order*'s conclusion that "any remaining unaddressed harms" about paid priority were "small relative to the costs of implementing more heavy-handed regulation."[397] The D.C. Circuit concluded that this "Rorschachian speculation is hardly the focused and specific study of public safety implications that the law requires."[398] "Nothing in this provision links it to public safety," Government Petitioners emphasize.[399]

"Moreover, claiming the Commission considered public safety as an 'unaddressed' harm recognizes the Commission's failure to meet its obligation to 'explicitly acknowledge' the issue under the APA as required by *American Trading Transp. Co. v. United States*."[400] Intervenors' attempts to insert public safety into the text do not substitute for the FCC's failure to carry out its statutory duty to address public safety, and the APA's requirements to address the reasons for the agency's changed position and the record before the agency.[401] A "court may uphold agency action only on the grounds that the agency invoked when it took the action."[402]

---

[395] Government Petitioners Reply Brief, *supra* note 242, at 6.

[396] *Mozilla*, ___ F.3d at 96–97. *See also* Sandoval, *Reply Comments*, *supra* note 5, at 25, 41, 47, 49, 50; *see also* Brief for Government Petitioners, *supra* note 345, at 23 (citing CATHERINE J.K. SANDOVAL, WRITTEN STATEMENT 34–35 (2014)) [hereinafter *Sandoval Net Neutrality September 2014 Testimony*].

[397] ISP Intervenor Brief, *supra* note 388, at 37 (citing *Restoring Internet Freedom*, 33 FCC Rcd. at 378).

[398] *Mozilla*, ___ F.3d at 100. *See also* Government Petitioners Reply Brief, *supra* note 242, at 6 (citing ISP Intervenor Brief, *supra* note 388, at 37) (quoting *Restoring Internet Freedom*, 33 FCC Rcd. at 378).

[399] *Id.*

[400] *Id.* (citing Am. Trading Transp. Co. v. United States, 791 F.2d 942, 949 n.7 (D.C. Cir. 1986)).

[401] *American Trading*, 791 F.2d at 949 n.7; *see also* Nuvio Corp. v. FCC, 473 F.3d 302, 307 (D.C. Cir. 2006); 47 U.S.C. § 151 (2018); *see also* 47 U.S.C. § 615 (2018).

[402] Michigan v. EPA, 135 S. Ct. 2699, 2710 (2015) (citing SEC v. Chenery Corp., 318 U.S. 80, 87 (1943)); *see also* Perez v. Mortg. Bankers Ass'n, 135 S. Ct. 1109, 1209 (2015) (quoting Fox Television Stations, Inc. v. FCC, 556 U.S. 509, 515 (2009)).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

Danielle Goldstein argued at the *Mozilla v. FCC* oral argument on behalf of the Government Petitioners that "Respondents' basic contention is that the FCC wasn't obligated to specifically address public safety as the record reflects no distinct issues that are unique to public safety. So, in other words, because the Commission considered the competitive harms to Netflix, it adequately considered the loss of life or property in the public safety context."[403] She emphasized that the FCC and DOJ "don't cite any case law for the proposition that the FCC can duck public safety in this way, and Congress of course delegated to the expert agency, not appellate counsel, the responsibility for weighing and evaluating public safety harms. So, it's not a proper defense of the Order."[404]

"But it's also an inaccurate characterization of the record. Commenters on this record did point to distinct issues that relate to public safety, Goldstein emphasized, and the D.C. Circuit recognized as the basis for its public safety remand my comments about the importance of the open Internet to energy management, natural gas leak detection, and fire safety and prevention.[405] The APA requires the FCC to articulate its analysis of its statutory duties, the rationale for and facts supporting changes from previous decisions, and discuss its consideration of the record in the proceeding before the Commission.

The FCC must argue its position in an intelligible and communicative way to satisfy its duty to make reasoned decision-making. Public safety factored into the *2015 Order* and its public comment and record.[406] The *2015 Order*'s protection of public safety generated reliance on rules protecting investments in the open Internet, such as those investments made by Santa Clara County and the CPUC. "An agency cannot ignore its prior factual findings that contradict its new policy nor ignore reliance interests."[407] The Commission's claims that no public safety interest is raised is wholly conclusory and contradicted by the record. Cursory footnotes that do not examine the issues raised are not a substitute for required legal analysis under the APA. "[A]n agency changing its course must supply a reasoned analysis indicating that prior policies and standards are being deliberately changed, not

[403] Mozilla v. FCC Oral Argument, *supra* note 30, at 1:46:55.

[404] *Id.*

[405] *Id.*; *Mozilla*, ___ F.3d at 95.

[406] In the Matter of Protecting & Promoting the Open Internet, 30 FCC Rcd. 5601, 5609, 5654–55 (2015).

[407] Nat'l Lifeline Ass'n v. FCC, 915 F.3d 19, 28 (D.C. Cir. 2019) (citing *Fox Television*, 556 U.S. at 502, 515–16).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

casually ignored, and if an agency glosses over or swerves from prior precedents without discussion it may cross the line from the tolerably terse to the intolerably mute."[408] The substantive change in policy, fundamental to the very fabric of the *2015 Order*, requires publication of the FCC's detailed analysis to support its decision in the *2018 Order*.

An agency's repeal of policy or interpretation is required to be published in the Federal Register:

> Each agency shall separately state and currently publish in the Federal Register for the guidance of the public . . . (d) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; and (e) each amendment, revision, or repeal of the foregoing.[409]

An essential part of an agency's repeal of a policy is the substantive reasoning for the agency's decision. Absent a publication of their reasoning, an agency's actions should not be given force of law.[410]

One purpose of notice and comment rulemaking is to allow the public to participate in the democratic development of policy, and shape the agency's rulemaking to ensure its effectiveness.[411]

> [A]n agency which is required to respond to the material data it has received from the public and to provide some public demonstration of its deliberative process will have a strong incentive to examine its data carefully, to identify and discard irrelevant, redundant, or erroneous information, and to develop a logical and coherent rationale for its ultimate decision.[412]

---

[408] Greater Boston Television Corp. v. FCC, 444 F.2d 841, 852 (D.C. Cir. 1970).

[409] 5 U.S.C. § 552(a)(1) (2012).

[410] Fertilizer Inst. v. EPA, 935 F.2d 1303, 1312 (D.C. Cir. 1990) ("[W]hen a regulation is not promulgated in compliance with the APA, the regulation cannot be afforded the 'force and effect of law.'") (quoting Chrysler Corp. v. Brown, 441 U.S. 281, 313 (1979)).

[411] *See* Cooley R. Howarth, Jr., *Informal Agency Rulemaking and the Courts: A Theory for Procedural Review*, 61 WASH. U. L.Q. 891, 899 (1984).

[412] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

The *2015 Order* and public comment process for the Internet Freedom docket established that public safety represented a serious reliance interest the Commission needed to consider in its repeal of net neutrality protections.[413] Footnotes dismissing national security interests without legal analysis, and failure to consider the public safety interests in the Open and neutral Internet mute critical topics through the silent treatment.[414] The FCC's cavalier dismissal of national security interests, and absence of discussion of the public's use of the Internet for public safety does not satisfy the APA's rigorous demands for publishing the agency's reasoned decision-making in the Federal Register.

To the extent that the FCC or intervenors rely on footnotes in the FCC's January *2018 Internet Freedom Order* published in order to support arguments that it complied with the APA, the FCC's February 22, 2018 publication of the Restoring Internet Freedom Final Rule in the Federal Register without footnotes undercuts the FCC's legal ability to rely on footnotes to support required analysis.[415] As the D.C. Circuit has explained about the APA's rulemaking requirements:

> Rulemaking must be accompanied by (1) advance publication in the Federal Register of the proposed rule or its substance; (2) opportunity for public participation through submission of written comments, with or without oral presentation; and (3) publication of the final rule, incorporating a concise statement of its basis and purpose, thirty days before its effective date.[416]

"Rules issued through the notice-and-comment process are often referred to as 'legislative rules' because they have the 'force and effect of law.'"[417] The D.C. Circuit observed that the APA's provisions "separate administrative rules that carry the force of law from those that do not."[418]

---

[413] In the Matter of Protecting & Promoting the Open Internet, 30 FCC Rcd. 5601 (2015).

[414] Greater Boston Television Corp. v. FCC, 444 F.2d 841, 852 (D.C. Cir. 1970).

[415] *Restoring Internet Freedom*, 83 Fed. Reg. 7852, 7852 (2018).

[416] Lewis v. Sec'y of the Navy, 195 F. Supp. 3d 277, 285 (D.D.C. 2016) (citing Batterton v. Marshall, 648 F.2d 694, 700 (D.C. Cir. 1980) (interpreting 5 U.S.C. § 553)).

[417] *Id.* (citing Perez v. Mortg. Bankers Ass'n, 135 S. Ct. 1199, 1203 (quoting Chrysler Corp. v. Brown, 441 U.S. 281, 302–03 (1979))).

[418] *Batterton*, 648 F.2d at 701.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

The FCC's failure to publish its footnotes in the Federal Register as part of the FCC's "Final Rule" indicate that the footnotes may not "carry the force of law" under the APA.[419] The FCC did not publish reasoning in its text analyzing public safety uses of the Internet by the public, proffering no reasoning that carries the force of law under the APA.

2. The APA Requires the Agency to Analyze the Facts that Underlay Prior Policies and to Discuss its Rationale for Changing Policy

When evaluating whether to change a policy, the APA requires an agency to consider the facts, circumstances, and statutory duties that supported its prior policy.[420] The FCC's *Internet Freedom Order* "failed to offer sufficient consideration of the values the FCC's *2015 Open Internet Order* protected. . . ."[421] Those values include public safety and critical infrastructure such as the energy sector, national security, and democracy.[422]

National Lifeline Ass'n v. Federal Communications Commission, which was decided the same day as the net neutrality appeal oral argument (Feb. 1, 2019), found the FCC's decision regarding its Tribal Lifeline program arbitrary and capricious for its failure to consider the rationale that supported prior relevant decisions.[423] *National Lifeline Ass'n* emphasized that when an agency changes its prior policy, "the new policy must be permissible under the statute, and the agency must acknowledge it is changing its policy and show that 'there are good reasons' for the new policy and 'that the agency *believes* it to be better, which the conscious change of course adequately indicates.'"[424] The D.C. Circuit emphasized that an "agency cannot ignore its prior factual findings that contradict its new policy nor ignore

[419] *Id.*

[420] U.S. Telecom Ass'n v. FCC, 825 F.3d 674, 708–09 (D.C. Cir. 2016).

[421] *Amici Brief, Professors of Administrative, Communications, Energy, Contract Law, and Policy*, *supra* note 5, at 2.

[422] *Id.*

[423] Nat'l Lifeline Ass'n v. FCC, 915 F.3d 19, 22–23 (D.C. Cir. 2019).

[424] *Id.* at 28 (FCC v. Fox Television Stations, Inc., 556 U.S. 502, 515 (2009)).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

reliance interests."[425] "[A] reasoned explanation is needed for disregarding facts and circumstances that underlay or were engendered by the prior policy."[426]

"When reversing existing policy, the APA requires an agency to provide more substantial justification 'when its new policy rests upon factual findings that contradict those which underlay its prior policy. . . .'"[427] "An agency rescinding a rule 'is obligated to supply a reasoned analysis for the change beyond that which may be required when an agency does not act in the first instance.'"[428] "[A] reasoned explanation is needed for disregarding facts and circumstances that underlay or were engendered by the prior policy."[429] In other words, the D.C. Circuit stated in *USTA v. FCC*, "[i]t would be arbitrary and capricious to ignore such matters."[430]

3. *Chevron* Deference Is Merited Only for Agency Decisions that Comply with the APA

"[U]nexplained inconsistency" in agency policy is 'a reason for holding an interpretation to be an arbitrary and capricious change from agency practice.'"[431] "An 'arbitrary and capricious' regulation of this sort is itself unlawful and receives no *Chevron* deference" to an administrative agency's interpretation of an ambiguous statute.[432] Whether the Court defers to the FCC's decision-making under *Chevron* depends on the Commission's determination based on "whether its findings are by adequate analysis and substantial evidence in the record considered as a whole."[433]

The FCC's *2018 Internet Freedom Order* failed to consider public safety issues, including those affecting critical infrastructure, concerns the prior agency decision relied on in adopting net neutrality rules. "The *2015 Order* considered

---

[425] *Id.* (citing *Fox Television*, 556 U.S. at 515–16).

[426] *Id.* (citing *Fox Television*, 556 U.S. at 516).

[427] *Amici Brief, Professors of Administrative, Communications, Energy, Contract Law, and Policy*, *supra* note 5, at 5.

[428] *Id.* (citing Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 42 (1983)).

[429] U.S. Telecom Ass'n v. FCC, 825 F.3d 674, 708–09 (D.C. Cir. 2016) (quoting *Fox Television*, 556 U.S at 515–16).

[430] *Id.* (quoting *Fox Television*, 556 U.S. at 515).

[431] *Amici Brief, Professors of Administrative, Communications, Energy, Contract Law, and Policy*, *supra* note 5, at 12 (citing Encino Motorcars, LLC v. Navarro, 136 S. Ct. 2117, 2126 (2016)).

[432] *Id.* (citing United States v. Mead Corp., 533 U.S. 218, 227 (2001)).

[433] Mo.-Kan.-Tex. R.R. Co. v. United States, 632 F.2d 392, 400 (5th Cir. 1980).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

critical infrastructure sector needs in rejecting proposals to allow paid priority or individualized negotiations for fast Internet access with a 'minimum speed' guaranteed."[434] The *Open Internet Order* cited my comments that expressed concern that "paid prioritization undermines public safety and universal service, and increases barriers to adopting Internet-based applications," such as Internet-enabled demand response deployed to "prevent power blackouts, forestall the need to build fossil-fueled power plants, promote environmental sustainability, and manage energy resources."[435] Those comments supported the FCC's paid priority ban in 2015, requiring the FCC to address this rationale in its *2018 Internet Freedom Order*.

In banning paid prioritization, the FCC stated that "[o]ther forms of traffic prioritization, including practices that serve a public safety purpose, may be acceptable under our rules as reasonable network management."[436] The FCC's *2015 Order* discussed several concerns commenters raised about paid prioritization, including concerns that paid priority would "introduce artificial barriers to entry, distort the market, harm competition, harm consumers, discourage innovation, undermine public safety and universal service, and harm free expression."[437] The *2015 Order* noted that "[c]ommenters assert that if paid prioritization became widespread, it would make reliance on consumers' ordinary, non-prioritized access to the Internet an increasingly unattractive and competitively nonviable option."[438]

The *2015 Order* observed that "consumers bear the harm when they experience degraded access to the applications and services of their choosing due to a dispute between a large broadband provider and an interconnecting party."[439] The *2015 Order* cited my comments that such carrier disputes "raise concerns about public

[434] *Amici Brief, Professors of Administrative, Communications, Energy, Contract Law, and Policy*, *supra* note 5, at 6 (citing Commissioner Sandoval, *Ex Parte Letter*, *supra* note 4, at 14) ("[A]ny of the minimum level of access standards the FCC proposes would be insufficient to support the needs of a diversity of Internet users including Critical Infrastructure.").

[435] In the Matter of Protecting & Promoting the Open Internet, 30 FCC Rcd. 5601, 5655 n.291 (2015) (citing Commissioner Sandoval, *Ex Parte Letter*, *supra* note 4, at 2).

[436] *Id.* at 5653 n.284.

[437] *Id.* at 5653–55 nn.298–92.

[438] *Id.*

[439] *Id.* at 5689–90.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

safety and network reliability."[440] Based on these and other concerns, the *2015 Order* adopted case-by-case approach to monitor traffic exchange and developments.[441]

The *2018 Internet Freedom Order* failed to articulate any consideration of the public safety consequences of "repealing the *2015 Order*'s restrictions on ISP throttling or unreasonable interference with or disadvantage to Internet users including those with 'unlimited' data plans."[442] The D.C. Circuit's *Mozilla v. FCC* decision cited as a basis for remanding the *2018 Internet Freedom Order* record comments that raised concern that "allowing broadband providers to prioritize Internet traffic as they see fit, or to demand payment for top-rate speed, could imperil the ability of first-responders, providers of critical infrastructure, and members of the public to communicate during a crisis."[443] To support its public safety remand, the D.C. Circuit used my comments about the Internet's integration into energy management that enable "demand response systems," which are "activated during times of high demand, or when fire or other emergencies make conservation urgent, and call on people and connected devices to save power."[444] The D.C. Circuit cited my comments about the importance of Internet-based tools such as a natural "gas-detection box" that uses readily available GIS platforms and tablets to quickly survey damaged areas following an earthquake to "identify and prioritize work to address gas leaks."[445]

The *2018 Internet Freedom Order* failed to address these and other record comments that underscored the importance of net neutrality to public safety. An agency's decision "can be upheld only 'on the basis articulated by the [Commission]

[440] *Id.* at 5690 n.503 (citing Commissioner Sandoval, *Ex Parte Letter*, *supra* note 4, attach. at 24) (asserting, for example, that difficulties in using interconnected VoIP service amidst a broadband provider dispute with a server host or content provider raise grave concerns about public safety and network reliability).

[441] *Id.* at 5692–93.

[442] *Amici Brief, Professors of Administrative, Communications, Energy, Contract Law, and Policy*, *supra* note 5, at 10–11.

[443] *Id.* at 5690 n.503 (citing Commissioner Sandoval, *Ex Parte Letter*, *supra* note 4, attach. at 24) (asserting, for example, that difficulties in using interconnected VoIP service amidst a broadband provider dispute with a server host or content provider raise grave concerns about public safety and network reliability).

[444] *Id.* at 5692–93.

[445] *Amici Brief, Professors of Administrative, Communications, Energy, Contract Law, and Policy*, *supra* note 5, at 10–11.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

itself'—not on 'appellate counsel's post hoc rationalizations.'"[446] Government Petitioners observe that Respondents, the FCC and U.S. DOJ, "concede that the *Order* failed to separately consider public safety."[447] Respondents' brief characterizes this omission as "inconsequential" arguing without citation to the Order that "the Commission's discussion of market forces adequately addressed public safety" and that "there is nothing 'distinct' about public safety."[448]

The FCC's *Internet Freedom Order* did not articulate the argument that market forces would address public safety.[449] The APA requires the reviewing court to consider only the reasons the agency articulated in its decision at issue in the litigation.[450] Government Petitioners observe that the market argument for addressing public safety was not "articulated by the [Commission]" in the *Order*.[451] Government Petitioners emphasize that "the Commission never considered public safety in its analysis, much less found it addressed by market incentives."[452] It was "incumbent upon [the agency] explicitly to acknowledge and address" public safety in the *Order* to "carry out with fidelity its statutory charge."[453]

Government Petitioners point out that the FCC has previously rejected market-based solutions to address public safety.[454] The FCC concluded previously that

[446] Government Petitioners Reply Brief, *supra* note 242, at 3 (citing Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 50 (1983)).

[447] *Id.* at 4.

[448] *Id.*

[449] *See generally* In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311 (2018).

[450] Michigan v. EPA, 135 S. Ct. 2699, 2710 (2015) ("[A] court may uphold agency action only on the grounds that the agency invoked when it took the action.") (citing SEC v. Chenery Corp., 318 U.S. 80, 87 (1943)); *see also* Beno v. Shalala, 30 F.3d 1057, 1073 (9th Cir. 1994) ("[W]e cannot infer an agency's reasoning from mere silence.").

[451] Government Petitioners Reply Brief, *supra* note 242, at 4.

[452] *Id.* at 4 (noting the lack of public safety analysis in the Internet Freedom's discussing of major issues) (citing *Restoring Internet Freedom*, 33 FCC Rcd. at 362–75 (public policy discussion with no reference to public safety); *Restoring Internet Freedom*, 33 FCC Rcd. at 375 (concluding that "economic" factors support the order); *id.* at 450–52 (eliminating open Internet protections without discussion of public safety); *id.* at 452–56 (finding general conduct standard not in the "public interest" without considering public safety); *id.* at 466–70 (disclaiming need for bright-line rules without considering public safety); *id.* at 490–95 (cost-benefit analysis without discussion of public safety)).

[453] *Id.* at 4–5 (citing Am. Trading Transp. Co. v. United States, 791 F.2d 942, 949 n.7 (D.C. Cir. 1986)).

[454] *Id.* at 5.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

"public safety interests are not driven solely by economic considerations."[455] Government Petitioners argue that "the Communications Act does not regard public safety as addressed or subsumed by market forces, but addresses these factors separately."

The FCC's order cannot comply with the APA and is not due *Chevron* deference absent FCC analysis of the public safety risks of net neutrality repeal.[456] Contemporary concerns about attempts to undermine cybersecurity at critical infrastructure facilities, including energy plants, underscore the importance of addressing the effects of net neutrality repeal on public safety.

4. Public Safety Risks to Critical Infrastructure Including Energy and Water from Net Neutrality Repeal

In 2017, President Trump issued an Executive Order on Cybersecurity which directed the Secretary of Commerce and the Secretary of Homeland Security to:

> [J]ointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets).[457]

Despite this directive to improve cybersecurity for all sectors relying on the Internet including Critical Infrastructure and public safety, the FCC's *2018 Internet Freedom Order* skipped over these pivotal issues.[458]

The increasing integration of the Internet into the energy sector and public safety uses underscore the importance of evaluating proposals to permit ISPs to engage in paid priority that may disadvantage other Internet traffic. Proposals to permit ISPs to block or throttle Internet signals raise public safety, cybersecurity, energy security, reliability and attendant public safety concerns. Government

---

[455] *Id.* at 7 (*compare* 47 U.S.C. § 151 (mandate to consider public safety), *with* 47 U.S.C. § 230(b) (policy to promote market competition)).

[456] *See* Encino Motorcars, LLC v. Navarro, 136 S. Ct. 2117, 2126 (2016) (concluding that arbitrary and capricious decision-making is not entitled to *Chevron* deference).

[457] Exec. Order No. 13800, 82 FR 2391 § 2(d) (2017) (Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure).

[458] *See generally* In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311 (2018).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

Petitioners emphasized the importance of the open Internet to energy and public safety. "As part of the effort to modernize the nation's electrical grid, electric utilities in California and other States have invested ratepayer funds in integrated systems of smart meters, communications networks, and data management systems that enable two-way communication between utilities and customers."[459]

Government Petitioners' brief emphasized that "[i]nstant communication between customers, suppliers, energy generators, contractors, regulators, and safety personnel is essential to maintaining a safe and reliable grid, and must thus remain free from blocking or delay due to throttling or deprioritization."[460] Protecting institutional users such as energy utilities would be insufficient to protect the energy safety and reliability. Access to mass-market public Internet plans is critical to the energy ecosystem's reliability and safety.

> As a statutory basis for requiring reliable communications to support the energy sector's communication with its suppliers, customers, and others, Government Petitioners cited the Critical Infrastructures Protection Act of 2001 (CIPA).[461] CIPA was adopted as part of the USA Patriot Act in the wake of the September 11, 2001 attacks to protect sectors critical to the U.S. economy, public safety, and democracy. CIPA defines critical infrastructure as those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[462]

CIPA "defines critical infrastructure *not* with reference to the identity of the target, but by the consequences of an attack on it."[463]

---

[459] Sandoval, *Reply Comments*, *supra* note 5, at 51.

[460] *Id.* (citing Critical Infrastructures Protection Act of 2001, 42 U.S.C. § 5195c (2012); Sandoval, *Reply Comments*, *supra* note 5, at 47).

[461] Critical Infrastructures Protection Act § 5195c.

[462] *See* Sandoval, *Reply Comments*, *supra* note 5, at 12 n.53 (citing 42 U.S.C. § 5195e).

[463] Nicholas Bagley, *Benchmarking, Critical Infrastructure Security, and the Regulatory War on Terror*, 43 HARV. J. ON LEGIS. 47, 50 (2006).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

The Energy Policy Act of 2005 ("EPAct") amended the Federal Power Act ("FPA") to require electric power grid operators to ensure grid reliability.[464] EPAct defined reliable operation of the "bulk-power system" to including the prevention of "uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."[465] The bulk-power system is composed of "(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation facilities needed to maintain transmission system reliability" but "does not include facilities used in the local distribution of electric energy."[466]

States have a duty to ensure that energy utilities under their jurisdiction provide safe, reliable service, at just and reasonable rates.[467] Illinois Public Utilities Commissioner Sherina Maye Edwards observed that "[a]s utility infrastructure becomes increasingly automated, ensuring the security of critical energy infrastructure is becoming a major concern."[468] Companies that "own and operate such assets," must address these risks, as well as local, "state and federal regulators tasked with ensuring the safety, reliability and cost-effectiveness of the services delivered."[469] Ephram Glass and Victor Glass argued that to make the electric grid more resilient against unforeseen attacks on the electric grid's cyber and physical infrastructure, "the U.S. needs to increase distributed generation to ensure no substations are critical to the stability of the electric grid."[470] Government Petitioners' brief argued that the *Order* interferes with state public utility regulators' ability to comply with federal and state statutory mandates to promote universal service and protect public safety.[471]

---

[464] Sandoval, *Cybersecurity Paradigm Shift*, *supra* note 322, at 95–96 (citing Energy Policy Act of 2005, Pub. L. No. 109–58, 119 Stat. 594 (2005); 16 U.S.C. § 824o, § 215(b)).

[465] Energy Policy Act of 2005, 16 U.S.C. § 824o(a), (4) (2018).

[466] *Id.* at § 824o(a)(1).

[467] *See, e.g.*, CAL. PUB. UTIL. CODE § 451 (2019).

[468] Sherina Maye Edwards et al., *Opportunities and Challenges for State Utility Regulators*, PUB. UTIL. FORT. (Feb. 2017), https://www.fortnightly.com/fortnightly/2017/02/cybersecurity-part-1.

[469] *Id.*

[470] Ephram Glass & Victor Glass, *We Are One Terrorist Attack Away from a Major Nationwide Blackout, What Should We Do?*, RUTGERS BUS. REV., Fall 2018, at 144, 153.

[471] Brief for Government Petitioners, *supra* note 345, at 14.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

States such as California have been leaders in developing the Energy-Internet nexus to manage energy resources at just and reasonable rates, consistent with climate change mitigation goals. Government Petitioners brief emphasized that "California has relied on demand response services offered by utilities and third parties to directly balance load, manage congestion, and satisfy state and federal reliability standards," quoting my Reply Comments submitted for the FCC's *2015 Order* record.[472] California's electric grid operator, CAISO, "dispatches demand response to achieve immediate load reduction when high temperatures, wildfire, or other emergencies make conservation urgent."[473] New Jersey, Massachusetts, and other states also rely on Internet-enabled demand response to balance energy supply and demand and protect public safety dependent on energy access.[474]

Wholesale energy markets overseen by the Federal Energy Regulatory Commission ("FERC") also rely on demand response as a grid-balancing resource approved by FERC Order 745 adopted in 2011. The Supreme Court's 2016 decision in *F.E.R.C. v. Electric Power Supply Ass'n* upheld wholesale demand response which "pays consumers for commitments to curtail their use of power, so as to curb wholesale rates and prevent grid breakdowns, authorizing demand response to participate as a resource in wholesale energy markets."[475]

FERC reported in 2018 that by the end of 2015, approximately 27,541 megawatts of demand response participated in FERC wholesale markets, a number that continues to grow.[476] Demand response accounted for 5.6% of the resources to meet peak energy need in 2017, up from 5.3% in 2016.[477] When the grid is under pressure such as during energy shortages or the 2014 or 2019 polar vortex, demand response can be the difference between energy stability and blackouts that increase risks to health and public safety. The PJM regional wholesale electricity market under FERC jurisdiction has increased its use of "demand response" programs which "include contracts in which businesses and institutions get paid for agreeing to

---

[472] *Id.* at 24 (citing *Sandoval Net Neutrality September 2014 Testimony*, *supra* note 396, at 34–35).

[473] *Id.*

[474] *Id.* (citing MASS. GEN. LAWS ch. 25, § 21(b) (2018) (mandating energy efficiency plans that include demand response programs); *Rockland Electric Co.*, Case No. ER16060524 (N.J. Bd. of Pub. Util., Aug. 23, 2017)).

[475] FERC v. Elec. Power Supply Ass'n, 136 S. Ct. 760, 769–70 (2016).

[476] FED. ENERGY REGULATORY COMM'N, 2018 ASSESSMENT OF DEMAND RESPONSE AND ADVANCED METERING 1 (2018).

[477] *Id.* at 1–2.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

reduce their use when called upon. These agreements add up to 4,800 megawatts, which is up from 1,500 megawatts in 2014."[478] The Internet is critical to notifying customers to reduce energy use, whether manually by changing the temperature on a thermostat, or through Internet-enabled "auto-DR" signals.[479]

During the 2014 Polar Vortex, when natural gas traders took advantage of high prices in the East and created shortages in California that threatened electric power reliability, "[d]emand response programs deployed a virtual power plant to reduce energy consumption."[480] Demand response produced 800 megawatts ("MW") of load reduction "during the evening ramp and peak of the electric demand . . . relieving pressure on the supply" in California on February 6, 2014.[481] This level of demand response is more than two and a half times the size of a 300 MW peaker plant.[482] "CAISO reported demand response and Distributed Energy Resources ("DERs") are well-tailored to address local needs in areas where gas-fired power plants were short on gas."[483]

The *2018 Internet Freedom Order* endangers the ability to use the Internet to balance energy demand, stave off blackouts, or protect public safety. The FCC's Order "imposes no eligibility requirements for paid priority buyers—whether foreign or domestic—and fails to analyze public safety and national security consequences of authorizing paid priority without restriction or FCC jurisdiction."[484] The FCC relies on "market forces" and its limited disclosure rules to deter ISP action that could harm public safety. Respondent's Reply Brief argues that "Petitioners do not explain why it would make any business sense for a broadband provider to intentionally

---

[478] Dan Gearino, *Power Companies vs. the Polar Vortex: How Did the Grid Hold Up?*, INSIDE CLIMATE NEWS (Feb. 2, 2019), https://insideclimatenews.org/news/01022019/polar-vortex-utilities-gas-coal-renewable-energy-midwest-demand-response.

[479] *See*, *e.g.*, Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 7, at 38.

[480] *Id.* at 33 (CAISO, GAS EVENTS AND MARKET RESULTS OF FEBRUARY 6, 2014, at 16 (2014)).

[481] *Id.*

[482] *Cf.* Barry Cassell, *New 800-MW Natural Gas-Fired Power Plant Begins Operation Early*, POWER ENGINEERING (May 17, 2013), https://www.power-eng.com/articles/2013/05/new800-mw-natural-gas-fired-power-plant-begins-operations-early.html ("Eight units with quick-starting and fast-ramping capability make the project a perfect fit for summer peak seasons, while also backing up California's growing solar and wind farms that literally surround the plant" and providing 800-MW of capacity.).

[483] CAISO, *supra* note 480, at 16.

[484] *Amici Brief, Professors of Administrative, Communications, Energy, Contract Law, and Policy*, *supra* note 5, at 10 (citing In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311, 312–13 (2018); Sandoval, *Reply Comments*, *supra* note 5, at 4, 25, 27, 46).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

impair public safety. The Commission's transparency rule requires providers to disclose these practices, at which point 'public opprobrium' and 'fierce consumer backlash' would inevitably ensue."[485]

The energy sector faces reliability and cybersecurity duties under the federal Energy Policy Act of 2005 and state public utility law.[486] The energy sector and other critical infrastructure providers and regulators are not legally entitled to rely on market forces, disclosures which do not address paid priority, public opprobrium and consumer backlash to protect reliability, security, and public safety.[487] An open and neutral internet—net neutrality—is necessary to protect energy reliability crucial to American's economy, public safety, national security, and deployment of climate change solutions.

Electric reliability is federally mandated by the Electricity Modernization Act of 2005 passed during the administration of President George W. Bush.[488] The energy sector is among the critical infrastructure protected by CIPA whose "systems and assets, whether physical or virtual," are "vital to the United States" and whose "incapacity or destruction" would debilitate "security, national economic security, national public health or safety, or any combination of those matters."[489] Despite the record urging the FCC to consider the risks of net neutrality repeal to energy reliability, critical infrastructure, and public safety, the FCC failed to consider whether ISP paid priority deals would degrade energy reliability or create public safety risks.

The "need to protect open and neutral Internet access for the energy sector is commensurate with the distributed energy ecosystem's reach."[490] The home used to be thought of as the "grid edge where people consumed electricity, but did not

[485] Reply Brief for Respondent at 94, Mozilla Corp. v. FCC, No. 18-1051 (Nov. 27, 2018).

[486] Energy Policy Act of 2005, 16 U.S.C. § 824o, § 215(b) (2018); *see, e.g.*, CAL. PUB. UTIL. CODE § 451 (2019). "Every public utility shall furnish and maintain such adequate, efficient, just, and reasonable service, instrumentalities, equipment, and facilities, including telephone facilities, as defined in Section 54.1 of the Civil Code, as are necessary to promote the safety, health, comfort, and convenience of its patrons, employees, and the public." *Id.*

[487] Sandoval, *Cybersecurity Paradigm Shift*, *supra* note 322, at 137–38.

[488] Electricity Modernization Act of 2005, 42 U.S.C.A. § 15801 (West 2018) (charging the Federal Energy Regulatory Commission (FERC) with adopting reliability standards).

[489] 42 U.S.C. § 5195c(e) (2018); Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 7, at 1, 3 n.3, 7, 8 n.26.

[490] Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 7, at 18.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

produce it."[491] The smart grid era empowered by mass-market Internet access makes home energy resources, connected by Wi-Fi to mass-market, BIAS services, deployable energy resources. "Many solar resources at residential and some business properties use the premise's Wi-Fi to connect the inverter to the Internet, enabling solar panel monitoring."[492] "The Internet enables a home or a building to serve as an energy generator, or to decrease or shift energy on demand to aid the grid, save money, prevent blackouts, and protect the environment by reducing GHG emissions."[493]

AT&T argued in the *Internet Freedom* docket that the FCC's removal of the 2*015 Order*'s bar on paid priority would allow it to, "begin implementing isolated paid-prioritization arrangements to support [QoS] for unusually latency-sensitive applications, such as high-definition videoconferencing or massively multiplayer online gaming ("MMOG")."[494] My Article *Net Neutrality Powers Energy and Forestalls Climate Change* observed that "an ISP's priority deal with a video game provider—whether foreign or domestic—could impact a range of communications to and from the subscriber's account."[495] "The ISP's priority transmission of the video game may delay . . . a demand response communication with an Internet-connected thermostat or a DER, or a DER's response to a request to provide voltage support."[496]

The California Independent System Operator ("CAISO"), which oversees large parts of California's grid under FERC jurisdiction observed that "[t]he same companies that support the retail Internet support the increasingly digitally interconnected North American reliability and energy infrastructure.[497] My comments submitted for the FCC's *2015 Order* proceeding emphasized that protecting public access to the Open Internet is critical to protect public safety and

[491] *Id.*

[492] Sandoval, *Cybersecurity Paradigm Shift*, *supra* note 322 n.378 (citing Scott Partlin, *Three Ways to Communicate with a Solar Inverter*, SMA (Apr. 6, 2015), https://www.sma-sunny.com/en/3-ways-on-how-to-communicate-with-a-solar-inverter/).

[493] Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 7, at 18.

[494] *Id.* at 47 (citing AT&T Services, Inc., Comment Letter on In the Matter of Restoring Internet Freedom 5 (July 17, 2017), https://ecfsapi.fcc.gov/file/10717906301564/AT%26T%20Internet%20Freedom%20Comments.pdf).

[495] *Id.*

[496] *Id.*

[497] CAISO, BUSINESS PRACTICE MANUAL FOR DIRECT TELEMETRY 31–32 (2018).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

critical infrastructure.[498] Those comments argued, "[a]ny proposal to exempt Critical Infrastructure sectors from ISP negotiations over Internet speed and terms on a closed and differentiated basis" would not "protect American safety, security, the economy, and the polity."[499]

Government Petitioners' *Mozilla v. FCC* brief emphasized that "[a]s with many private-sector services, large portions of critical infrastructure used by governments and utilities have moved to the Internet. This modernization enables more robust, responsive, and efficient service delivery. Consumers' access to the open Internet is essential to the effective provision of these online services."[500]

"Innovation depends on openness, the entrepreneur's idea, the National Lab's, the scholar's, or the student's research, and the community's input. A truly Open Internet facilitates innovation that improves utility operations and saves lives," my comments submitted for the *2015 Order* proceeding observed.[501] The open Internet safeguarded from ISP interference "enables new means to save energy such as using the Internet to send requests to people or connected devices to provide 'demand response' to reduce load on the electric grid."[502]

Mass-market Internet access also plays a critical role in enabling democratic participation in decision-making about issues ranging from public utility commission to city and county council agenda items. "The Internet invigorates public participation in regulatory proceedings," critical to government decision-making.[503] Santa Clara County has invested heavily "in Internet-based solutions to promote civic engagement, including, for example, live broadcast of public meetings and web publication of its laws."[504] Charges for paid priority, Government Petitioners contend, "threaten to make such innovative systems for connecting citizens to their governments available only to those who can pay, or to those whose governments pay for access."[505]

---

[498] Sandoval, *Reply Comments*, *supra* note 5, at 46–47.

[499] *Sandoval Net Neutrality September 2014 Testimony*, *supra* note 396, at 4.

[500] Brief for Government Petitioners, *supra* note 345, at 22–23.

[501] *Sandoval Net Neutrality September 2014 Testimony*, *supra* note 396, at 4–5.

[502] *Id.* at 5.

[503] *Id.*

[504] Brief for Government Petitioners, *supra* note 345, at 28 n.16.

[505] *Id.* (citing Santa Clara Comments at 4–6).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

The open Internet "facilitates two-way and multi-party communication between customers, businesses, regulators, and the public," crucial during emergencies.[506] Such communication daily "improves governance and operations, safety, and reliability," my FCC comments observed in 2014.[507] Subsequent evolutions in Internet use after my 2014 comments underscore the importance of open public access to the Internet to democratic discourse.

5. Public Safety Risks to Fire Safety, Public Health, Criminal Justice, Individual and Community Safety from Net Neutrality Repeal

Santa Clara County emphasized that the Internet is crucial to the execution of its law enforcement, health care, social services, and public safety duties, and its 1.9 million residents.[508] Santa Clara County, like many other government agencies, businesses, families, institutions, and individuals, has made significant investments to modernize its systems using web-based systems that "rely on high-bandwidth, latency-sensitive exchanges of information with the public."[509] The County's Fire Protection District "relies on Internet-based systems to provide crucial public safety services."[510]

State and local government public health and safety systems increasingly depend on both government and "the public's access to BIAS on nondiscriminatory terms."[511] Federal Courts use an electronic system Case Management, Electronic File System, CM/ECF, available through PACER to facilitate public document filing and

[506] *Sandoval Net Neutrality September 2014 Testimony*, *supra* note 396, at 5.

[507] *Id.*

[508] Brief for Government Petitioners, *supra* note 345, at 9.

[509] *Id.* at 10.

[510] *Id.*

[511] *Id.* at 14 (citing Santa Clara County, *Comment Letter*, *supra* note 19, at 2–14; Sandoval, *Reply Comments*, *supra* note 5, at 25–27, 30–32; Representatives of Eleven Counties in Ohio, Comment Letter on In the Matter of Restoring Internet Freedom 3–4, 8 (July 21, 2017), https://www.fcc.gov/ecfs/filing/107202155401703; Representatives of Seven West Virginia Counties, Comment Letter on In the Matter of Restoring Internet Freedom 3–4 (July 21, 2017), https://www.fcc.gov/ecfs/filing/1072028938157).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

access.[512] The FCC did not analyze how paid priority sold could degrade Internet access for court filers, limiting access to justice.

Tom Johnson argued for the FCC at the *Mozilla v. FCC* oral argument that the FCC made two findings regarding paid prioritization generally in paragraph 258 of the *Internet Freedom Order*.[513] He characterized as the first finding the FCC's rejection of "the idea that paid prioritization, prioritizing certain packets for delivery, would affect best efforts service."[514] "The FCC believes ISPs don't have the incentive to do that independently on their own accord, and that there are network management practices that can continue best efforts services even if particular packets are prioritized," Johnson argued.[515]

The text of paragraph 258 of the *Internet Freedom Order* does not specifically discuss "best efforts" Internet service—or define any standard Internet service. Footnote 939 briefly mentions, without analysis, the theory that ISPs will not have incentives to slow best efforts traffic. Paragraph 258 including its footnotes as published by the FCC in January 2018 states:

> We reject assertions that allowing paid prioritization would lead ISPs to create artificial scarcity on their networks by neglecting or downgrading non-paid traffic.[516] This argument has been strongly criticized as having "no support in economic theory that such incentives exist or are sufficiently strong as to outweigh countervailing incentives."[517] Moreover, as discussed above, in practice paid

[512] *Public Access to Electronic Court Records*, PACER, https://www.pacer.gov/cmecf/ (last visited Feb. 11, 2019).

[513] Mozilla v. FCC Oral Argument, *supra* note 30, at 3:22.

[514] *Id.* at 3:23–24.

[515] *Id.*

[516] In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311, 660–61 n.938 (2018) (citing *Title II Order*, 30 FCC Rcd. at 5653–54, ¶ 126; Vimeo Comments at 14; Internet Association Comments at 22; Consumers Union Comments at 15; Public Knowledge Comments at 113; Netflix Reply at 8–9; *see also* AARP Comments at 22 ("Pay-for-priority and fast lanes will cause customer confusion and will degrade the value of broadband connections. Incentives consumers would have to upgrade to higher capacity broadband connections will be muted, as the full value of more bandwidth can only be achieved if *all web sites and content* have the potential to be delivered at the 'up to' speed for which broadband subscribers pay.")).

[517] *Id.* at n.939 (*see* J. Gregory Sidak & David J. Teece, *Innovation Spillovers and the "Dirt Road" Fallacy: The Intellectual Bankruptcy of Banning Optional Transactions for Enhanced Delivery Over the Internet*, 6 J. COMPETITION L. & ECON. 521–94 (2010); *see also* AT&T Comments at 42 ("Mobile and fixed-line providers would not be investing tens of billions of dollars a year to increase their speeds . . . if

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

> prioritization is likely to be used to deliver enhanced service for applications that need QoS guarantees.[518] As AT&T explains, "[l]ast-mile access is not a zero-sum game, and prioritizing the packets for latency sensitive applications will not typically degrade other applications sharing the same infrastructure,"[519] such as email, software updates, or cached video.[520] Because of these practical limits on paid prioritization, we reject the argument that non-profits and independent and diverse content producers, who may be less likely to need QoS guarantees, will be harmed by lifting the ban.[521]

---

it were commercially viable for them to consign their customers to a 'dirt road' in any context. If Broadband Provider X began degrading its best-effort Internet access platform to favor its 'prioritized' content, such that most applications and content loaded more slowly on X's network than on its rivals' Internet access platforms, customers would begin switching to those rivals en masse."). While other studies are more equivocal, even studies finding that there may be an effect find that it does not reduce economic efficiency, but merely transfers costs from ISPs to certain edge providers. Employing simulations to test the robustness of their welfare results, Commission staff in 2014 found that in many simulations the welfare of edge providers, as a group, declines under paid prioritization. Mark Bykowsky & William Sharkey, *Welfare Effects of Paid for Prioritization Services: A Matching Model with Non-Uniform Quality of Service* 28 (July 2014), https://sites.google.com/site/williamwsharkey12/unpublished-work).

[518] *Id.* at 462–63.

[519] *Id.* at 462 (citing AT&T Comments at 44–45).

[520] *Id.* at 462 (*see* R Street Comments at 23–24; ACLP Comments at 20 ("The brief history of the Internet teaches that, regardless of how much capacity might be available, there will always be some level of congestion. Accordingly, there is significant evidence to support allowing firms to prioritize certain kinds of socially important content . . . over others."); CTIA Comments at 14–16; Ericsson Comments at 6 ("[B]ecause not all IoT connections place equal demands on the network, an inflexible version of net neutrality in this context could harm innovation. The notion that every data bit sent between connected cars should be treated with the same degree of priority as email traffic or that an augmented reality service is barred from obtaining a certain quality of service ignores the difference in requirements of the devices, applications, and users (not all of whom will be human) that will increasingly connect to the wireless Internet."). We thus reject arguments premised on the theory that ISPs could and would act to create artificial scarcity on their networks and thereby broadly require paid prioritization. *See, e.g.*, Engine Reply at 6–7 ("While ISPs are fond of noting that telemedicine and autonomous vehicle services are far more latency-sensitive than email traffic, these types of unique services are likely to represent a tiny fraction of the prioritization deals ISPs will seek to cut if the existing ban on paid prioritization is removed."); TDI et al. Comments at 11–12 ("[W]e have yet to observe concrete examples where (a) congestion exists sufficient to degrade traffic from accessibility-oriented applications (b) where accessibility oriented prioritization would provide a solution (c) that would function as well as simply provisioning more bandwidth for all users to relieve congestion."); OTI New America Reply at 24).

[521] *See* Vimeo Comments at 15–17 ("This two-tiered Internet would privilege certain business models and types of content over others. For example, edge providers that provide studio content . . . are better positioned to pay premium rates . . . [and] may be able to pass increased delivery costs onto consumers. Not all video content, however, allows for such fee shifting . . . non-studio content will generally be

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

Footnote 939 cites AT&T's Comments at 42 that if "[b]roadband Provider X began degrading its best-effort Internet access platform to favor its 'prioritized' content, such that most applications and content loaded more slowly on X's network than on its rivals' Internet access platforms, customers would begin switching to those rivals en masse."[522] This is the only mention of "best efforts" associated with this paragraph. Footnote 939 does not state that the FCC rejects the idea that paid prioritization would affect best efforts service. Nor does it explain any basis for assuming that the theory that consumers could switch if Internet traffic were delayed would protect other Internet traffic including public safety communications using mass-market broadband access.

Footnote 939 recognizes that AT&T's comments about incentives are not conclusive. It acknowledges that "[w]hile other studies are more equivocal, even studies finding that there may be an effect find that it does not reduce economic efficiency, but merely transfers costs from ISPs to certain edge providers." "Employing simulations to test the robustness of their welfare results," footnote 939 states, "Commission staff in 2014 found that in many simulations the welfare of edge

---

relegated to the 'slow lane,' thus diminishing its potential audience."); Independent Film and Television Alliance at 5; Future of Music Comments at 1 (Allowing paid prioritization "would allow big [ISPs] to create new pay-to-play fast lanes, disadvantaging those who cannot pay for preferential treatment, and replicating the industry's past problems with payola."); American Association of Law Libraries et al. Comments at 16 ("A world in which libraries and other noncommercial enterprises are limited to the internet's 'slow lanes' while HD movies can obtain preferential treatment undermines a central priority for a democratic society—the necessity of all citizens to inform themselves and each other just as much as the major commercial and media interests can inform them."); American Association of Community Colleges et al. Comments at 13; Digital Content Next Comments at 3–4; AARP Comments at 23; Public Knowledge Comments at 115–17. We reject related arguments about a reduction in consumer choice, because paid prioritization is unlikely to affect choice for content that does not demand QoS guarantees and is likely to *increase* choice for content that would benefit from QoS guarantees. Consumers Union Comments at 16 ("Without restrictions upon paid prioritization, the internet could very well become commoditized in a way where it would look and feel different, with an expensive tier of prioritized access, and an 'everything else' tier of slower service. We do not believe this alternative, two-tiered—and likely, more expensive—internet benefits consumers."); Internet Association Comments at 22–23; DigitalOcean Comments at 6. Nor do we think we need to address assertions that paid prioritization would endanger U.S. national security as they are vague and lack any substantiation whatsoever. *See* Catherine Sandoval Reply at 25 ("Proposals to permit unregulated paid prioritization on the Internet reflect a September 11-type of failure of imagination about risks to America's national security and democracy. Foreign governments and their agents would relish the opportunity to buy priority Internet access to slow American messages or create a priority blockade. . . . The FCC fails to connect the dots between the dangers of allowing any person or entity, including foreign actors or agents, to buy paid prioritization in an unregulated U.S. Internet market if the FCC adopts its proposal. This colossal omission recalls the failure of imagination that contributed to the September 11 attacks against our nation.").

[522] *Restoring Internet Freedom*, 33 FCC Rcd. at 462 n.939.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

providers, as a group, declines under paid prioritization.[523] The FCC offers no explanation of this simulation or its methodologies. Neither does it quantify the decline in the welfare edge of providers. Nor does footnote 939 or paragraph 258 recognize that public safety traffic is among the mass-market Internet traffic that paid priority could affect.

Neither footnote 939 nor any rationale contained within is published in the Federal Register Final Rule in Restoring Internet Freedom.[524] The Internet Freedom Final Rule published in the Federal Register does not mention "best efforts." The FCC may not rely on absent reasoning to comply with the APA.

Johnson also argued that, in paragraph 258, the FCC found that quality of service arrangements will help benefit small, niche providers—the type of providers he asserted public safety officials might want to utilize by giving them the ability to have dedicated networks.[525] In response to Judge Millet's question about whether those asserted benefits or discussion of how these niche providers will effect [*sic*] public safety are in the order, Mr. Johnson said "[n]o, your honor."[526]

Johnson argued that "the types of concerns these petitioners [public safety] are bringing are the same types of concerns that other edge providers are bringing."[527] He argued that the footnotes in paragraph 258 talk about how telemedicine might benefit from latency-sensitive applications, which might benefit from paid priority.[528] Johnson argued that the *Order* rejects the notion that U.S. national security would be hurt by a paid prioritization scheme.[529] Johnson contended that paragraph 258 supports providing more consumer choice, more quality options and functionalities, and that the order says the same thing regarding non-profits.[530]

Paragraph 258 of the *Internet Freedom Order* cites AT&T's comments which contend that, "[l]ast-mile access is not a zero-sum game, and prioritizing the packets

---

[523] *Id.* at n.939 (citing Bykowsky & Sharkey, *Welfare Effects of Paid for Prioritization Services: A Matching Model with Non-Uniform Quality of Service*, *supra* note 517, at 28).

[524] *See generally Restoring Internet Freedom*, 83 Fed. Reg. 7852 (2018).

[525] Mozilla v. FCC Oral Argument, *supra* note 30, at 3:24:36–3:24:38.

[526] *Id.*

[527] *Id.* at 3:24:36–3:24:50.

[528] *Id.* at 3:25:00–3:25:07.

[529] *Id.* at 3:25:07–3:25:27.

[530] *Id.* at 3:25:19–3:25:30.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

for latency sensitive applications will not typically degrade other applications sharing the same infrastructure, such as email, software updates, or cached video."[531] The FCC's conclusion in paragraph 258 "does not analyze the qualifiers in AT&T's explanation that prioritizing latency-sensitive application packets will not *typically* degrade other applications sharing the same infrastructure."[532] "AT&T's statement recognizes degradation is possible but projects that it would not be *typical* for other applications, while the FCC only conjectured its effect on email, software updates, or cached video."[533] The FCC fails to analyze the effect of paid priority on the range of other traffic which shares the same infrastructure.

The FCC's Order omits discussion of paid priority consequences for applications and Internet use apart from "email, software updates, or cached video."[534] Santa Clara County's fire department's Office of Emergency Service incident support unit uses "specialized software and Google Sheets," deployed during fires such as California's 2018 Mendocino Complex Fire.[535] These applications allow the fire agency "to do near-real-time resource tracking through the use of cloud computing over the Internet."[536] "The FCC's list omits analysis of paid priority's impact on streaming video or audio, large file transfers, mapping, and other common applications."[537]

Utility work crews "commonly use mapping applications for service calls, maintenance, and emergency response, as do millions of Americans."[538] "Modern firefighters rely on real-time geographic information system ("GIS") mapping to monitor fires and coordinate emergency response, track information, and save lives."[539] "Live stream video is becoming increasingly important to monitoring

[531] In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311, 462–63 (2018).

[532] Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 7, at 44 (emphasis added).

[533] *Id.* (emphasis added).

[534] *Id.* at 19.

[535] Addendum to Brief for Government Petitioners, *supra* note 365, para. 6.

[536] *Id.*

[537] Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 7, at 45.

[538] *Id.*

[539] *Amici Brief, Professors of Administrative, Communications, Energy, Contract Law, and Policy*, *supra* note 5, at 11–12 (citing CAL. PUB. UTIL. COMM'N, *supra* note 285, at 33–34).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

energy system conditions, physical and cyber security, and daily operations."[540] The FCC failed to consider the effect of paid priority on such applications or the evolving nature of Internet use.

In the *Mozilla v. FCC* oral argument, Judge Millet asked Johnson to explain how paid priority would work. "To let something else go faster, don't you either stop or slow down other things?" Judge Millet asked.[541] Johnson acknowledge that the packets would be prioritized, and asserted "[t]here would be network management tools . . . such as, you know, you're getting an email 10 milliseconds later."[542] The *Internet Freedom Order* makes no finding that paid priority would delay emails by only 10 milliseconds.[543] Commissioner O'Rielly's statement in footnote 35 quotes Judge William's dissent in *United States Telecom Ass'n* regarding the asserted benefits of paid prioritization for latency-sensitive Internet traffic, as opposed to traffic where "timeliness (especially timeliness measured in milliseconds) is relatively unimportant."[544] The only mention of milliseconds is in a footnote in Commissioner O'Rielly's statement, not in the FCC's Final Rule published in the Federal Register,[545] and thus, the FCC cannot rely on that citation to comply with the APA. Neither does Commissioner O'Rielly's statement mention that any paid priority delay would be limited to a certain number of milliseconds, nor any other time threshold. Footnote 35 does not state that email will be received "10 milliseconds later" in a paid priority regime, nor there any such finding in the FCC's *Internet Freedom Order* or Final Rule.

Neither does the *Internet Freedom Order* address delays to other Internet applications such as live video or photos. Judge Millet asked at the *Mozilla v. FCC* oral argument what happens when public safety "is trying to share photos as fast as they can . . . or they're trying to deal with wildfires . . . they may need videos, they may need things that require a lot of the bandwidth that you're going to have this,

---

[540] Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 7, at 45.

[541] Mozilla v. FCC Oral Argument, *supra* note 30, at 3:29–31.

[542] *Id.*

[543] *See* In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311 (2018) (Statement of Commissioner O'Rielly).

[544] *Id.* at 316 n.35 (quoting U.S. Telecom Ass'n v. FCC, 825 F.3d 674, 763 (Williams, J., concurring in part and dissenting in part)).

[545] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

but they aren't going to get to go first."[546] "We respectfully disagree," Johnson replied.[547] Johnson never answered Judge Millet's question about whether the FCC believes that such delays "won't happen or it's ok if that happens . . . to public safety."[548] Johnson added, "[w]e can't anticipate all harms or resolve all harms with this order."[549]

The FCC did, however, make predictions about harms from paid priority concluding that "[b]ecause of these practical limits on paid prioritization, we reject the argument that non-profits and independent and diverse content producers, who may be less likely to need QoS guarantees, will be harmed by lifting the ban."[550] The FCC did not explain the boundaries of the asserted "practical limits" of paid priority, nor did it consider the harm of paid priority for public safety.[551]

The *Internet Freedom Order* "neither defines the range of 'typical' degradation anticipated" from paid priority, "nor discusses paid priority's potential to degrade other Internet applications deployed by public safety agencies, critical infrastructure, courts, education, businesses, and families."[552] Johnson's argument that network management practices can continue best efforts services even if particular packets are prioritized[553] is not addressed in paragraph 258, the *Internet Freedom Order*'s footnotes, nor its Final Rule. The FCC must offer more detailed analysis of what those network management practices are and how they would work with a range of Internet traffic. The FCC must examine and explain the range of likely consequences apart from relying on AT&T's projection about what is typical for a limited set of applications. The APA requires the FCC to consider paid priority's the effects on all Internet users and consider public safety use of mass-market Internet access in that analysis.

Johnson cited the FCC's cursory dismissal in a footnote of my comments that cautioned the FCC to examine whether paid prioritization would harm U.S. national

---

[546] Mozilla v. FCC Oral Argument, *supra* note 30, at 3:30–31.

[547] *Id.*

[548] *Id.*

[549] *Id.*

[550] *Restoring Internet Freedom*, 33 FCC Rcd. at 462–63.

[551] *See id.*

[552] *Amici Brief, Professors of Administrative, Communications, Energy, Contract Law, and Policy*, *supra* note 5, at 9.

[553] Mozilla v. FCC Oral Argument, *supra* note 30, at 3:23:26–3:24:03.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

security.[554] Footnote 943 quips, "[n]or do we think we need to address assertions that paid prioritization would endanger U.S. national security as they are vague and lack any substantiation whatsoever."[555] The FCC offered no explanation or analysis to support its derisive treatment of my comments that observed in the wake of revelations of Russian interference in the 2016 elections that "[f]oreign governments and their agents would relish the opportunity to buy priority Internet access to slow American messages or create a priority blockade. . . . The FCC fails to connect the dots between the dangers of allowing any person or entity, including foreign actors or agents, to buy paid prioritization in an unregulated U.S. Internet market."[556]

The record I cited to support my concerns about the national security implications of net neutrality repeal included the Countering America's Adversaries with Sanctions Act,[557] CIPA,[558] and the EPAct's reliability duties for the energy sector.[559] Yet, the FCC ignored the legislative, statutory, and FCC record on which my concerns rested. The FCC failed to examine how allowing paid priority with no rules restraining ISPs after the FCC revoked its ISP jurisdiction (except for limited disclosure requirements which do not required details about paid priority deals) would affect national security.[560] The absence of analysis and cursory dismissal of concerns about national security rooted in federal and statute constitute arbitrary and capricious decision-making "contrary to law because the Commission failed to give an adequate reason for its decision."[561]

The oral argument also raised questions about the affordability of paid priority for public safety. Judge Millet asked, "[i]f local governments can't afford to pay for that for their firefighters, and ambulances, and other emergency services and disease

---

[554] *Id.* at 3:25:07–3:25:27.

[555] In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311 at n.943.

[556] *Id.* (citing Sandoval, *Reply Comments*, *supra* note 5, at 25).

[557] *See* Sandoval, *Reply Comments*, *supra* note 5, at 56 ("The *Countering America's Adversaries Through Sanctions Act* made a Congressional finding that '[o]n January 6, 2017, an assessment of the United States intelligence community entitled, "Assessing Russian Activities and Intentions in Recent U.S. Elections" stated, "Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the United States presidential election."'" (citing *Countering America's Adversaries Through Sanctions Act*, Pub. L. No. 115-44, 131 Stat. 886, Title II (211) (2017))).

[558] Critical Infrastructure Protection Act of 2001, 42 U.S.C. § 5291c (2001).

[559] In the Matter of Protecting & Promoting the Open Internet, 30 FCC Rcd. 5601, 5655 n.291 (2015).

[560] *See Restoring Internet Freedom*, 33 FCC Rcd. at 463.

[561] Fox Television Stations, Inc. v. FCC, 280 F.3d 1027, 1047 (D.C. Cir. 2002).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

control announcements, how does this help them?"[562] Johnson replied that he did not think it is true that public safety entities cannot afford paid priority.[563]

The CPUC expressed concern in its *Internet Freedom Order* comments that if governments have to pay for priority, "their ability to provide comprehensive, timely information to the public in a crisis could be profoundly impaired," a concern that D.C. Circuit recognized in ordering the public safety remand.[564] Respondents argued that "State Petitioners speculate that, without comprehensive conduct rules, broadband providers will seek to block or throttle government services unless first responders pay for prioritization."[565] Government Petitioners pointed out that "[b]ecause governments are obligated to be cost conscious, neither governments nor the businesses that serve them are likely to pay to prioritize their traffic."[566] Nothing in the record suggests that ISPs are offering to prioritize public safety Internet traffic for free. The *Internet Freedom Order* erects no limits on how much ISPs could charge for paid priority, neither does it offer any protection from slowdowns to accommodate prioritized traffic.

Johnson asserted that many states and municipalities rely on enterprise services, and emphasized that the *Internet Freedom Order* addresses mass-market channel services.[567] He emphasized that "there are dedicated communications pathways that deal with emergency alerts, EIS is one, there's one for broadcast, and there's the FirstNet system and other systems available that are outside this order."[568]

Johnson's arguments fail to recognize the distinctions between broadcast and the Internet. The Internet allows dialogic engagement and user-initiated communications in a way broadcast does not. Broadcasters have editorial discretion to determine what to air, and although they are likely to air institutional public safety messages consistent with their public safety mandate, they exercise editorial control

[562] Mozilla v. FCC Oral Argument, *supra* note 30, at 3:27–28.

[563] *Id.*

[564] *CPUC*, *Comments*, *supra* note 23, at 28–29.

[565] Brief for Respondents at 94, Mozilla Corp. v. FCC (Nov. 27, 2018), https://docs.fcc.gov/public/attachments/DOC-354525A1.pdf (citations omitted).

[566] Brief for Government Petitioners, *supra* note 345, at 28.

[567] Mozilla v. FCC Oral Argument, *supra* note 30, at 3:28.

[568] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

over which, if any, public messages to air.[569] FirstNet will only support institutional public safety users' emergency communications, not communications from the public to each other or different agencies.[570] Johnson's proffered alternatives are not substitutes for the Internet's functions.

Institutions such as universities, which may not qualify for FirstNet, also have a critical interest in the Internet's dialogic function to protect the campus community's public safety. For example, Brazil's largest university, the University of São Paulo, has upgraded to a "smart safety" system that integrates smart cameras, communications platforms, and a mobile app to improve safety for its 90,000 students, 6,000 professors, and 14,000 staff members.[571] Through a mobile phone, users can report an emergency through an app that displays digital "buttons," that allow users to: (1) report an issue that needs attention, such as a leak; (2) access a security map which shows past security instances for a selected time period, or; (3) enter into "watch over me" mode to have campus safety monitor their status.[572] In "watch over me" mode, while walking across campus, users can shake the phone to summon campus police if there's an incident, which increases response time and accuracy.[573] Such apps enable users to interact with safety officials through their mass-market phones to increase public safety.

Johnson's comments reveal the FCC's institutional public safety frame that ignores the public's role in public safety, and the importance of mass-market Internet access to public safety. The FCC was created "for the purpose of promoting safety of life and property through the use of wire and radio communications."[574] The FCC's statutory public safety mission is not confined to government or enterprise use of public safety services.

Goldstein argues that while Santa Clara County may use enterprise services, the people they are trying to reach with public safety messages about health threats,

---

[569] *See* CBS v. DNC, 412 U.S. 94 (1973) (upholding the editorial discretion of broadcasters to choose what content to air including commercials or other non-program messages).

[570] *See* FirstNet, *First Responder Network Authority*, ABOUT US, https://firstnet.gov/about (last accessed Aug. 2, 2019).

[571] JOÃO EDUARDO FERREIRA ET AL., IEEE, SMART SERVICES: A CASE STUDY ON SMARTER PUBLIC SAFETY BY A MOBILE APP FOR UNIVERSITY OF SÃO PAULO (2017).

[572] *Id.* § III.

[573] *Id.* §§ III–IV.

[574] 47 U.S.C. § 151 (1996).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

for example, use mass-market Internet services.[575] Government agencies including tribal entities are not legally required to use enterprise services and may use mass-market services and plans. Mass-market services may be used to convey and receive public safety information in a vertical fashion, such as information about vaccines during a flu pandemic.[576] Others may use mass-market plans to share public safety information in a horizontal fashion and create opportunities for dialogue and interaction.

Goldstein emphasized that paid prioritization's impact on mass-market Internet users, and public safety users are issues for the FCC to analyze, "and [the FCC] did not even mention them."[577] The burden is on the FCC to consider public safety, which it didn't do, Goldstein argues, concluding "this omission is fatal to the *Internet Freedom Order*."[578]

As this Article was going to press, the D.C. Circuit in October 2019 remanded the *Internet Freedom Order* for failing to address public safety, recognizing that a reviewing court cannot substitute its judgment or insert a potential rationale where the agency failed to articulate its reasoning. "A reviewing court is not authorized to conjecture an explanation the agency did not offer."[579]

6. Making Public Safety a Market Commodity Through Net Neutrality Repeal

Government Petitioners argued that ". . . while not 'intentionally' harming public safety, BIAS providers have, following market incentives, prioritized profit at the expense of public safety."[580] For example, in July 2018, a BIAS provider throttled the connection of a County Fire emergency response vehicle involved in the response to the largest wildfire in California history and did not cease throttling even when informed that this practice threatened public safety.[581]

---

[575] Mozilla v. FCC Oral Argument, *supra* note 30, at 4:17–18.

[576] *Id.* at 4:18.

[577] *Id.*

[578] *Id.* at 4:18:24–50.

[579] *Amici Brief, Professors of Administrative, Communications, Energy, Contract Law, and Policy*, *supra* note 5, at 13.

[580] Brief for Government Petitioners, *supra* note 345, at 22–23.

[581] Addendum to Brief for Government Petitioners, *supra* note 365, ¶ 9.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

The emails submitted in support of Government Petitioners' declaration regarding Verizon's throttling of its Fire Department's Internet use to fight the Mendocino Complex Fire showed Verizon deliberated slowed the fire department's Internet speed, demanding the department change to a new plan for $2 a month more.[582] As a public agency, the fire department could not quickly change its plan to one that costs even $2.00 a month more.[583]

After Government Petitioners' disclosed Verizon's throttling of the Fire Protection District's Internet speed during the Mendocino Complex Fire, Verizon promised not to slow the data of first responders on the West Coast and Hawaii.[584] Verizon then promised that "in the event of another disaster, it will lift restrictions on public safety customers, providing full network access."[585] Verizon's promise is triggered only "in the event of another disaster."[586] Verizon does not define who will determine whether a disaster exists or the time frame after disaster declaration that it will lift restrictions on "public safety customers."[587]

Neither does Verizon define who is a "public safety customer."[588] Are energy utilities public safety customers when they support firefighters by managing energy resources during a firefight? Are energy utilities, resources, regulators, and the distributed energy ecosystem "public safety customers?" Verizon's press release does not protect daily operation or management for critical infrastructure sectors including energy and water, or exigent public safety issues.

Verizon's institutional focus on "public safety customers" ignores the role of the public in protecting public safety. Flood monitoring through Internet-enabled river gauges and public posting of videos that inform flood protection districts, first responders, and communities of flood dangers, all protect life and property. The distributed energy network relies on all of its users, suppliers, researchers, public

---

[582] *Id.* ex. A, at 8–13.

[583] *Id.* ex. A, at 13.

[584] Wendy Davis, *Verizon Promises to Stop Throttling First Responders*, MEDIA POST (Aug. 24, 2018), https://www.mediapost.com/publications/article/324091/verizon-promises-to-stop-throttling-first-responde.html.

[585] *Verizon Statement on California Wildfire and Hurricane Lane in Hawaii*, VERIZON (Aug. 24, 2018), https://www.verizon.com/about/news/verizon-statement-california-wildfires-and-hurricane-lane-hawaii.

[586] *Id.*

[587] *Id.*

[588] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

safety, regulators, and the public to achieve energy reliability, public safety, and environmental goals.[589] Likewise, the open Internet supports distributed public safety, making each subscriber able to contribute to public safety using FEMA's Whole Community approach to public safety. Verizon's promise not to throttle "public safety" agencies in a disaster[590] fails to recognize that community Internet access is key to public safety.

The DOJ and FCC *Internet Freedom* appeal brief argued that ISPs will quickly respond to problems, as it asserts Verizon did through its pledge not to throttle Public Safety customers after disclosure of its dramatic slowing of the Fire District during a major firefight.[591] The FCC argued to the D.C. Circuit that ISPs have no business incentives to "intentionally impair public safety," because doing so will result in "public opprobrium" and "fierce consumer backlash."[592]

Judge Millet asked the FCC's lawyer whether post-hoc remedies work for public safety, in light of their arguments that such harms are not a fraud or antitrust issue, and that post-hoc remedies do not work for public safety.[593] A colloquy ensued in which Johnson contended that it is the burden of public safety commenters to show concrete harm.[594] Judge Millet noted that public safety obligations are statutory and that public safety concerns were on the record. Johnson did not try to justify post-hoc remedies for public safety.[595]

Neither did Johnson, nor the FCC's *Internet Freedom Order*, nor the D.C. Circuit's *Mozilla v. FCC* decision address the objections my comments raised that antitrust law remedies only harms to competition, not harms to public safety.[596]

---

[589] *Id.*

[590] *Id.*

[591] Mozilla Corp. et al. v. FCC, 2018 WL 6242647 (C.A.D.C.), 94–95 (Nov. 27, 2018).

[592] *Id.* at 94 (citing In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311, 467, 495 (2018)).

[593] Mozilla v. FCC Oral Argument, *supra* note 30, at 3:25.

[594] *Id.* at 3:25–27.

[595] *Id.* at 3:26–27.

[596] Sandoval, *Reply Comments*, *supra* note 5, at 45 n.236 (citing Atlantic Richfield Co. v. USA Petroleum Co., 495 U.S. 328, 334 (1990) (holding that antitrust laws were intended to prevent and protect against "antitrust injury" "attributable to an anti-competitive aspect of the practice under scrutiny")); Reply Brief of Internet Association, *supra* note 25, at 12 (citing Br. of Professors of Admin., Commc'ns, Energy, Antitrust, and Contract Law and Policy 7–8) ("Consequently, antitrust laws are ill-suited to address harms to consumers, free speech, investment, and innovation in the net neutrality context."). *Cf. Mozilla*, ___

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

Antitrust law's limited remedies that redress only harms to competition make it unsuited to address public safety harms, risks to energy, water, or critical infrastructure reliability or other types of harm.

"Corrections that come weeks, months, or years after an emergency come too late because crises happen in an instant, and the first few minutes of an emergency response are the most critical," Goldstein emphasized.[597] "That's when members of the community are getting these shelter-in-place or evacuation orders, and when first-responders are gathering information about on-the-ground conditions."[598]

The FCC's reliance on *post-facto* solutions after the customer publicly reveals ISP network management interference leaves customers, public safety, and energy reliability exposed to ISP conduct, increasing public safety risks. For the energy sector, throttling, paid priority that degrades other users, intentional interference or disadvantage, blocking, and any other ISP practices thwart vital energy operations, reliability, and public safety.[599] Whether the ISP's goal was to "intentionally impair public safety"[600] does not excuse the FCC, ISPs, the federal government, or energy, water, telecom, or other regulators from turning a blind eye to the public safety consequences of such actions.

Government Petitioners argued in their Reply Brief that "[r]espondents and Intervenors erroneously dismiss the record evidence of potential harm to the public—from consumer protection to public safety to government services—as sufficiently addressed by market forces."[601] Such "post hoc argument that market forces may protect public safety was not presented in the *Order* and cannot cure the Commission's failure to fulfill its statutory duty to consider public safety," Government Petitioners argued.[602] Neither does the market forces rationale for protecting public safety appear in the Final Rule the FCC published in the Federal Register.

F.3d at 93 (holding that the FCC's antitrust analysis "barely survives" arbitrary and capricious review, without analyzing the limits of antitrust remedy to only competition harms).

[597] Mozilla v. FCC Oral Argument, *supra* note 30, at 1:48.

[598] *Id.*

[599] *Id.*

[600] *Id.*

[601] Government Petitioners Reply Brief, *supra* note 242, at 1.

[602] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

7. The APA Requires the Agency Consider Reliance Interests on its Prior Decisions

The APA requires an agency changing its position from prior decisions to consider the reliance interests its previous decisions engendered.[603] Public agency investments in Internet-based services based on the *2015 Order* rules that prohibited ISP paid priority are examples of reliance interests the agency must subsequently consider. *Nat'l Lifeline Ass'n* requires the FCC to address "serious reliance interests" in its decision-making.[604] In *Nat'l Lifeline*, the Commission did not discuss service providers based around Lifeline nor the substantial number of customers relying on Lifeline services through those providers.[605] The public comments raised both of these concerns, yet

> [t]he Commission neither attempted to estimate the number of consumers who would be unable to afford service without the enhanced subsidy or would lose access to service altogether when non-facilities-based providers discontinued their plans, nor did it consider alternatives to ensure coverage for these consumers or respond to these objections.[606]

The change in policy absent "reasoned explanation" required the Court to vacate the Lifeline Order for a lack of necessary decision-making.[607] The Commission's *Internet Freedom Order* displays the same disregard of the public safety reliance interests raised in the *2018 Order*'s record.

My Reply Comments in the *Internet Freedom* docket emphasized the CPUC's reliance on net neutrality proscriptions in authorizing ratepayer investments when I served as a CPUC Commissioner. "Enforceable rules that prohibited ISPs from blocking, throttling, or engaging in paid prioritization encouraged our [CPUC]

[603] Nat'l Lifeline Ass'n v. FCC, 915 F.3d 19, 28 (D.C. Cir. 2019) (citing FCC v. Fox TV Stations, Inc., 556 U.S. 502, 513 (2009)) ("An agency cannot ignore its prior factual findings that contradict its new policy nor ignore reliance interests.").

[604] *Id.* at 31 (citing *Fox TV Stations*, 556 U.S. at 515–16).

[605] *Id.*

[606] *Id.*

[607] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

decisions to authorize Internet-enabled investments by energy and water ratepayers," my Reply Comments emphasized.[608] They further stated:

> The CPUC's November 2016 Energy Savings Assistance Program (ESAP) Decision, for which I served as the Assigned Commissioner, approved state investments to help low-income Californians save energy in a manner that benefits all and reduces greenhouse gases. The ESAP Decision approved ratepayer investment in several Internet-based services including those that leverage customer-facing programs such as funding "a smart thermostat that can participate in a demand response program, or a lighting control that can be internet enabled to track entry/exit behavior."[609]

The CPUC also adopted "D.16-12-026 [in December 2016] order[ing] large investor owned water utilities in California to consider filing proposals for Advanced Metering Infrastructure (AMI) to improve water leak detection and harness data communication that benefits customers, saves water, and increases water sustainability and rate affordability."[610] These decisions "safeguarded by the *2015 Open Internet Order*, enable ratepayers to save water, a precious resource during times of drought, increase reliability, improve water quality and safety, and maintain just and reasonable rates."[611] Santa Clara County extensively documented its investments in the Internet-based services that depend on mass-market Internet access free of blocking, throttling, and degradations associated with paid priority to carry out its civic functions and public safety duties.[612] The FCC has a duty to consider the reliance interests of governments, public safety agencies, firms with public safety responsibilities, businesses, institutions, families, and the public on the open Internet.

[608] Sandoval, *Reply Comments*, *supra* note 5, at 51.

[609] *Id.*

[610] *Id.*

[611] *Id.* at 52.

[612] Santa Clara County, *Comment Letter*, *supra* note 19.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

V. RECOMMENDATIONS AND CONCLUSION: REMAND AND REFRAME TO RECOGNIZE THE PUBLIC ROLE IN PUBLIC SAFETY, EMPOWERED BY AN OPEN INTERNET

The FCC's *Internet Freedom Order* and *Final Rule* is arbitrary and capricious in violation of the APA for its failure to articulate why it departed from prior FCC decisions that considered the impact of net neutrality on public safety.[613] Neither did the FCC address the extensive public safety record in the *Internet Freedom* docket. *National Lifeline Ass'n v. FCC* found the FCC's Tribal Lifeline decision arbitrary and capricious under the APA for failure to consider crucial issues presented by its record, or to justify its departure from past FCC decisions.[614] The FCC commits the same error in its *Internet Freedom Order* and *Final Rule*; the FCC failed to address its statutory mission to protect public safety.[615]

The FCC's founding statute, the Communications Act of 1934, and the Wireless Safety Act, require it to consider public safety in its rulemakings.[616] *Nuvio* affirmed in 2006 the statutory mandate for the FCC to consider public safety in its FCC rulemakings.[617] Analysis of the public safety considerations in reviewing whether to retain, repeal, or modify the 2015 net neutrality rules is absent from the FCC's *2018 Internet Freedom Order* and its *Final Rule* published in the Federal Register, despite its statutory duty to conduct and articulate such analysis.

The FCC and Intervenor ISPs proffered post-hoc arguments in the net neutrality appeal, arguing that FCC consideration of public safety was inherent in the FCC's analysis.[618] The APA requires the FCC to make that analysis explicit, not *sub silentio*. "It was 'incumbent upon [the agency] explicitly to acknowledge and address' public safety in the *Order* and *Final Rule* to 'carry out with fidelity its statutory charge.'"[619]

---

[613] Fox TV Stations, Inc. v. FCC, 280 F.3d 1027, 1047 ("[The Commission] failed to explain its departure from its previously expressed views," rendering its decision "arbitrary and capricious" and "contrary to law.").

[614] Nat'l Lifeline Ass'n v. FCC, 915 F.3d 19, 19 (D.C. Cir. 2019).

[615] *See* In the Matter of Restoring Internet Freedom, 33 FCC Rcd. 311 (2018); *Restoring Internet Freedom*, 83 Fed. Reg. 7852 (Feb. 22, 2018).

[616] 47 U.S.C. § 151 (1996); 47 U.S.C. § 615 (1999).

[617] Nuvio Corp. v. FCC, 473 F.3d 302, 307 (D.C. Cir. 2006).

[618] Government Petitioners Reply Brief, *supra* note 242, at 1.

[619] *Id.* at 4–5 (citing Am. Trading Transp. Co. v. United States, 791 F.2d 942, 949 n.7 (D.C. Cir. 1986)).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu

This obligation required the FCC to consider the public's use of the Internet for public safety, not merely institutional access through commercial accounts.

These failures support the *Internet Freedom Order*'s remand to the FCC for new proceedings and would, in my view, support the Order's vacatur.[620] On remand as ordered by the D.C. Circuit, the FCC and all proceeding participants must consider the public's role in public safety. The FCC's statutory duty is not merely to serve institutional public safety agencies. The FCC's statutory mandate is "promoting safety of life and property through the use of wire and radio communications."[621] Public safety paradigms must be reframed to recognize the Internet's importance to "distributed public safety" as practiced by the whole community, not just by government agencies.

The public's role in public safety, supported by an open Internet and safeguarded by enforceable rules, must take center stage in net neutrality analysis. The remand must analyze the regulatory framework necessary to protect public safety uses of the Internet. Abdication of FCC jurisdiction over ISPs is inconsistent with the FCC's public safety mission, and would leave the Commission unable to police ISP conduct that harms public safety. The remand must also examine the limits of antitrust and unfair competition remedies which provide no redress for public safety harms. Regulation, public comment, and academic analysis of net neutrality and public safety must consider and protect the whole community's interest in an open Internet that supports our collective well-being and public safety.

[620] *See* Fox TV Stations, Inc. v. FCC, 280 F.3d 1027, 1048 (citing Allied-Signal, Inc. v. U.S. Nuclear Reg. Comm'n, 988 F.2d 146, 150–51 (D.C. Cir. 1993) ("The decision whether to vacate depends on the seriousness of the order's deficiencies (and thus the extent of doubt whether the agency chose correctly) and the disruptive consequences of an interim change that may itself be changed.")). The D.C. Circuit declined to vacate the *Internet Freedom Order*'s remanded issues—the failure to analyze the Order's impact on public safety, Lifeline program qualifications, and utility pole access—concluding that the FCC "may well be able to address on remand the issues it failed to consider in the 2018 Order." *Mozilla*, ___ F.3d at 145. The D.C. Circuit vacted the Order's attempt to preempt state ISP regulation as having no basis in statute or authority. *Id.* at 146.

[621] 47 U.S.C. § 151 (2018).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.658
http://lawreview.law.pitt.edu