

# UNIVERSITY OF PITTSBURGH LAW REVIEW

---

Vol. 81 • Winter 2019

UNAVAILABLE

Andrea M. Matwyszyn

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2019.677  
<http://lawreview.law.pitt.edu>



This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works 3.0 United States License.



This site is published by the University Library System of the University of Pittsburgh as part of its D-Scribe Digital Publishing Program and is cosponsored by the University of Pittsburgh Press.

# UNAVAILABLE

Andrea M. Matwyshyn\*

## I. INTRODUCTION

“You get the chicken by hatching the egg, not by smashing it.”<sup>1</sup>

Our economy is counting its proverbial chickens before they hatch. On the one hand, we are building a society that increasingly relies on the Internet for its functionality and economic success.<sup>2</sup> But, on the other hand, our current Internet infrastructure suffers from troubling security flaws,<sup>3</sup> a deficit of high-quality, redundant Internet access in both rural and urban areas,<sup>4</sup> and shortages in key fields

---

\* Professor of Law and Engineering and Associate Dean of Innovation and Technology, Penn State Law—University Park/Professor of Engineering Design, Penn State Engineering/Founding Director, PSU PILOT Lab. The author wishes to thank Michael Antonio, Matt Blaze, Jim Green, Brian Martin, Eric Meyer, Terrell McSweeney, Stephanie Pell, Abigail Slater, and Marcia Tiersky for their critiques and comments. Any bugs remain her own.

<sup>1</sup> Arnold H. Glasow, BRAINYQUOTE, [https://www.brainyquote.com/authors/arnold\\_h\\_glasow](https://www.brainyquote.com/authors/arnold_h_glasow) (last visited Apr. 2, 2019).

<sup>2</sup> See *infra* notes 150–74 and accompanying text.

<sup>3</sup> Joseph Cox, *Criminals Are Tapping into the Phone Network Backbone to Empty Bank Accounts*, MOTHERBOARD (Jan. 31, 2019), [https://motherboard.vice.com/en\\_us/article/mbzvxxv/criminals-hackers-ss7-uk-banks-metro-bank](https://motherboard.vice.com/en_us/article/mbzvxxv/criminals-hackers-ss7-uk-banks-metro-bank); see also Andrea M. Matwyshyn, *CYBER!*, 2017 BYU L. REV. 1109, 1109 (2018).

<sup>4</sup> See *infra* notes 81–84 and accompanying text. According to some estimates, 162.8 million people in the United States are not using the Internet at broadband speeds. John Kahan, *It's Time for a New Approach for Mapping Broadband Data to Better Serve Americans*, MICROSOFT: ON THE ISSUES (Apr. 8, 2019), <https://blogs.microsoft.com/on-the-issues/2019/04/08/its-time-for-a-new-approach-for-mapping-broadband-data-to-better-serve-americans/>. Indeed, despite inventing the Internet, the United States has steadily fallen behind other countries in Internet access quality. For example, the United States currently ranks tenth in the world on Internet speed. See *infra* note 270 and accompanying text.

of the technology workforce.<sup>5</sup> In other words, we are missing the necessary precursors for the next generation society we (think we) are building. Indeed, it also might be said that we are playing an imprudent game of technology chicken<sup>6</sup> with both our economic future and national security.

This disconnect in United States technology policy between the frenetic pace of innovation and the lack of robust technological infrastructure to support it in the long term can be called the “technology hatching problem.” The technology hatching problem divides into two types of issues—“pipes”<sup>7</sup> issues and “people” issues.<sup>8</sup> This Article addresses a portion of the “pipes” issues—the availability of high-quality, stable Internet access.<sup>9</sup> Today, this issue is initially classified, for better or worse, under the policy rubric of “network neutrality.”<sup>10</sup>

Specifically, this Article argues that instead of struggling to unwind the definitional tangles of the current “net neutrality” debate, policymakers should reframe the discussion in a broader context—the context of the technology hatching problem. When we analyze Internet availability as part of critical infrastructure—i.e., as an essential component of our national security and economy—a new guiding principle for law and policy emerges: redundancy. Thus, this Article argues that fostering Internet access redundancy should become an animating policy objective for Congress. To measure progress toward this goal, this Article introduces a new

---

<sup>5</sup> *Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher*, (ISC)<sup>2</sup> (June 7, 2017), <https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage>.

<sup>6</sup> Janet Chen et al., *Chicken*, GAME THEORY, <https://cs.stanford.edu/people/eroberts/courses/soco/projects/1998-99/game-theory/chicken.html> (last visited Mar. 29, 2019).

<sup>7</sup> “Pipes” issues involve the mechanics of Internet access and the physical conveyance of bits—the security, design of deployment, and quality of United States Internet infrastructure. Meanwhile, “people” issues relate to the economic and social impact of the “pipes” on end users, workers, and entrepreneurs in the technology economy.

<sup>8</sup> Traditionally, the two sets of issues have been compartmentalized, with one group of scholars engaging issues of content and a different group engaging issues of conveyance. This Article argues that these issues must be analyzed instead in tandem and reciprocally. See *infra* notes 53–87 and accompanying text.

<sup>9</sup> See Andrea M. Matwyshyn, *Silicon Ceilings: Information Technology Equity, the Digital Divide and the Gender Gap Among Information Technology Professionals*, 2 NW. J. TECH. & INTELL. PROP. 35, 35 (2003) (discussing one set of the “people issues”).

<sup>10</sup> For a discussion of the various definitions of “net neutrality,” see *infra* notes 28–52 and accompanying text.

paradigm and metric—“Internet Access Insecurity.”<sup>11</sup> Internet Access Insecurity refers to the condition where a (human or corporate) end-user cannot engage in desired Internet behavior<sup>12</sup> due to the unavailability<sup>13</sup> of Internet access<sup>14</sup> or content.<sup>15</sup> This new paradigm captures the spirit of the net neutrality concerns expressed by advocates, while more cleanly engaging with traditional bodies of law. It also opens unexplored legal avenues for Internet infrastructure improvement and new enforcement roles for agencies outside the Federal Communications Commission (“FCC”).<sup>16</sup>

Section II of this Article summarizes the current state of the law with respect to the term “network neutrality,” highlighting the term’s definitional imperfections and the policy ramifications of the FCC’s current policy paralysis. Section III explains the policy implications of the (re)classification of the Internet as critical infrastructure for national security purposes. Section III then begins to reframe network neutrality in the context of the broader technology hatching problem using two case studies—a recent incident of intentional throttling that impacted public safety and the availability concerns implicated by the next generation of Internet-reliant innovation, the “Internet of Bodies.”<sup>17</sup> Section III also offers insights from

---

<sup>11</sup> Internet Access Insecurity is inspired by the United States Department of Agriculture (“USDA”) and Food and Drug Administration’s (“FDA”) notion of food insecurity. Economic Research Service, *Definitions of Food Security*, U.S. DEP’T OF AGRIC., <https://www.ers.usda.gov/topics/food-nutrition-assistance/food-security-in-the-us/definitions-of-food-security.aspx> (last updated Sept. 4, 2019).

<sup>12</sup> See *infra* notes 249–74 and accompanying text.

<sup>13</sup> The National Institute of Standards and Technology defines availability as “ensuring timely and reliable access to and use of information.” Computer Security Resource Center, *Availability*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, <https://csrc.nist.gov/glossary/term/availability> (last visited Feb. 21, 2020).

<sup>14</sup> The question of access extends to issues of adequately reliable and robust Internet access to enable the end-user to engage in the desired conduct, not merely whether some inferior level of Internet access is available to the user. See *infra* notes 160–67 and accompanying text.

<sup>15</sup> Internet Access Insecurity explicitly combines the issues raised by earlier generations of the “digital divide” conversation with national security concerns, and the concerns expressed by net neutrality advocates. It also includes the information security notion of redundancy as part of defense. See Fahmida Y. Rashid, *A Lesson from Network Outage: Redundancy Matters*, INFOWORLD (Jan. 2, 2017), <https://www.infoworld.com/article/3153357/a-lesson-from-network-outages-redundancy-matters.html>.

<sup>16</sup> See *infra* notes 283–303 and accompanying text.

<sup>17</sup> See *infra* notes 137–48 and accompanying text; see also Andrea M. Matwyshyn, *The ‘Internet of Bodies’ Is Here. Are Courts and Regulators Ready?*, WALL ST. J. (Nov. 12, 2018), <https://www.wsj.com/articles/the-Internet-of-bodies-is-here-are-courts-and-regulators-ready-1542039566>; Andrea M. Matwyshyn, *The Internet of Bodies*, 61 WM. & MARY L. REV. 77 (2019).

two historical sources relevant to the future of Internet infrastructure: first, the history of the United States Post Office's evolution from a limited information service to a critical component of national security policy and, second, the history of the relationship between telecommunications companies and the Advanced Research Projects Agency Network ("ARPANET"). Section IV introduces the Internet Access Insecurity model and offers specific legal avenues that do not rely on the FCC alone for improving the redundancy and availability of Internet infrastructure. Section IV also offers a concrete proposal for a new statute: the Internet Infrastructure Availability Act. The proposed Act should include the creation of a blue-ribbon commission, direct multiple federal agencies outside the FCC to oversee portions of the Internet infrastructure, and encourage state and local community programs to buttress Internet infrastructure redundancy. Section V concludes and summarizes the arguments of the Article.

## II. ERROR 504<sup>18</sup>: THE NETWORK NEUTRALITY GATEWAY HAS TIMED OUT

Network neutrality has been called "the most discussed, least understood concept in the world of Internet policy."<sup>19</sup> As former FCC Commissioner Deborah Tate<sup>20</sup> has explained, her first question in any net neutrality conversation is "what is your definition of net neutrality?"<sup>21</sup> She cautions that she "rarely receive[s] the same response."<sup>22</sup> Indeed, other legal commentators have also described the term as "more a term of art than a precise goal or singular definition."<sup>23</sup> As Professor Thomas Nachbar put it, "neither [network] 'neutrality' nor 'open access' are self-defining concepts, and different proponents of network neutrality offer differing visions of

---

<sup>18</sup> *Hypertext Transfer Protocol (HTTP) Status Code Registry*, INTERNET ASSIGNED NUMBERS AUTHORITY, <https://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml> (last visited Apr. 8, 2019) [hereinafter *HTTP Status Code Registry*].

<sup>19</sup> Deborah T. Tate, *Net Neutrality 10 Years Later: A Still Unconvinced Commissioner*, 66 FED. COMM. L.J. 509, 517 (2014).

<sup>20</sup> Former Commissioner Tate has argued that the net neutrality dialogue should be concerned about whether the Internet is "safe and secure." *Id.* at 510 (citing Deborah Taylor Tate, *A Tangled Web: Moving from "Open and Free" to "Safe and Secure,"* PERSPECTIVES FROM FSF SCHOLARS, Apr. 28, 2010, at 1 (2010)).

<sup>21</sup> *Id.* at 516–17.

<sup>22</sup> *Id.* at 517.

<sup>23</sup> Babette E.L. Bolick, *Wireless Net Neutrality Regulation and the Problem with Pricing: An Empirical, Cautionary Tale*, 16 MICH. TELECOMM. TECH. L. REV. 1, 9 (2009).

what neutrality requires.”<sup>24</sup> However, today the line between proponent and opponent of network neutrality has also become slippery, as both sides of the debate have begun to use the term strategically under varying definitions.<sup>25</sup> Meanwhile, the FCC has struggled to find a definitive path as the regulator—or non-regulator—of network neutrality (under any definition) and continues to be embroiled in litigation on the subject.<sup>26</sup> This uncertainty has brought us to the point of today’s policy stalemate.

*A. Error 506<sup>27</sup>: Network Neutrality Variant Also Negotiates*

“Network neutrality” discussions first started almost two decades ago.<sup>28</sup> The phrase was popularized by Professor Tim Wu in 2003, who defined a “neutral network” as one “that does not favor one application . . . over others.”<sup>29</sup> Professor Wu argued that the “basic principle behind a network anti-discrimination regime is to give users the right to use non-harmful network attachments or applications, and

---

<sup>24</sup> Thomas B. Nachbar, *The Public Network*, 17 COMMLAW CONSPECTUS 67, 123 (2008). Nachbar continues:

Because discrimination in modern communications networks can take place along so many lines, “network neutrality” is a necessarily vague concept, potentially signifying any number of limits on discrimination, whether user- or use-based, and applied either to business arrangements or technologies. Any network will discriminate against some uses as compared to others—the Internet’s failure to accommodate service level guarantees discriminates against streaming video in favor of e-mail—and what is “neutral” to one party may not seem so to another. Not only is neutrality technically contingent, it’s socially contingent.

*Id.* at 112 (footnotes omitted).

<sup>25</sup> April Glaser, *Comcast Wants You to Think It Supports Net Neutrality While It Pushes for Net Neutrality to Be Destroyed*, SLATE (Nov. 28, 2017), <https://slate.com/technology/2017/11/comcast-wants-you-to-think-it-supports-net-neutrality-while-it-pushes-for-net-neutrality-to-be-destroyed.html>.

<sup>26</sup> Jon Reid, *2019 Outlook: Net Neutrality ‘Ping Pong’ Battle to Rage on*, BLOOMBERG LAW (Dec. 27, 2018), <https://news.bloomberglaw.com/tech-and-telecom-law/2019-outlook-net-neutrality-ping-pong-battle-to-rage-on>.

<sup>27</sup> *HTTP Status Code Registry*, *supra* note 18.

<sup>28</sup> Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. ON TELECOMM. & HIGH TECH. L. 141, 145 (2003) (defining a “neutral network” as one that does not “favor one application . . . over others”). This original definition offers minimal guidance on some of the forms of practices that trouble various network neutrality advocates today, such as the question of tiers of service at variable speeds.

<sup>29</sup> *Id.*

give innovators the corresponding freedom to supply them.”<sup>30</sup> Wu analogized the Internet to another network, the electric grid, stating: “[t]he electric grid does not care if you plug in a toaster, an iron, or a computer.”<sup>31</sup>

Significant conceptual overlap exists in many (though not all) network neutrality proponents’ understanding of the types of “wrongs” that a network neutrality approach seeks to address. The common network neutrality intuitions shared by proponents generally relate to their concerns over packet and device discrimination by intermediaries in a network. These concerns have primarily included the risk of selective, often undisclosed,<sup>32</sup> throttling<sup>33</sup> or degradation<sup>34</sup> of content based on the nature of the communication, discrimination based on the equipment used<sup>35</sup> or the identity of the packet sender or recipient,<sup>36</sup> creation of tiers of service that extract additional fees,<sup>37</sup> and privileging the communications of the people willing to pay more over the communications of others.<sup>38</sup> These two shared understandings might be viewed as generally arising from preserving the technical

---

<sup>30</sup> *Id.* at 142 (emphasis omitted).

<sup>31</sup> Tim Wu, *Network Neutrality FAQ*, TIMWU.ORG, [http://www.timwu.org/network\\_neutrality.html](http://www.timwu.org/network_neutrality.html) (last visited Oct. 3, 2019).

<sup>32</sup> As explained succinctly by Professor Andrew Odlyzko, “[c]ompanies engaging in discriminatory practices try to conceal it, dissemble when caught, and cite various seemingly less objectionable objectives (safety, performance. . .) as the reasons for their policies. Very seldom do they come out and admit what they are doing.” ANDREW ODLYZKO, NETWORK NEUTRALITY, SEARCH NEUTRALITY, AND THE NEVER-ENDING CONFLICT BETWEEN EFFICIENCY AND FAIRNESS IN MARKETS 3 (2009).

<sup>33</sup> Christina Bonnington, *Surprise, Surprise: Comcast is Already Throttling Users*, DAILY DOT (July 2, 2018), <https://www.dailydot.com/debug/comcast-throttling-Internet-speeds/>.

<sup>34</sup> Andrew Webster, *Major ISPs Accused of Deliberately Throttling Traffic*, VERGE (May 6, 2014), <https://www.theverge.com/2014/5/6/5686780/major-isps-accused-of-deliberately-throttling-traffic>; see also Pedro Casas et al., *Unveiling Network and Service Performance Degradation in the Wild with Mplane*, 54 IEEE COMM. MAG. 71 (Mar. 2016) (proposing a technical method for measuring and identifying potential causes of internet degradation).

<sup>35</sup> Ed Felten, *Nuts and Bolts of Net Discrimination: Encryption*, FREEDOM TO TINKER (Mar. 21, 2006), <https://freedom-to-tinker.com/2006/03/21/nuts-and-bolts-net-discrimination-encryption/>.

<sup>36</sup> Olga Kharid, *YouTube, Netflix Videos Found to Be Slowed by Wireless Carriers*, BLOOMBERG (Sept. 4, 2018), <https://www.bloomberg.com/news/articles/2018-09-04/youtube-and-netflix-throttled-by-carriers-research-finds>.

<sup>37</sup> Brad Reed, *Net Neutrality vs. Tiered Services*, NETWORKWORLD (Oct. 26, 2007), <https://www.networkworld.com/article/2287516/-net-neutrality-vs--tiered-services.html>.

<sup>38</sup> Tom Geoghegan, *Why is Broadband More Expensive in the US?*, BBC NEWS (Oct. 28, 2013), <https://www.bbc.com/news/magazine-24528383>.

Internet design principles<sup>39</sup> of the end-to-end<sup>40</sup> principle,<sup>41</sup> a four-layer model of Internet architecture,<sup>42</sup> and the openness of Internet protocols.<sup>43</sup> When framed together, these two sets of concerns—avoiding discrimination and preserving the Internet’s original technical design principles—generally comprise the bundle of issues debated as part of network neutrality.<sup>44</sup>

---

<sup>39</sup> For a discussion of a portion of these design principles, see Kevin Werbach, *The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart*, 42 U.C. DAVIS L. REV. 343, 373–77 (2008).

<sup>40</sup> Professor Lawrence Lessig and Professor Robert McChesney argue that “the simple but brilliant ‘end-to-end’ design of the Internet [has] made it such a powerful force for economic and social good.” Lawrence Lessig & Robert W. McChesney, *No Tolls on the Internet*, WASH. POST (June 8, 2006), <http://www.washingtonpost.com/wp-dyn/content/article/2006/06/07/AR2006060702108.html>.

<sup>41</sup> Professor David Post advocates for end-to-end, neutral network principles, arguing that the ease of adding similarly functioning endpoints increases the potential of the system as a whole. See DAVID G. POST, IN SEARCH OF JEFFERSON’S MOOSE: NOTES ON THE STATE OF CYBERSPACE 80–89 (2009).

<sup>42</sup> Most policy discussions of Internet layer architecture today simplify into four layers: the physical infrastructure layer, the logical or code layer, the applications layer, and the content layer. Davina Sashkin, *Failure of Imagination: Why Inaction on Net Neutrality Regulation Will Result in A De Facto Legal Regime Promoting Discrimination and Consumer Harm*, 15 COMMLAW CONSPECTUS 261, 270 (2006).

<sup>43</sup> As explained by the FCC, the Internet is a “global, packet-switched network of networks that are interconnected through the use of the common network protocol—IP.” In the Matter of IP-Enabled Services, 19 FCC Rcd. 4863, 4868 n.23 (2004).

<sup>44</sup> Vinton Cerf explained this combination as follows:

This “neutral” network has supported an explosion of innovation at the edges of the network, and the growth of companies like Google, Yahoo, eBay, Amazon, and many others. Because the network is neutral, the creators of new Internet content and services need not seek permission from carriers or pay special fees to be seen online. As a result, we have seen an array of unpredictable new offerings—from Voice-over-IP to wireless home networks to blogging—that might never have evolved had central control of the network been required by design.

Vinton G. Cerf, *Prepared Statement of Vinton G. Cerf—Hearing on “Network Neutrality,”* PARAGRAPH (Feb. 07, 2016), <https://theparagraph.com/documents/prepared-statement-of-vinton-g-cerf-hearing-on-%E2%80%9Cnetwork-neutrality%E2%80%9D/>.



However, even Professor Wu himself acknowledges that:

Neutrality, as a concept, is finicky, and depends entirely on what set of subjects you choose to be neutral among. A policy that appears neutral in a certain time period, like “all men may vote,” may lose its neutrality in a later time period, when the range of subjects is enlarged.<sup>45</sup>

To wit, this finicky nature of neutrality has resulted in numerous scholarly debates about the possibility and modalities of operationalizing the concept of network neutrality, ultimately arriving at a policy impasse. Thus, net neutrality joins a list of other well-worn technology policy frameworks that faltered in implementation.<sup>46</sup>

Technology history teaches us that effectively translating technology terminology and related normative design values into workable policy and legal frameworks always presents a formidable challenge.<sup>47</sup> Similarly, policy impasse often signals a need for a critical reevaluation and, possibly, a conceptual reframing of the debate. Indeed, many technology law regimes have struggled with this task (and failed in varying degrees). For example, the key terms of Section 1201 of the Digital Millennium Copyright Act (“DMCA”)<sup>48</sup> and the Computer Fraud and Abuse Act (“CFAA”)<sup>49</sup> both bear the scars (and circuit splits)<sup>49</sup> of imperfect technical-legal translation.<sup>50</sup> While the DMCA’s approach has improved across time and the United States Copyright Office has clarified some definitional ambiguities,<sup>51</sup> the CFAA’s approach has arguably become less effective and even more definitionally vague, necessitating legislative update.<sup>52</sup>

---

<sup>45</sup> Wu, *supra* note 28, at 147–48 (footnote omitted).

<sup>46</sup> See *infra* Section II.B.

<sup>47</sup> For a discussion of the formidable definitional challenges presented by the Computer Fraud and Abuse Act, see generally Andrea M. Matwyshyn & Stephanie K. Pell, *Broken*, 32 HARV. J.L. & TECH. 481–502 (2019).

<sup>48</sup> See Matwyshyn, *supra* note 3, at 1146 (offering “a cautionary tale of how lawyers’ faux-technical words end badly for security”); Andrea M. Matwyshyn, *Cyber Harder*, 24 B.U. J. SCI. & TECH. L. 450, 465–68 (2018).

<sup>49</sup> See Andrea M. Matwyshyn, *The Law of the Zebra*, 28 BERKELEY TECH. L.J. 156, 156 (2013).

<sup>50</sup> See Matwyshyn & Pell, *supra* note 47, at 517–18.

<sup>51</sup> *Id.* at 533–34.

<sup>52</sup> *Id.* at 481.

Mirroring some of the definitional challenges visible in these other technology law contexts, various network neutrality implementation specifics can diverge in irreconcilable ways. Scholarly opinions begin to significantly differ on particular points, even among proponents of network neutrality.<sup>53</sup> As Professor Frank Pasquale notes, “scholars tend to model Internet communications as a form of transport of information” and argue that it should be subject to common carriage rules<sup>54</sup>—a metaphor and a substantive characterization, which “may raise as many questions about broadband governance as it answers.”<sup>55</sup> In particular, scholarly opinions vary in their assessments of the desirability of various particular network management

---

<sup>53</sup> For example, although Professor Wu’s original article offered a draft statute, the definitional vagueness in its drafting may have limited the possibility of meaningful implementation. *See* Wu, *supra* note 28, at 172.

<sup>54</sup> For example, Professor Brett Frischmann argues that networks are a form of infrastructure similar to roads, bridges, and public transport. *See* Brett Frischmann, *Why the FCC Should Prevent ISPs from Micromanaging Our Lives*, FREEDOM TO TINKER (Dec. 12, 2017), <https://freedom-to-tinker.com/2017/12/12/why-the-fcc-should-prevent-isps-from-micromanaging-our-lives/>.

<sup>55</sup> Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 NW. U. L. REV. 105, 128 (2010).

practices,<sup>56</sup> competition concerns,<sup>57</sup> pricing models,<sup>58</sup> and other business model specifics. For example, scholarly opinions differ<sup>59</sup> on the desirability<sup>60</sup> of the

---

<sup>56</sup> As explained by Professor Andrew Odlyzko:

What is acknowledged, whether explicitly or implicitly, in most discussions of net neutrality is that the basic issue is of price discrimination. There are frequent claims about the need to manage network traffic, but when one gets deeper into them, one typically finds complaints about “5% of the users generating 50% of the traffic” and the like, which have less to do with providing adequate service, and more with a way to apportion the cost. And the usual practices that have been observed have tended to be more about restricting some applications than about managing congestion, say.

Andrew Odlyzko, *Network Neutrality, Search Neutrality, and the Never-Ending Conflict Between Efficiency and Fairness in Markets*, 8 REV. NETWORK ECON. 40, 41–42 (2009).

<sup>57</sup> Professor Barbara van Schewick has stated that “increasing the amount of application-level innovation through network neutrality regulation is more important than the costs associated with it.” See Dr.-Ing. Barbara van Schewick, Ass. iur., *Towards an Economic Framework for Network Neutrality Regulation*, 5 J. TELECOMM. & HIGH TECH. L. 329, 329 (2007). She warns that, without network neutrality rules, network operators would potentially elevate the accessibility of partners’ applications and content, degrading access to competitors’ applications. *Id.* at 390. Professor Brett Frischmann and Professor Barbara van Schewick argue in favor of network neutrality structured as an “infrastructure commons” to “insulat[e] end users from market-driven restrictions on access and use.” See Brett M. Frischmann & Barbara van Schewick, *Network Neutrality and the Economics of an Information Superhighway: A Reply to Professor Yoo*, 47 JURIMETRICS J. 383, 386 (2007). They assert that nondiscrimination principles at an infrastructural layer are necessary for ensuring innovation in the layers that run on top of it and they note a disconnect between ISP profit maximization and maximization of the overall social gains that unrestricted Internet access can generate. *Id.* Professor Larry Lessig and Professor Mark Lemley similarly argue that, as ISPs expand beyond the functions they have traditionally performed, an ISP might be in a position to foreclose all competition in an increasing range of services and users would then be determined by the captive ISPs owned by each local cable company, which would contradict the principle that the network should remain neutral and empower users. See Mark A. Lemley & Lawrence Lessig, *Open Access to Cable Modems*, 22 WHITTIER L. REV. 3, 19 (2000).

<sup>58</sup> In the context of United Kingdom and European Union debates over network neutrality, Professor Christopher Marsden argues that types of discriminatory (non-neutral) behaviors by ISPs that pose harm to consumer welfare are primarily non-transparency and misleading advertising, “throttling” or blocking, charging, certain types of more extreme and anti-competitive “walled gardens.” Christopher T. Marsden, *Net Neutrality: The European Debate*, 12 J. INTERNET L. 1, 7 (2008). With respect to non-transparency, Professor Marsden highlights that “certain programs are being throttled . . . [and] a [potentially illegitimate] security justification is used and is often unchallenged by regulators.” *Id.* at 8. Marsden views blocking and throttling to constitute “the furthest deviation from neutrality.” *Id.* He explains that while some economists think it justified, it results in a potential distortion of competition between the blocked and unblocked companies in practice. *Id.* Further, Marsden highlights that these practices generate “confusion among users as to whether and how content is throttled” and that “[c]ertain types of traffic that

practice<sup>61</sup> of zero-rating.<sup>62</sup> Still other scholars who support network neutrality in principle have argued that certain circumstances warrant exceptions to a baseline of network neutrality,<sup>63</sup> focusing instead on the broader role of Internet intermediaries.<sup>64</sup>

Meanwhile, as Professor Pasquale also explains, “net neutrality’s opponents have been promoting competition as a cure-all for years.”<sup>65</sup> Indeed, opponents of network neutrality argue that a “fast lane” of Internet access is needed to defray the costs of infrastructural improvement and that price discrimination is the best way to

---

are highly valued by the end-user of the Internet can be discriminated against in whole or in part by service providers.” *Id.* In particular, Marsden highlights the risk of an “arms race” in blocking and throttling technologies, with the end-users potentially bearing the costs. *Id.*

<sup>59</sup> Professor Ellen Goodman argues that “depending on how [zero-rating] offers are structured, they can be anti-competitive and violate net neutrality norms of open access . . . [or] they may also subsidize broadband access and increase expressive opportunities for users.” Ellen P. Goodman, *Zero-Rating Broadband Data: Equality and Free Speech at the Network’s Other Edge*, 15 COLO. TECH. L.J. 63, 63 (2016).

<sup>60</sup> Professor Rob Frieden points to the need for “a speedy and fair complaint resolution process to remedy content carriage disputes.” Rob Frieden, *Freedom to Discriminate: Assessing the Lawfulness and Utility of Biased Broadband Networks*, 20 VAND. J. ENT. & TECH. L. 655, 655 (2018).

<sup>61</sup> Some authors see the practice as inherently negative, while others view the practice as largely beneficial and deem a majority of objections unconvincing. For example, Professor Scott Hemphill “differentiates two access provider strategies thought to justify a zero-price rule.” C. Scott Hemphill, *Network Neutrality and the False Promise of Zero-Price Regulation*, 25 YALE J. ON REG. 135, 135 (2008). Hemphill claims the following: “Exclusion is anticompetitive behavior that harms a content provider to favor its rival. Extraction is a toll imposed upon content providers to raise revenue. Neither strategy raises policy concerns that justify implementation of a broad zero-price rule.” *Id.*

<sup>62</sup> As explained by Professor Goodman, “[w]hen broadband providers ‘zero-rate’ data, they offer certain services or buckets of data for free without counting consumption against the user’s data caps.” Goodman, *supra* note 59, at 63.

<sup>63</sup> For example, Professor Jonathan Zittrain is focused on API neutrality rather than network neutrality, recommending deviation from neutrality principles to address certain cases. JONATHAN ZITTRAIN, *THE FUTURE OF THE INTERNET AND HOW TO STOP IT* 67 (2008). In particular, he argues that new intermediaries are needed to help address security issues, even though such intermediaries render the network non-neutral, containing and isolating packets deemed to be security threats. *Id.*

<sup>64</sup> Zittrain was not alone in his consideration of intermediaries. See, e.g., Yochai Benkler, *Communications Infrastructure Regulation and the Distribution of Control over Content*, 22 TELECOMM. POL’Y 183, 185–86 (1998) (describing intermediaries and information flow: “technology, institutional framework, and organizational adaptation . . . determine . . . who can produce information, and who may or must consume, what type of information, under what conditions, and to what effect?”).

<sup>65</sup> Pasquale, *supra* note 55, at 151.

ensure efficient allocation of Internet access.<sup>66</sup> They analogize Internet network congestion to the difference between the consumer-facing services<sup>67</sup> provided by the United States Postal Service and a hypothetically speedier private carrier,<sup>68</sup> arguing that broadband policy should allow network providers to experiment with different institutional forms until it can be shown that a particular practice is actively “harming competition.”<sup>69</sup> However, current market reality forces us to question the accuracy of these scholars’ core underlying assumption: the assumption that a baseline of meaningful competition currently exists. Both the FCC’s data<sup>70</sup> and extensive consumer complaints<sup>71</sup> signal that competition<sup>72</sup> among broadband providers appears to be impoverished, at best.<sup>73</sup> Indeed, the FCC’s data shows that approximately 50% of Americans are served by only one or zero wireline broadband service providers meeting the current FCC speed benchmark of 25 megabits-per-second download and 3 megabits-per-second upload.<sup>74</sup> Rural broadband is sporadic at best.<sup>75</sup> But even in

---

<sup>66</sup> See, e.g., Christopher S. Yoo, *Beyond Network Neutrality*, 19 HARV. J.L. & TECH. 1, 8–9 (2005).

<sup>67</sup> These opponents do not consider the role that USPS plays in national security and that private providers are not similarly situated. See *infra* Section IV.

<sup>68</sup> Christopher S. Yoo, *Network Neutrality, Consumers, and Innovation*, 2008 U. CHI. LEGAL F. 179, 232 (2008); Yoo, *supra* note 66, at 54. However, the speed of service for USPS and private carriers are substantially comparable in practice. For example, both FedEx and USPS offer overnight service. *Compare Overnight Shipping and Delivery*, FEDEX, <https://www.fedex.com/en-us/shipping/overnight.html> (last visited Oct. 3, 2019), with *Priority Mail Express*, USPS, <https://www.usps.com/ship/priority-mail-express.htm> (last visited Oct. 3, 2019).

<sup>69</sup> Yoo, *supra* note 66, at 75.

<sup>70</sup> Brief of Internet Association et al., Intervenor-Petitioners, Mozilla Corp. v. Fed. Comm’n Comm’n, 2019 WL 4777860 (D.C. Cir. 2019) (No. 18-1051).

<sup>71</sup> See, e.g., *21 Times Comcast Was the Worst Company in America*, BILLFIXERS (June 8, 2016), <https://billfixers.com/blog/21-times-comcast-worst-company-america>.

<sup>72</sup> For example, consumers are not empowered to bargain for better terms such as more privacy. See Pasquale, *supra* note 55, at 152. Pasquale cites Professor Paul Ohm, who explains that that “ISPs, faced with changes in technology, extraordinary pressures to increase revenues, and murky ethical rules, will continue aggressively to expand network monitoring.” *Id.* (citing Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1426 (2009)).

<sup>73</sup> Pasquale, *supra* note 55, at 152.

<sup>74</sup> Brief of Internet Association et al., *supra* note 70, at 11–12.

<sup>75</sup> Monica Anderson, *About a Quarter of Rural Americans Say Access to High-Speed Internet is a Major Problem*, PEW RES. CTR. (Sept. 10, 2018), <https://www.pewresearch.org/fact-tank/2018/09/10/about-a-quarter-of-rural-americans-say-access-to-high-speed-internet-is-a-major-problem/>; April Simpson, *State Laws Slow Down High-Speed Internet for Rural America*, PEW RES. CTR. (Jan. 11, 2019), <https://>

densely-populated cities such as Chicago,<sup>76</sup> historically some residents have perceived themselves to have only one option for broadband access.<sup>77</sup> Thus, meaningful competition and redundancy of choice in Internet access appears to be aspirational fiction rather than experienced market reality in many parts of the United States.

Other opponents, including FCC Commissioners,<sup>78</sup> have raised First Amendment concerns, warning that net neutrality threatens to “neuter the First Amendment in the digital age.”<sup>79</sup> However, as Professor Jack Balkin explains, although

under current First Amendment doctrine, at least, the Constitution does not require network neutrality . . . [but the] argument that network neutrality rules actually violate the First Amendment . . . [also] do[es not] succeed; network neutrality rules treat network providers as conduits for the speech of others and regulate them in their capacity as conduits.<sup>80</sup>

He elaborates that “[i]f network neutrality violates the First Amendment, it is hard to see why common carrier obligations for phone companies—which are also treated

---

[www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2019/01/11/state-laws-slow-down-high-speed-internet-for-rural-america](http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2019/01/11/state-laws-slow-down-high-speed-internet-for-rural-america).

<sup>76</sup> See email from Miluska Novota (on file with author) (confirming that in her experience formerly living in Chicago zip code 60646, at least some portions of this zip code historically had only one option for broadband access).

<sup>77</sup> *Id.*

<sup>78</sup> See Michael O’Rielly, Comm’r, Fed. Comm’n Comm’n, Remarks at Media Institute “Free Speech America” Gala (Oct. 24, 2018), <https://docs.fcc.gov/public/attachments/DOC-354770A1.pdf> (“In addition to creating competitive distortions and misdirecting scarce resources that should go to bringing broadband to the truly unserved areas, municipal broadband networks have engaged in significant First Amendment mischief. As Professor Enrique Armijo of the Elon University School of Law has shown in his research, municipalities such as Chattanooga, Tennessee, and Wilson, North Carolina, have been notorious for their use of speech codes in the terms of service of state-owned networks, prohibiting users from transmitting content that falls into amorphous categories like ‘hateful’ or ‘threatening.’ These content-based restrictions, implicating protected categories of speech, would never pass muster under strict scrutiny. In addition to conditioning network use upon waiver of the user’s First Amendment rights, these terms are practically impossible to interpret objectively, and are inherently up to the whim of a bureaucrat’s discretion. How frightening.”).

<sup>79</sup> Randolph J. May, *Net Neutrality Mandates: Neutering the First Amendment in the Digital Age*, 3 I/S: J.L. & POL’Y FOR INFO. SOC’Y 197, 210 (2007).

<sup>80</sup> Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 429–30 (2009).

as conduits for the speech of others—do not violate the First Amendment as well,”<sup>81</sup> a presumably undesirable result.

But, perhaps most glaringly, in addition to these definitional and implementational concerns, policy and market(ing) reality begs for a reboot of “network neutrality.” As a practical matter, the usefulness of the term “network neutrality” itself appears to have also run its course. “Network neutrality” has arguably descended into the status of a “buzzword bingo”<sup>82</sup> DC Beltway insider incantation—a type of recognizable, soothing phrase used by both opponents and proponents alike to prevent public maelstrom<sup>83</sup>—rather than a shared reference to a particular set of concrete policy and legal proposals. Or, as explained by Professor Susan Crawford, “[l]anguage matters: ‘Net neutrality’ causes eyes to glaze and attention to wander.”<sup>84</sup> Indeed, members of Congress who both support and oppose the concepts identified by net neutrality proponents are now introducing various “net neutrality” laws to leverage public recognition of this term.<sup>85</sup> Similarly, Internet Service Providers (“ISPs”) now claim to support “net neutrality,” which at least one defines as “enforceable Open Internet protections without relying on rigid, innovation-killing utility regulation that was developed in the 1930s.”<sup>86</sup> In other words, some versions of “network neutrality” present a circular definition that mandates a particular legal outcome that is not in line with the aspirations of most net neutrality proponents.

---

<sup>81</sup> *Id.* at 430.

<sup>82</sup> Geoffrey James, *How to Play Buzzword Bingo*, INC. (Mar. 2, 2012), <https://www.inc.com/geoffrey-james/how-to-play-buzzword-bingo.html>.

<sup>83</sup> Kate Cox, *No, AT&T, Comcast, and Verizon Are Not Suddenly in Favor of Net Neutrality*, CONSUMER REP. (July 12, 2017), <https://www.consumerreports.org/consumerist/no-att-comcast-and-verizon-are-not-suddenly-in-favor-of-net-neutrality/>. The corporate and government sensitivity to the term “network neutrality” arose in part because of the public response to a television segment by comedian John Oliver, which elicited a response from then FCC Chairman Wheeler, stating “I am not a dingo.” Amy Schatz, *FCC’s Wheeler on Viral Net Neutrality Video: “I Am Not a Dingo,”* VOX (June 13, 2014), <https://www.vox.com/2014/6/13/11627962/fccs-wheeler-on-viral-net-neutrality-video-i-am-not-a-dingo>.

<sup>84</sup> Susan Crawford, *Net Neutrality is Just a Gateway to the Real Issue: Internet Freedom*, WIRED (May 18, 2018), <https://www.wired.com/story/net-neutrality-is-just-a-gateway-to-the-real-issue-internet-freedom/>.

<sup>85</sup> Dell Cameron, *The GOP Is Introducing More Fake Net Neutrality Bills*, GIZMODO (Feb. 7, 2019), <https://gizmodo.com/gop-lawmakers-introduce-another-fake-net-neutrality-bil-1832431221>.

<sup>86</sup> David L. Cohen, *Comcast Supports Net Neutrality on the Internet Day of Action*, COMCAST (July 12, 2017), <https://corporate.comcast.com/comcast-voices/on-the-Internet-day-of-action-comcast-supports-net-neutrality>.

The imprecision and lexical gaming surrounding the term “network neutrality” has also contributed to the undesirable narrowing of the policy conversation around Internet infrastructure. In particular, “network neutrality” has artificially cabined the framing of the discussion in a manner fixated on the role of the FCC.<sup>87</sup> In this way, it has distracted policy from other fruitful legal avenues to bolster the creation of a successful next generation United States Internet infrastructure. As the next section explains, as legal scholars and policy experts alike have struggled with finding a workable definition of network neutrality. So too has the FCC, ultimately reversing itself on its network neutrality posture and culminating in agency paralysis.

*B. Error 505<sup>88</sup>: Network Neutrality Version Not Supported*

The role of the FCC in the first two decades of the network neutrality debate has been checkered,<sup>89</sup> and the agency’s position on the topic might be described as indecisive and uncertain. As former Commissioner Tate explained, while her first question to counsel involved the definition of network neutrality, her second question asked “what is the basis of the FCC’s legal authority to establish net neutrality regulations?”<sup>90</sup> Indeed, it is this question that has caused decades of contention among FCC Commissioners and courts alike.

The first hints of FCC activity on network neutrality might be traced to a talk given by Chairman Michael Powell in 2004, where he challenged “the broadband network industry to preserve the . . . Internet freedoms [of] . . . Freedom to Access Content, Freedom to Use Applications, Freedom to Attach Personal Devices, and Freedom to Obtain Service Plan Information.”<sup>91</sup> Shortly thereafter, in 2005, the Supreme Court in *National Cable & Telecomms. Ass’n v. Brand X Internet Services*<sup>92</sup> affirmed the FCC determination that broadband ISPs are not regulated common

---

<sup>87</sup> See *infra* notes 286–307 and accompanying text.

<sup>88</sup> *HTTP Status Code Registry*, *supra* note 18.

<sup>89</sup> FCC Commissioners have often been opposed to the FCC’s involvement in network neutrality regulatory undertakings. See, e.g., O’Rielly, *supra* note 78.

<sup>90</sup> Tate, *supra* note 19, at 517.

<sup>91</sup> Michael K. Powell, Chairman, Fed. Comm’n Comm’n, Remarks at the University of Colorado School of Law Silicon Flatirons Symposium: The Digital Broadband Migration: Toward a Regulatory Regime for the Internet Age (Feb. 8, 2004) (“I challenge the broadband network industry to preserve the following Internet Freedoms: Freedom to Access Content; Freedom to Use Applications; Freedom to Attach Personal Devices; Freedom to Obtain Service Plan Information.”).

<sup>92</sup> *Nat’l Cable & Telecomms. v. Brand X Internet Servs.*, 545 U.S. 967 (2005).



carriers.<sup>93</sup> Thus, ISPs were deemed not subject to the requirement to carry all messages neutrally and to grant compelled access.<sup>94</sup> In particular, the Court explained that “[w]here a statute’s plain terms admit of two or more reasonable ordinary usages, the Commission’s choice of one of them is entitled to deference.”<sup>95</sup>

On the heels of *Brand X*, in September 2005, the FCC released a broadband plan containing a set of network neutrality principles comprised of the following:

[(1)] To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to access the lawful Internet content of their choice; [(2)] To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement; [(3)] To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to connect their choice of legal devices that do not harm the network; [(4)] To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to competition among network providers, application and service providers, and content providers.<sup>96</sup>

---

<sup>93</sup> In the underlying Ninth Circuit case, the court explained:

The first group of petitioners argues that cable modem service is both an information service and a telecommunications service and is therefore subject to regulation on a common-carriage basis. The second group of petitioners asserts that cable modem service is both an information service and a cable service, and therefore is subject to regulation by local authorities as provided in the Act. The final petitioner, Verizon, advances a third variation on “the FCC did not go far enough” theme, arguing that the Commission was correct to classify cable modem service as solely an information service, but should have taken the additional step of conferring the same designation on the DSL service provided by telephone companies.

*Brand X Internet Servs. v. FCC*, 345 F.3d 1120, 1127 (9th Cir. 2003) (footnotes omitted).

<sup>94</sup> *Nat’l Cable & Telecomms.*, 545 U.S. at 987–88.

<sup>95</sup> *Id.* at 989.

<sup>96</sup> Fed. Comm’n Comm’n, Policy Statement on Broadband Access to the Internet Over Wireline Facilities, 20 FCC Rcd. 14986 (2005) (emphasis omitted).

This policy was ultimately embodied in an Open Internet Order issued in 2010,<sup>97</sup> which highlighted the three principles of transparency, no blocking, and no unreasonable discrimination.<sup>98</sup>

In April 2010, in *Comcast v. FCC*, the Federal Court of Appeals overturned an action taken by the FCC against Comcast Corp.<sup>99</sup> The FCC had reprimanded Comcast for throttling peer-to-peer traffic among users on its network, although it had chosen not to levy fines against Comcast for the practice because the company voluntarily complied with the order.<sup>100</sup> The FCC argued that this type of network management ran afoul of both its broadband plan and congressional statements of policy, but the argument was deemed unconvincing by the court.<sup>101</sup> Next, in July

---

<sup>97</sup> Preserving the Open Internet Order, 25 FCC Rcd. 17905, 17906 (2010), *aff'd in part, vacated and remanded in part* Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014).

<sup>98</sup> *Id.* The principles are defined as follows:

- i. Transparency. Fixed and mobile broadband providers must disclose the network management practices, performance characteristics, and terms and conditions of their broadband services;
- ii. No blocking. Fixed broadband providers may not block lawful content, applications, services, or non-harmful devices; mobile broadband providers may not block lawful websites, or block applications that compete with their voice or video telephony services; and
- iii. No unreasonable discrimination. Fixed broadband providers may not unreasonably discriminate in transmitting lawful network traffic.

*Id.* (emphases omitted).

<sup>99</sup> Comcast Corp. v. FCC, 600 F.3d 642, 644 (D.C. Cir. 2010).

<sup>100</sup> *Id.* at 645.

<sup>101</sup> However, in finding for Comcast, the court noted that the FCC:

[a]cknowledg[ed] that it has no express statutory authority over such practices, the Commission relies on section 4(i) of the Communications Act of 1934, which authorizes the Commission 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. The Commission may exercise this “ancillary” authority only if it demonstrates that its action—here barring Comcast from interfering with its customers’ use of peer-to-peer networking applications—is “reasonably ancillary to the . . . effective performance of its statutorily mandated responsibilities. . . . [The Commission] relies principally on several Congressional statements of policy . . . [and] various provisions of the Communications Act that do create such responsibilities, but for a variety of substantive and procedural reasons those provisions cannot support its exercise of ancillary authority over Comcast’s network management practices.

2012, the FCC released an order adopting a consent decree with Verizon, ordering the company to pay a fine of \$1.25 million in connection with the filtering of applications from the Verizon store that allowed for customer tethering to their phones, a service for which Verizon was charging an extra fee.<sup>102</sup> Then, in 2014, as a consequence of Verizon's challenge to the 2010 Open Internet Order, the D.C. Circuit Court of Appeals explained in *Verizon v. FCC* that the Communications Act "subjects telecommunications carriers, but not information-service providers, to Title II common carrier regulation."<sup>103</sup>

As a consequence of these rulings, in 2015, FCC Chairman Tom Wheeler announced the Open Internet Order of 2015, which he described as a "light-touch

---

*Id.* at 644 (internal citations, quotation marks omitted).

<sup>102</sup> Cellco P'ship, 27 FCC Rcd. 8932 (2012) (consent decree), <https://docs.fcc.gov/public/attachments/DA-12-1228A1.pdf>.

Verizon Wireless's customer agreements in place in 2011 required that subscribers, both those on unlimited data plans and those on usage-based plans, pay an additional monthly fee if they tethered additional devices to their smartphones. Verizon Wireless referred to this feature as Mobile Broadband Connect. In April 2011, Verizon Wireless asked an Application Store Operator to filter from its Application Store eleven tethering Applications that customers could use to tether without paying Verizon Wireless's monthly tethering fee. The Application Store Operator subsequently filtered those Applications so that Verizon Wireless customers could no longer access them through the Application Store.

*Id.*

<sup>103</sup> *Verizon v. FCC*, 740 F.3d 623, 628 (D.C. Cir. 2014) (citing 47 U.S.C. § 153(53) (2011)); see *Nat'l Cable & Telecomms. v. Brand X Internet Servs.*, 545 U.S. 967, 975–76 (2005). The D.C. Circuit in *Verizon* highlighted:

[T]he Commission has established that section 706 of the Telecommunications Act of 1996 vests it with affirmative authority to enact measures encouraging the deployment of broadband infrastructure . . . [and] has reasonably interpreted section 706 to empower it to promulgate rules governing broadband providers' treatment of Internet traffic, and its justification for the specific rules at issue here—that they will preserve and facilitate the "virtuous circle" of innovation that has driven the explosive growth of the Internet—is reasonable and supported by substantial evidence.

*Verizon*, 740 F.3d at 628. However, the court vacated part of the Open Internet Order. *Id.* ("Given that the Commission has chosen to classify broadband providers in a manner that exempts them from treatment as common carriers . . . the Commission has failed to establish that the anti-discrimination and anti-blocking rules do not impose per se common carrier obligations.").

regulatory framework” and Title II “for the 21st Century,”<sup>104</sup> reclassifying broadband Internet access service as a “telecommunications service” under Title II of the Communications Act of 1934.<sup>105</sup> According to Chairman Tom Wheeler, the 2015 Order was designed to enforce “carefully-tailored” open Internet rules to protect and promote broadband innovation and investment through the enforcement of three bright-line rules: no blocking,<sup>106</sup> no throttling,<sup>107</sup> and no paid prioritization.<sup>108</sup> However, this Order’s effect was ultimately short-lived. The telecommunications industry immediately challenged the 2015 Order in the courts,<sup>109</sup> and in 2016, FCC Chairman Ajit Pai defied public opinion in favor of the 2015 Order<sup>110</sup> and announced the agency’s reversal of its position on network neutrality in the FCC’s Restoring Internet Freedom Order.<sup>111</sup> In response to this reversal, a group of plaintiffs, led by Mozilla, challenged the FCC’s 2016 Restoring Internet Freedom Order.<sup>112</sup> Meanwhile, the 2015 litigation also continued, and, in *U.S. Telecom. Ass’n v.*

---

<sup>104</sup> Tom Wheeler, *This is How We Will Ensure Net Neutrality*, WIRED (Feb. 4, 2015), <https://www.wired.com/2015/02/fcc-chairman-wheeler-net-neutrality/>.

<sup>105</sup> Protecting and Promoting the Open Internet, 79 FCC Rcd. 37447 (2015).

<sup>106</sup> No Blocking: “A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not block lawful content, applications, services, or non-harmful devices, subject to reasonable network management.” *Id.* ¶ 15.

<sup>107</sup> No Throttling: “A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not impair or degrade lawful Internet traffic on the basis of Internet content, application, or service, or use of a non-harmful device, subject to reasonable network management.” *Id.* ¶ 16.

<sup>108</sup> No Paid Prioritization: “A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not engage in paid prioritization.” *Id.* ¶ 18.

<sup>109</sup> *U.S. Telecom. Ass’n v. FCC*, 825 F.3d 674 (D.C. Cir. 2016) (challenging the validity of the Open Internet Order of 2015).

<sup>110</sup> Studies indicate that an overwhelming majority of Americans do not support a reversal of the 2015 Open Internet Order. Approximately 83% of those Americans surveyed did not support the FCC’s 2016 revisions to the 2015 Open Internet Order. NIELSEN SCARBOROUGH SCH. OF PUB. POLICY, UNIV. OF MD., NET NEUTRALITY SURVEY (2017).

<sup>111</sup> *Restoring Internet Freedom*, FED. COMM’N COMM’N, <https://www.fcc.gov/restoring-Internet-freedom> (last visited Apr. 6, 2019).

<sup>112</sup> Denelle Dixon, *Mozilla Files Arguments Against the FCC—Latest Step in Fight to Save Net Neutrality*, MOZILLA BLOG (Aug. 20, 2018), <https://blog.mozilla.org/blog/2018/08/20/mozilla-files-arguments-against-the-fcc-latest-step-in-fight-to-save-net-neutrality/>.

FCC,<sup>113</sup> the D.C. Circuit Court of Appeals refused to review<sup>114</sup> an underlying decision upholding the 2015 Order.<sup>115</sup> In other words, in a remarkable self-contradiction, in 2016 the FCC found itself simultaneously litigating to defend both the 2015 Order and the 2016 Order—two orders adopting diametrically opposite policy positions. It is fair to say we have now arrived at a network neutrality stalemate at the FCC. Whether the FCC is capable of meaningfully moving discussions of net neutrality forward in the future remains uncertain.

As a wisely programmed computer in a popular movie about the Internet and national security once cautioned, in some games the only winning move is not to play.<sup>116</sup> To wit, the next section argues in favor of a conceptual reframing of the net neutrality conversation around the bigger infrastructure security picture and a role for agencies outside the FCC. It explains the need for better metrics in Internet availability and the creation of access redundancy because of the national security role that the Internet now plays in our society.

---

<sup>113</sup> U.S. Telecom. Ass'n v. FCC, 825 F.3d 674 (D.C. Cir. 2016). Three separate groups of petitioners, consisting primarily of broadband providers and their associations, challenge the 2015 Order, arguing that the FCC lacked statutory authority to reclassify broadband as a telecommunications service, that the FCC's decision was arbitrary and capricious, that the FCC impermissibly classified mobile, broadband as a commercial mobile service, that the Commission impermissibly forbore from certain provisions of Title II, and that some of the rules violate the First Amendment. *Id.*

<sup>114</sup> See Christopher S. Yoo, *Common Carriage's Domain*, 34 YALE J. ON REG. 991 (2018) (“[T]he judicial decision invalidating the Federal Communications Commission’s first Open Internet Order has led advocates to embrace common carriage as the legal basis for network neutrality.”). Professor Yoo argues that “network neutrality proponents have overlooked the academic literature on common carriage as well as lessons from its implementation history” and that “common carriage is not particularly well suited as a basis for regulating broadband Internet access.” *Id.*

<sup>115</sup> *U.S. Telecom Ass'n*, 825 F.3d at 739.

<sup>116</sup> Movieclips, *WarGames Movie Clip-The Only Winning Move*, YOUTUBE (July 30, 2013), <https://www.youtube.com/watch?v=MpmGXeAtWUw> (“A strange game. The only winning move is not to play.”) (WARGAMES (Metro Goldwyn Meyer 1983)).

### III. ERROR 510<sup>117</sup>: NOT (YET) EXTENDED—REFOCUSING ON AVAILABILITY AND REDUNDANCY

“I did not become a vegetarian for my health, I did it for the health of the chickens.”<sup>118</sup>

In 2018, California was devastated by a series of wildfires.<sup>119</sup> As Californians evacuated and the fires burned, the heroic efforts of firefighters to contain the blaze and issue safety communications were hindered by an unexpected foe: unavailability of Internet access.<sup>120</sup> In the midst of the crisis, firefighters in Santa Clara County discovered that their Internet access had deteriorated to a dysfunctional level, and they contacted their ISP, Verizon, to correct the problem.<sup>121</sup> Verizon’s response was not what the firefighters expected.<sup>122</sup>

According to the firefighters, Verizon responded by informing them in the middle of this public safety emergency that Internet access had been throttled because the department had purchased an “incorrect” tier of service: the “unlimited” plan the department had purchased was contractually subject to throttling in the sole discretion of Verizon.<sup>123</sup> The exchange between Verizon and the firefighters was memorialized in a series of progressively more desperate, plaintive emails from the firefighters to Verizon.<sup>124</sup> Even after they explained the gravity of the situation, the firefighters perceived the Verizon representative to be more concerned with

---

<sup>117</sup> *HTTP Status Code Registry*, *supra* note 18.

<sup>118</sup> Michelle Kretzer, *PETA Honors St. Francis and Isaac Bashevis Singer on World Animals*, PETA (Oct. 6, 2016), <https://www.peta.org/blog/peta-honors-st-francis-isaac-bashevis-singer-world-animals-day/>.

<sup>119</sup> Cleve R. Wootson, Jr., *The Deadliest, Most Destructive Wildfire in California’s History Has Finally Been Contained*, WASH. POST (Nov. 26, 2018), <https://www.washingtonpost.com/nation/2018/11/25/camp-fire-deadliest-wildfire-californias-history-has-been-contained/>.

<sup>120</sup> Jon Brodtkin, *Fire Dept. Rejects Verizon’s “Customer Support Mistake” Excuse for Throttling*, ARS TECHNICA (Aug. 22, 2018), <https://arstechnica.com/tech-policy/2018/08/fire-dept-rejects-verizons-customer-support-mistake-excuse-for-throttling/>.

<sup>121</sup> *Id.*

<sup>122</sup> *Id.*

<sup>123</sup> Brief for Government Petitioners, *Mozilla Corp. v. FCC*, 2019 WL 4777860 add. at \*4–6, \*8–14 (D.C. Cir. 2019) (No. 18-1062).

<sup>124</sup> *Id.*

attempting to upsell the department on a higher tier of service than assisting them during the crisis.<sup>125</sup> As explained by the Santa Clara Fire Department, “[t]he Internet has become an essential tool in providing fire and emergency response . . . County Fire has experienced throttling by its ISP, Verizon. This throttling has had a significant impact on our ability to provide emergency services.”<sup>126</sup> In response, Verizon asserted: “‘This was a customer support mistake’ and not a net neutrality issue.”<sup>127</sup> The Fire Department disagreed, stating that “Verizon’s throttling has everything to do with net neutrality—it shows that the ISPs will act in their economic interests, even at the expense of public safety.”<sup>128</sup> Nevertheless, this throttling incident galvanized the California state legislature and citizenry, and net neutrality legislation passed shortly thereafter.<sup>129</sup>

As this incident demonstrates, the stakes of Internet access have changed. Now Internet unavailability is no longer a matter of inconvenience and disappointment over limited access to cat videos;<sup>130</sup> instead, it is a matter of physical safety and,

---

<sup>125</sup> *Id.*

<sup>126</sup> *Id.* at \*5. Moreover, the Santa Clara Fire Department argued:

Verizon imposed these limitations despite being informed that throttling was actively impeding County Fire’s ability to provide crisis-response and essential emergency services. . . . In light of our experience, County Fire believes it is likely that Verizon will continue to use the exigent nature of public safety emergencies and catastrophic events to coerce public agencies into higher cost plans ultimately paying significantly more for mission critical service—even if that means risking harm to public safety.

*Id.* at \*4, \*6.

<sup>127</sup> Brodtkin, *supra* note 120.

<sup>128</sup> *Id.* The former FCC Chairman, Wheeler, agreed. *See generally id.*

<sup>129</sup> Barbara van Schewick, *Gov. Jerry Brown Signs SB 822, Restoring Net Neutrality to California*, CENTER FOR INTERNET & SOC’Y AT STANFORD LAW SCH. (Sept. 30, 2018), <http://cyberlaw.stanford.edu/blog/2018/09/gov-jerry-brown-signs-sb-822-restoring-net-neutrality-california>.

<sup>130</sup> Commissioner O’Rielly stated:

I, for one, see great value in the prioritization of telemedicine and autonomous car technology over cat videos. . . . Consider that each autonomous vehicle is predicted to generate an additional four terabytes of data a day, much of which will be carried by wireless networks. It’s hard to imagine that some prioritization of traffic won’t be necessary, further undermining attempts to ban such practices.

Issie Lapowsky & Clint Finley, *The Biggest Whoppers from the FCC’s Net Neutrality Meeting*, WIRED (Dec. 14, 2017), <https://www.wired.com/story/the-biggest-whoppers-from-the-fccs-net-neutrality->

potentially, national security.<sup>131</sup> Human bodies now rely on Internet availability for their safety, functionality, and integrity, and the Internet is part of our country's critical infrastructure.<sup>132</sup> Because of these materially changed circumstances of the last five years, the paradigm of "net neutrality" needs updating. Net neutrality is a policy framing based on a last-generation mental model of the Internet's role in society.

Two historical case studies offer useful lessons for updating the policy conversation over Internet availability. The first involves the evolution of the United States Postal Service from a limited periodical distribution network into a lynchpin component of our national security terrorism response.<sup>133</sup> The second example is the creation of ARPANET, which grew into today's Internet, through partnerships with universities<sup>134</sup>—a collaboration. This history that becomes particularly interesting when juxtaposed against the opportunities simultaneously missed by the private sector.<sup>135</sup> Together, these two examples highlight the critical role that government-sponsored innovation and leadership have played in responding to private sector gaps in network infrastructure development and deployment.

*A. Error 502<sup>136</sup>: Unreliable Gateway—Unavailability and the Internet of Bodies*

In addition to the public-safety concerns arising from unavailability of Internet access needed for emergency services, a second set of concerns threatens to damage physical safety: when human bodies rely on body-attached and body-embedded Internet of Things devices, unavailability will mean physical injury to human bodies.<sup>137</sup> This emerging "Internet of Bodies" ("IoB") requires reliable Internet

---

meeting/. But see Jessica Gall Myrick, *Study Shows the Paw-sitive Effects of Watching Cat Videos*, CONVERSATION (June 18, 2015), <http://theconversation.com/study-shows-the-paw-sitive-effects-of-watching-cat-videos-43454>; Nadia Kounang, *Your Love of Grumpy Cat and Cute Cat Videos is Instinctive and Good for You—Seriously*, CNN (May 17, 2019), <https://www.cnn.com/2016/01/20/health/your-brain-on-cute/index.html>.

<sup>131</sup> See *infra* Section III.A–C.

<sup>132</sup> See *infra* Section III.A.

<sup>133</sup> See *infra* Section III.C.1.

<sup>134</sup> See *infra* Section III.C.2.

<sup>135</sup> *Id.*

<sup>136</sup> *HTTP Status Code Registry*, *supra* note 18.

<sup>137</sup> The Internet of Bodies ("IoB") refers to the creeping progression of the human body being used as a technology platform. As I explain elsewhere, a growing number of both medical devices and workplace



access for continued safe functionality of these connected devices (and the bodies that rely on them). These Internet of Bodies devices include everything from life-saving devices medical devices such as artificial pancreases to recreational (body-attached or permanently implanted) devices such as augmented reality injected contact lenses.<sup>138</sup> Thus, unreliable, low-quality or unavailable Internet access will begin to directly or indirectly threaten the physical functionality of some human bodies. When considered in tandem with estimates that, at present 162.8 million people in the United States lack internet access at broadband speeds, the tension becomes obvious.<sup>139</sup>

For example, a recent case involving a CPAP machine is a harbinger of the sorts of problems unavailable Internet access can cause to human bodies.<sup>140</sup> Sufferers of sleep apnea rely on CPAP machines to enable their breathing during episodes of the condition as they sleep.<sup>141</sup> Like other medical devices, CPAP machines are expensive and usually subsidized by an apnea sufferer's insurance provider.<sup>142</sup> However, as with most insurance contexts, insurance providers seek increasingly granular ways to identify non-essential expenses by patients.<sup>143</sup> Presumably for this reason, insurance providers have progressively shifted toward Internet-enabled CPAP machines which inform the insurer in real time that the sleep apnea sufferer is using the machine.<sup>144</sup> A challenge in this reporting structure arises when Internet access is unavailable or unreliable. In such circumstances, the machine cannot successfully report back to the insurer that the insured is using the device.<sup>145</sup> In this

---

or recreational Internet of Things devices are moving inside the human body. *See generally* Matwyshyn, *supra* note 17, at 103–12. The consequence of this merger of bodies and bits creates new attack vectors and physical risks to the safety, integrity, and availability of human bodies. *Id.*

<sup>138</sup> *Id.*

<sup>139</sup> Kahan, *supra* note 4.

<sup>140</sup> Marshall Allen, *You Snooze, You Lose: How Insurers Dodge the Costs of Popular Sleep Apnea Devices*, NPR (Nov. 21, 2018), <https://www.npr.org/sections/health-shots/2018/11/21/669751038/you-snooze-you-lose-how-insurers-dodge-the-costs-of-popular-sleep-apnea-devices>.

<sup>141</sup> *Id.*

<sup>142</sup> *Id.*

<sup>143</sup> *See, e.g.*, David Lazarus, *Column: When Your Insurer Denies a Valid Claim Because of 'Lack of Medical Necessity'*, L.A. TIMES (Jan. 23, 2018), <https://www.latimes.com/business/lazarus/la-fi-lazarus-healthcare-claim-denials-20180123-story.html>.

<sup>144</sup> Allen, *supra* note 140.

<sup>145</sup> *Id.*

way, because of the Internet unavailability problem, the insurer may be left with the incorrect impression that the patient is not using the CPAP machine regularly. Indeed, insurers have sometimes sought to deny coverage for the machines based on this alleged lack of regular use because of the absence of a real-time report from the machine, despite insureds' attestations to the contrary.<sup>146</sup>

But imagine that, in lieu of a CPAP machine, the medical device with the Internet unavailability problem is an artificial pancreas or a bionic limb that requires regular software updates, particularly when a newly-discovered security vulnerability may threaten the continued functionality of the device. Now imagine that, much like the Santa Clara fire department, the human attached to this IoB device has purchased the "wrong" tier of service, or perhaps the latest software patch for the device exceeds the data caps instituted by the ISP, which then chooses to throttle the traffic. Meanwhile, an unpatched security vulnerability in an IoB device might be remotely exploitable by an attacker. Because the window to patch before attackers begin to exploit a newly-identified security vulnerability can be small,<sup>147</sup> without prompt patching, remote attackers may be able to assume control over an IoB device. Similarly, a denial of service for life-saving medical devices will soon include not only refusals to cover the cost of devices from insurers, but also distributed denial of service attacks from malicious third-party attackers who have harnessed vulnerable IoB devices into botnets. In this way, a human relying on a potentially life-saving Internet-reliant medical device may find her physical safety jeopardized in a manner even more direct than the residents of California experienced during the firefighter-Verizon throttling incident.<sup>148</sup>

---

<sup>146</sup> *Id.*

<sup>147</sup> For a discussion of vulnerability exploitability, see, for example, *Analysis of The RANDOM Report on Zero-days and Vulnerability Rediscovery*, RISK BASED SECURITY (July 24, 2017), <https://www.riskbasedsecurity.com/2017/07/24/analysis-of-the-random-report-on-zero-days-and-vulnerability-rediscovery/>.

<sup>148</sup> At least one author has proposed prioritized "fast lanes" for health care uses. Christina Susanto, *Net Neutrality and a Fast Lane for Health*, 37 J. LEGAL MED. 105, 105 (2017).

[T]he proposed solution recommends (1) only health care technologies that are approved or approvable by the Centers for Medicare & Medicaid Services process should go in the fast lane and (2) the government and private insurers should pay for health care prioritization. By including an exception to the net neutrality rules, the health care system can accommodate the changing technological landscape and remain viable for years to come.

But, in addition to these individual level safety concerns, the Internet also now plays a key role in our nation's critical infrastructure, defense, and national security.

*B. Status 308<sup>149</sup>: Permanent Redirect—The Internet as Critical Infrastructure*

During the last two decades, the Internet has evolved from a recreational communication method into a force that drives both our economy and aspects of national security. In 2001, President George W. Bush issued Executive Order 13,231, which declared communication networks, including the Internet, to be integral to national security.<sup>150</sup> In May of 2009, President Barack Obama enhanced this commitment and declared digital infrastructure a strategic national asset and protection of this infrastructure a “national priority.”<sup>151</sup> Subsequently, in 2013, Executive Order—Improving Critical Infrastructure Cybersecurity further explained the nature of the connection between national security and Internet defense.<sup>152</sup> This Order stated that the

cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges [to] . . . the national and economic security of the United States [which] depends on the reliable functioning of the Nation's critical infrastructure. . . . It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a

---

*Id.* However, as the line between medical and nonmedical devices and uses begins to blur in the IoB era, the viability of implementing this type of structure becomes progressively less possible as a practical matter. See Matwyshyn, *supra* note 17, at 107.

<sup>149</sup> *HTTP Status Code Registry*, *supra* note 18.

<sup>150</sup> Exec. Order No. 13,231, 3 C.F.R. § 814 (2002).

Sec. 11. *National Communications System*. Changes in technology are causing the convergence of much of telephony, data relay, and Internet communications networks into an interconnected network of networks. The NCS and its National Coordinating Center shall support use of telephony, converged information, voice networks, and next generation networks for emergency preparedness and national security communications functions assigned to them in Executive Order 12472.

*Id.*

<sup>151</sup> Remarks by the President on Securing Our Nation's Cyber Infrastructure, 2009 DAILY COMP. PRES. DOC. 3 (May 29, 2009).

<sup>152</sup> Exec. Order No. 13,636, 3 C.F.R. § 217 (2014).

cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.<sup>153</sup>

Indeed, not only does the Department of Defense rely on the Internet,<sup>154</sup> but the Internet also underpins the communication networks for our stock markets,<sup>155</sup> emergency services,<sup>156</sup> power grids,<sup>157</sup> hospitals,<sup>158</sup> and other safety-critical systems. For example, the FCC recently awarded a contract to AT&T for the buildout of FirstNet, a critical emergency responder network intended to connect the country's first responders through the Internet.<sup>159</sup>

Simultaneously, the role of the Internet has shifted internationally. In 2011, a United Nations Special Rapporteur report asserted that “the unique and transformative nature of the Internet is not only to enable individuals to exercise their right to freedom of opinion and expression but also a range of other human rights, and to promote the progress of society as a whole.”<sup>160</sup> Again in 2016, using the

---

<sup>153</sup> *Id.*

<sup>154</sup> *Our Mission*, U.S. ARMY CYBER COMMAND, <https://www.arcyber.army.mil/> (last visited Apr. 7, 2019).

<sup>155</sup> Mathew J. Belvedere, *Nasdaq ‘Shocking’ Outage Unacceptable, Says Pitt*, CNBC (Sept. 12, 2013), <https://www.cnbc.com/id/101028647>.

<sup>156</sup> Brian Fung, *A Nationwide CenturyLink Outage is Disrupting 911, and the FCC is Investigating*, WASH. POST (Dec. 28, 2018), [https://www.washingtonpost.com/technology/2018/12/28/nationwide-centurylink-outage-is-disrupting-fcc-is-investigating/?utm\\_term=.d4d4b3dcd7ee](https://www.washingtonpost.com/technology/2018/12/28/nationwide-centurylink-outage-is-disrupting-fcc-is-investigating/?utm_term=.d4d4b3dcd7ee).

<sup>157</sup> Nicole Perlroth & David E. Sanger, *Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says*, N.Y. TIMES (Mar. 15, 2018), <https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html>.

<sup>158</sup> *Internet Access Control for Hospitals*, HIPAA J., <https://www.hipaajournal.com/Internet-access-control-for-hospitals/> (last visited Apr. 7, 2019).

<sup>159</sup> John Egger, *AT&T Wins FirstNet Contract*, MULTICHANNEL NEWS, <https://www.multichannel.com/news/att-wins-firstnet-contract-411847> (last updated Mar. 29, 2018); *see also* *AT&T Selected by FirstNet to Build and Manage America’s First Nationwide Public Safety Broadband Network Dedicated to First Responders*, AT&T (Mar. 30, 2017), [https://about.att.com/story/firstnet\\_selects\\_att\\_to\\_build\\_network\\_supporting\\_first\\_responders.html](https://about.att.com/story/firstnet_selects_att_to_build_network_supporting_first_responders.html).

<sup>160</sup> Frank La Rue (Special Rapporteur on the Promotion of Freedom of Opinion and Expression), *Promotion and Protection of all Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development*, at 1, U.N. Doc. A/HRC/17/27 (May 16, 2011); *see also* Nicholas Jackson, *United Nations Declares Internet Access a Basic Human Right*, ATLANTIC (June 3, 2011), <https://www.theatlantic.com/technology/archive/2011/06/united-nations-declares-Internet-access-a-basic-human-right/239911/>.

language of the “digital divide,”<sup>161</sup> the UN Human Rights Council in a declaration entitled “The promotion, protection and enjoyment of human rights on the Internet” recognized “the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms,” and called “upon all states to promote and facilitate international cooperation aimed at the development of media and information and communication facilities and technologies in all countries.”<sup>162</sup> Studies of both United States adults<sup>163</sup> and people internationally<sup>164</sup> also indicate that affordable Internet access is now perceived to be a basic human right.<sup>165</sup> This growing sense that affordable Internet access is a human right blends into a shared expectation of human rights in economic and intellectual self-realization, a position in line with preexisting internationally recognized economic and social rights.<sup>166</sup> This changed perception has partially manifested in police departments around the world sometimes taking to Twitter to vent their frustrations when citizens call emergency services numbers to report Internet and website unavailability<sup>167</sup>—another sign of the central role that the Internet plays in peoples’ daily life.

---

<sup>161</sup> UN Human Rights Council Res., at 2, 32/13 U.N. Doc. A/HRC/32/L.20 (June 27, 2016) [hereinafter H.R.C. Res. 32/13]. The digital divide can be split into two subsidiary divides—the digital access divide and the digital production divide. *See generally* Andrea M. Matwyshyn, *Silicon Ceilings: Information Technology Equity, the Digital Divide and the Gender Gap Among Information Technology Professionals*, 2 NW. J. TECH. & INTELL. PROP. 35, 42–53 (2003). The First involves issues of “equal access for all potential consumers of information technology”; and the second involves issues of “equal access for all potential producers of information technology, enabling them to participate in the research, development, and production of information technology.” *Id.* at 42 (emphases omitted).

<sup>162</sup> H.R.C. Res. 32/13, *supra* note 161, at 3.

<sup>163</sup> CIGI & IPSOS, *supra* note 163 (polling people in twenty-four countries on their views about online privacy, Internet governance and concerns about Internet security).

<sup>164</sup> Valerie Hamilton, *Survey: Internet Access a “Basic Human Right,”* GOV’T TECH. (Nov. 25, 2014), <http://www.govtech.com/network/Survey-Internet-Access-a-Basic-Human-Right.html> (“The CIGI-Ipsos Global Survey on Internet Security and Trust polled people in 24 countries on their views about online privacy, Internet governance and concerns about Internet security. Eighty-three percent of people surveyed believed affordable access to the Internet should be a basic human right, with the highest numbers coming from countries with a history of authoritarian rule.”).

<sup>165</sup> CIGI & IPSOS, *supra* note 163.

<sup>166</sup> *See generally* International Covenant on Economic, Social and Cultural Rights, Dec. 16, 1966, 993 U.N.T.S. 14531.

<sup>167</sup> Johnny Lieu, *Youtube Is Down, Please Don’t Call the Police*, MASHABLE (Oct. 16, 2018), <https://mashable.com/article/youtube-down-Internet-freaks/#3ZBYuHyQiqT>; Canterbury Police NZ, (@NZPCanterbury), TWITTER (Mar. 13, 2019, 10:54 AM), <https://twitter.com/NZPCanterbury/status/1105889975713718273> (“We know. Our @facebook and @instagram haven’t been working either.”).

Along with the legal recognition of the changing role of the Internet, the number of United States end users has materially escalated in the last two decades. In 2000, only 52% of United States adults used the Internet,<sup>168</sup> but in 2018, a quarter of United States adults said they are “almost constantly” online,<sup>169</sup> and nine out of ten United States adults used the Internet<sup>170</sup>—numbers that are still expected to grow.<sup>171</sup> This figure now exceeds the rate of United States car ownership.<sup>172</sup> Additionally, two thirds of United States adults use digital banking services.<sup>173</sup> This shift in banking is part of a broader trend, which reflects that the availability of reliable Internet access appears to have moved from an optional tool to an expected component for consumers to be able to fully participate in the United States economy. As Professor Susan Crawford explains,

[e]veryone now understands that [I]nternet access is indispensable infrastructure for the 21st century economy. For every American business to compete and every citizen to be part of the modern world, America needs cheap, reliable, and world-

---

Unfortunately, we cannot do anything about this because, you know, they’re based in America and we’re the Police. So please don’t call us to report this. Pretty please.”); Philadelphia Police (@PhiladelphiaPolice), TWITTER (Oct. 16, 2018, 6:30 PM), <https://twitter.com/PhillyPolice/status/1052371210384891904> (“Yes, our @YouTube is down, too. No, please don’t call 911—we can’t fix it.”); see also Ben Brody, *LA Residents Call 911 When Facebook Goes Down*, CNN (Aug. 4, 2014), <https://money.cnn.com/2014/08/04/news/companies/facebook-outage-911/>; Elle Hunt, *Did You Make it Through the Facebook Outage Without Calling the Police?*, GUARDIAN (Mar. 14, 2019, 10:34 AM), <https://www.theguardian.com/technology/shortcuts/2019/mar/14/did-you-make-it-through-the-facebook-outage-without-calling-the-police>; DAVE KITTLES (@Dave\_Kittle), TWITTER (Feb. 2, 2015, 3:27 AM), [https://twitter.com/Dave\\_Kittle/status/562210648579657728](https://twitter.com/Dave_Kittle/status/562210648579657728).

<sup>168</sup> ANDREW PERRIN & MAEVE DUGGAN, PEW RESEARCH CTR., AMERICANS’ INTERNET ACCESS: 2000–2015, at 2 (June 26, 2015), [https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2015/06/2015-06-26\\_internet-usage-across-demographics-discover\\_FINAL.pdf](https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2015/06/2015-06-26_internet-usage-across-demographics-discover_FINAL.pdf).

<sup>169</sup> Andrew Perrin & Madhu Kumar, *About Three-in-Ten U.S. Adults Say They are ‘Almost Constantly’ Online*, PEW RES. CTR. (Mar. 14, 2018), <http://www.pewresearch.org/fact-tank/2018/03/14/about-a-quarter-of-americans-report-going-online-almost-constantly/>.

<sup>170</sup> PEW RESEARCH CTR., INTERNET/BROADBAND FACT SHEET (June 12, 2019), <http://www.pewInternet.org/fact-sheet/Internet-broadband/>.

<sup>171</sup> Yet, the number of adults with home broadband declined in 2018. *Id.*

<sup>172</sup> Jacob Poushter, *Car, Bike or Motorcycle? Depends on Where You Live*, PEW RES. CTR. (Apr. 16, 2015), <http://www.pewresearch.org/fact-tank/2015/04/16/car-bike-or-motorcycle-depends-on-where-you-live/>.

<sup>173</sup> American Bankers Association, *ABA Survey: Two-Thirds of Americans Use Digital Banking Channels Most Often*, ABA BANKING J. (Sept. 21, 2017), <https://bankingjournal.aba.com/2017/09/aba-survey-two-thirds-of-americans-use-digital-banking-channels-most-often/>.

class connections to the [I]nternet everywhere—just as we need cheap, reliable, and world-class electricity and water.<sup>174</sup>

Yet, as the demand and use of the critical infrastructure of the Internet has exploded, the service capabilities of ISPs have not kept pace. Dropped mobile connections,<sup>175</sup> mysteriously unavailable Internet access,<sup>176</sup> and undiagnosable stalled (or throttled?) data access are a recurring part of United States consumers' lives.<sup>177</sup> Internet Service Providers regularly earn spots in lists of most hated companies in America, often at rates higher than other industries,<sup>178</sup> sometimes claiming the dubious distinction of top spot.<sup>179</sup> Meanwhile, despite substantial profits,<sup>180</sup> major ISPs have recently chosen to decrease capital expenditures.<sup>181</sup>

---

<sup>174</sup> Crawford, *supra* note 84. Professor Susan Crawford frames issues of Internet availability in the language of “Internet freedom writ large” and “global competitiveness.” *Id.*

<sup>175</sup> See, e.g., Magenta3024992, Comment to *Dropped Calls*, T-MOBILE (Oct. 27, 2017, 2:42 PM), <https://support.t-mobile.com/thread/142269>.

<sup>176</sup> See, e.g., *DNS Server Unavailable? Here's What to Do*, 1&1 IONOS (Jan. 29, 2018), <https://www.ionos.com/digitalguide/server/know-how/dns-server-not-responding-whats-next/>.

<sup>177</sup> See, e.g., Todd Haselton, *Try This Trick If Your Phone Keeps Losing Its Data Connection*, CNBC (July 11, 2018), <https://www.cnbc.com/2018/07/11/how-to-fix-phone-no-data-conneciton-turn-off-wifi.html>.

<sup>178</sup> Samuel Stebbins et al., *Bad Reputation: America's Top 20 Most-Hated Companies*, USA TODAY (Feb. 12, 2018), <https://www.usatoday.com/story/money/business/2018/02/01/bad-reputation-americas-top-20-most-hated-companies/1058718001> (identifying Century Link, Comcast, and Sprint in the top 20 most hated companies in America).

<sup>179</sup> *Congratulations to Comcast, Your 2014 Worst Company in America!*, CONSUMERIST (Apr. 8, 2014), <https://consumerist.com/2014/04/08/congratulations-to-comcast-your-2014-worst-company-in-america>.

<sup>180</sup> Jonathan Ponciano, *The World's Largest Telecom Companies 2018: AT&T, Verizon Remain on Top As Sector Struggles*, FORBES (June 6, 2018), <https://www.forbes.com/sites/jonathanponciano/2018/06/06/worlds-largest-telecom-companies-2018/#79310f0b7d39> (noting that there are fifty-four telecommunications companies on the Forbes Global 2000 list, and they claimed more than \$3.4 trillion in assets and \$1.5 trillion in revenue in 2017).

<sup>181</sup> Jon Brodtkin, *Sorry, Ajit: Comcast Lowered Cable Investment Despite Net Neutrality Repeal*, ARS TECHNICA (Jan. 23, 2019), <https://arstechnica.com/information-technology/2019/01/sorry-ajit-comcast-lowered-cable-investment-despite-net-neutrality-repeal>; Jon Brodtkin, *Sorry FCC: Charter Will Lower Investment After Net Neutrality Repeal*, ARS TECHNICA (Feb. 8, 2018), <https://arstechnica.com/tech-policy/2018/02/sorry-fcc-charter-will-lower-investment-after-net-neutrality-repeal>.

In particular, multiple ISPs appear to have breached agreements with municipal governments regarding infrastructure buildout.<sup>182</sup> For example, some areas of Pennsylvania reportedly have been waiting over twenty years for one ISP to fulfill “its obligation to modernize its network to provide universal broadband availability to its customers”<sup>183</sup>—a set of promises it had made to the State of Pennsylvania in exchange for being granted the ability to charge higher prices for phone services in 1993.<sup>184</sup> The same ISP “agreed to upgrade its network to provide broadband to every New Jersey business and residential customer, school, and library for 100 percent of its service territory” and did not fulfill this obligation according to the state’s Division of Rate Counsel.<sup>185</sup> In New York City, this same ISP was ordered by city officials, in 2005, to complete fiber builds that were over a year late and fell short of covering 22% of households, according to a city audit.<sup>186</sup> Over a decade later, some New York City businesses still appeared to be limited in their ability to obtain high speed access.<sup>187</sup> Also in New York, the same ISP sought permission not to repair hurricane-damaged infrastructure, leaving consumers with only one, less hurricane-resilient option in the opinion of the New York Attorney General, who pressured the company into relenting.<sup>188</sup> Similarly, in California, this same ISP was accused by

---

<sup>182</sup> See, e.g., Jon Brodtkin, *22 Years After Verizon Fiber Promise, Millions Have Only DSL or Wireless*, ARS TECHNICA (June 9, 2015), <https://arstechnica.com/information-technology/2015/06/22-years-after-verizon-fiber-promise-millions-have-only-dsl-or-wireless>.

<sup>183</sup> *Id.*

<sup>184</sup> Verizon Pennsylvania, Inc., P-00930715 (Pa. Pub. Util. Comm’n, May 15, 2002); see also Brodtkin, *supra* note 182.

<sup>185</sup> Jon Brodtkin, *Verizon Led Massive Astroturf Campaign to End NJ Broadband Obligation*, ARS TECHNICA (Apr. 16, 2014), <https://arstechnica.com/tech-policy/2014/04/verizon-led-massive-astroturf-campaign-to-end-nj-broadband-obligation>. The ISP in question was also accused lobbying policymakers to end its obligations to the state of New Jersey. *Id.*

<sup>186</sup> *De Blasio Administration Releases Audit Report of Verizon’s Citywide FiOS Implementation*, CITY OF NEW YORK (June 18, 2015), <https://www1.nyc.gov/office-of-the-mayor/news/415-15/de-blasio-administration-releases-audit-report-verizon-s-citywide-fios-implementation> (“The lack of competition in the City’s broadband market is one of many issues at the root of this problem.”).

<sup>187</sup> See, e.g., Susan Crawford, *Bad Internet in the Big City*, WIRED (Feb. 28, 2018), <https://www.wired.com/story/new-york-city-verizon-Internet>.

<sup>188</sup> Elise Ackerman, *New York Attorney General Slams Verizon for Degrading Service to Customers, Requests Fines of \$100,000 Per Day*, FORBES (July 3, 2013), <https://www.forbes.com/sites/eliseackerman/2013/07/03/new-york-attorney-general-slams-verizon-for-degrading-service-to-customers-requests-fines-of-100000-per-day/#1f206d0859e9>.



residents of failing to fix existing infrastructure in order to force them onto a different product, which some residents viewed as materially inferior.<sup>189</sup>

The reasons for these ISPs' failure to fulfill their contractual commitments appear unrelated to cost. Professor Andrew Odlyzko explains that "[c]ontrary to many claims of opponents of net neutrality, networks are not very expensive to build."<sup>190</sup> Thus, it appears that the current marketplace demonstrates neither robust competition nor manifestly pleased customers, and the reasons for these failures are not self-evident. As succinctly explained by Senator John Kennedy commenting on a congressional attempt to revive the FCC 2015 Open Internet Rule, "[t]his . . . comes down to one thing and one thing only—the extent to which you trust your cable company."<sup>191</sup> This begs the question of whether it has been a strategic business and legal choice by ISPs to seek to maximize the short-term benefits of incumbency and incentives negotiated with governmental entities, even at the expense of companies' own long-term future revenue streams and the good of our society.

Industry defenders would reply that the private sector invented the modern Internet and is in the best position to govern its deployment—whatever that might mean. They would say that our approach should give maximum flexibility to telecommunications companies for the best results in infrastructure buildout.<sup>192</sup> Yet, the history of United States information networks' evolution tells a different story.

### C. *Error 508*<sup>193</sup>: *Loop Detected—Lessons from History*

The creation of the Internet is frequently viewed as the ultimate manifestation of a private sector success story.<sup>194</sup> Indeed, our culture reifies Silicon Valley origin stories of two entrepreneurs huddled in a garage or working in cramped quarters in

---

<sup>189</sup> Jon Brodtkin, *Verizon Accused of Refusing to Fix Broken Landline Phone Service*, ARS TECHNICA (Mar. 23, 2014), <https://arstechnica.com/information-technology/2014/03/verizon-accused-of-refusing-to-fix-broken-landline-phone-service> ("A man who identified himself as a San Jose resident said, 'Voice Link is a very shoddy, grossly inferior phone service that Verizon is trying to force onto its phone customers. . . . Voice Link is about as useful as talking with a can and string.'").

<sup>190</sup> Odlyzko, *supra* note 56, at 43.

<sup>191</sup> Crawford, *supra* note 84.

<sup>192</sup> Yoo, *supra* note 68, at 232.

<sup>193</sup> *HTTP Status Code Registry*, *supra* note 18.

<sup>194</sup> See Gordon Crovitz, *Who Invented the Internet?*, WALL ST. J. (July 22, 2012), <https://www.wsj.com/articles/SB10000872396390444464304577539063008406518> (rejecting the view that the government, not the private sector, is responsible for the Internet's creation and subsequent success).

a Silicon Valley incubator.<sup>195</sup> Meanwhile, ISP executives sometimes speak of investments in “their pipes”<sup>196</sup> and that others should not get a “free ride” on them.<sup>197</sup> In reality, however, the history of the information transmission networks and their “incubation” in the United States reveals an origin story driven by government investment, academia, national security, and concrete national policy objectives. Two such case studies of information transmission networks include the United States Postal Service (“USPS”) and its entry into parcel shipping and the creation of ARPANET, the predecessor network to the Internet.

### 1. The Problem of Unavailability and USPS

Advocates of granting ISPs unregulated control over Internet access pricing structures frequently fall back on an argument stating something along the lines of “just as you can ship things slowly through the Post Office or more quickly through FedEx, the Internet can have fast and slow lanes, and telecoms should be able to institute pricing regimes that facilitate that.”<sup>198</sup> Meanwhile, in the public sector, calls for scaling back or eliminating the USPS in favor of greater reliance on private sector options occur with regularity.<sup>199</sup> Both sets of critics appear unfamiliar with the full origin story of USPS, its current operations, and the critical role USPS plays in national security.

Instead, the evolution of USPS’s services and role in our society demonstrates that private sector markets sometimes require governmental supplementation to advance the next iteration of economic development. While most of us are familiar with USPS’s current parcel delivery capabilities, the key historical role that USPS played in launching new communication methods and modes of commerce is

---

<sup>195</sup> Rich Karlgaard, *Two Guys in a Garage*, FORBES (Dec. 19, 2005), <https://www.forbes.com/sites/digitalrules/2005/12/19/two-guys-in-a-garage/#657a97b21eff>.

<sup>196</sup> Phil Shook, *What to Know About Net Neutrality*, RICE BUS. WISDOM (Dec. 20, 2017), <https://business.rice.edu/wisdom/features/what-know-about-net-neutrality>. An AT&T CEO famously stated: “Why should they be allowed to use my pipes?” *Id.*

<sup>197</sup> Jon Healey, *Will Wheeler’s Net Neutrality Rules Lead to Online Toll Lanes?*, L.A. TIMES (Apr. 25, 2014), <https://www.latimes.com/opinion/opinion-la/la-ol-net-neutrality-broadband-prices-20140425-story.html> (“The Internet can’t be free in that sense because we and the cable companies have made an investment, and for a Google or Yahoo or Vonage or anybody to expect to use these pipes [for] free is nuts!”).

<sup>198</sup> See, e.g., Christopher S. Yoo, *Network Neutrality and the Economics of Congestion*, 94 GEO. L.J. 1847 (2006).

<sup>199</sup> Eli Lehrer, *The Postal Service Should Go... Now*, HUFFPOST (Nov. 25, 2012), [https://www.huffpost.com/entry/us-postal-service\\_b\\_2184645](https://www.huffpost.com/entry/us-postal-service_b_2184645).

perhaps less familiar.<sup>200</sup> The first post office was opened in 1775 in Philadelphia, and, at least initially, only delivered newsletters and personal correspondence.<sup>201</sup> Parcel delivery, in particular, was left to the private sector, and, for over a century, parcel delivery remained a solely private sector service.<sup>202</sup>

However, the private sector failed to successfully meet the needs of the population.<sup>203</sup> Because of public outcry over consistently expensive and unreliable private sector service particularly in rural areas, in 1916, USPS expanded its service to include parcel delivery.<sup>204</sup> This service expansion coincided with the rising popularity of the mail order catalog industry<sup>205</sup>—an industry which USPS assisted in reaching profitability through Rural Free Delivery of mail, including catalogs, in 1896.<sup>206</sup> Through the creation of reliable parcel delivery, the USPS corrected socially inefficient choices of the private sector,<sup>207</sup> enabled westward expansion of the

---

<sup>200</sup> The creation of the United States Postal Service (“USPS”) arises from congressional authority granted by Article I, Section 8 of the Constitution, which states “[t]he Congress shall have Power . . . to establish Post Offices and Post Roads.” U.S. CONST. art. I, § 8.

<sup>201</sup> Kevin Kosar, *Do We Need a Postal Service?*, NEWSWEEK (Apr. 2, 2015), <https://www.newsweek.com/do-we-need-postal-service-319243>; see also Rachel Pick, *Why is the Post Office Still a Thing?*, MOTHERBOARD (Feb. 19, 2016), [https://motherboard.vice.com/en\\_us/article/pgkpn/why-is-the-post-office-still-a-thing-outdated-technology-mail-letters-usps](https://motherboard.vice.com/en_us/article/pgkpn/why-is-the-post-office-still-a-thing-outdated-technology-mail-letters-usps); Philip F. Rubio, *Why We Need the Postal Service*, CNN (Sept. 12, 2011), <https://www.cnn.com/2011/09/09/opinion/rubio-postal-service-matters/index.html>.

<sup>202</sup> Rubio, *supra* note 201.

<sup>203</sup> *Id.*

<sup>204</sup> *Id.*

<sup>205</sup> As explained by the Sears Archives:

The time was right for mail order merchandise. Fueled by the Homestead Act of 1862, America’s westward expansion followed the growth of the railroads. The postal system aided the mail order business by permitting the classification of mail order publications as aids in the dissemination of knowledge entitling these catalogs the postage rate of one cent per pound.

*History of the Sears Catalog*, SEARS ARCHIVES, <http://www.searsarchives.com/catalogs/history.htm> (last visited Apr. 8, 2019).

<sup>206</sup> *Id.* (“The advent of Rural Free Delivery in 1896 also made distribution of the catalog economical.”).

<sup>207</sup> In addition to delivery companies’ lack of interest in shipping to some rural destinations, certain populations, particularly minorities, benefited from mail order catalogs since they had difficulty getting access to goods because local shopkeepers lacked inventory or refused to sell to them. Gaby Del Valle, *How the Sears Catalog Transformed Shopping Under Jim Crow, Explained by a Historian*, VOX (Oct. 19, 2018), <https://www.vox.com/the-goods/2018/10/19/18001734/sears-catalog-bankruptcy-jim-crow->

country, and materially enabled the flourishing of remote product purchasing through mail order catalogs.

Perhaps most significantly, this major commerce design shift from in person purchasing to mail order catalog purchasing then ultimately served as partial inspiration for the advent of Internet commerce a century later.<sup>208</sup> Catalog orders for everything from Model H motor cars to chicken incubators were shipped nationally by Sears through USPS in the early 1900s,<sup>209</sup> and Sears credits the role that USPS played in its success.<sup>210</sup> Later, USPS was also the first to offer expedited overnight mail, and it pioneered the creation of zip codes to facilitate faster delivery of parcels—an evolution that again spurred the growth of the private sector.<sup>211</sup> In other words, USPS led in network innovation in ways that the private sector did not. Its innovation filled critical gaps left by the private sector and proved obvious to the progress of the United States both in its economy and in its residents' quality of life.

Today, perhaps surprisingly, USPS and its parcel delivery capability also play a critical national security role in defending the United States against bioterrorism. In 2009, President Barack Obama signed Executive Order 13527, which aimed to “sustain critical infrastructure” through creating a distribution system using USPS: USPS serves as a key component of national security countermeasures in case of a biological attack.<sup>212</sup> In this way, USPS offers a vitally important backup distribution

---

racism-mail-order (interviewing Louis Hyman, a work historian at Cornell University and the director of the Institute for Workplace Studies).

<sup>208</sup> See Rebecca C. Ruiz, *Catalogs, After Years of Decline, Are Revamped for Changing Times*, N.Y. TIMES (Jan. 25, 2015), <https://www.nytimes.com/2015/01/26/business/media/catalogs-after-years-of-decline-are-revamped-for-changing-times.html> (touting the Sears catalog as a precursor to the online purchasing model).

<sup>209</sup> *Chronology of the Sears Catalog*, SEARS ARCHIVES, <http://www.searsarchives.com/catalogs/chronology.htm> (last visited Apr. 8, 2019).

<sup>210</sup> *History of Sears Catalog*, *supra* note 205.

<sup>211</sup> Rubio, *supra* note 201.

<sup>212</sup> The Executive Order states:

Section 1. Policy. It is the policy of the United States to plan and prepare for the timely provision of medical countermeasures to the American people in the event of a biological attack in the United States through a rapid Federal response in coordination with State, local, territorial, and tribal governments. This policy would seek to: (1) mitigate illness and prevent death; (2) sustain critical infrastructure; and (3) complement and supplement State, local, territorial, and tribal government medical countermeasure distribution capacity.

network as a redundancy<sup>213</sup> measure to supplement the countermeasure distribution capacity of other governmental organizations as part of bioterror response.

However, the Internet's own history also tells an origin story driven by national security policy, university-led innovation, and government funding. Again, history disputes the well-worn narrative of the "two entrepreneurs in a garage" model of innovation as the driving force behind the Internet.

## 2. The Problem of Redundancy and ARPANET

The earliest history of the Internet, i.e., the creation of ARPANET and its commercialization, is a national security story that again highlights the key role of government investment in stimulating innovation—not private sector leadership. During the 1970s, the Department of Defense sought to create a redundant,<sup>214</sup> faster communications network to engage with its defense contractors and other national security-relevant parties.<sup>215</sup> ARPA, the research agency of the Department of Defense at the time, provided funding that enabled universities to collaborate with ARPA to jointly undertake this foundational research.<sup>216</sup> This research ultimately resulted in the Internet's backbone.<sup>217</sup>

In other words, through a collaboration with ARPA in the 1970s, university academics and other researchers built ARPANET—a distributed, decentralized

---

Exec. Order No. 13,527, 3 C.F.R. § 327 (2010).

<sup>213</sup> While redundancy may be understood to mean "an unnecessary duplication" in common parlance, in information security discussions, redundancy is a critical tool in risk mitigation and incident response planning. See Fahmida Y. Rashid, *A Lesson from Network Outage: Redundancy Matters*, INFOWORLD (Jan. 2, 2017), <https://www.infoworld.com/article/3153357/a-lesson-from-network-outages-redundancy-matters.html>.

<sup>214</sup> YASHA LEVINE, *SURVEILLANCE VALLEY* 57 (2018).

<sup>215</sup> *Id.*

<sup>216</sup> "When I had this idea about building a network—this was in 1966—it was kind of an 'Aha' idea, a 'Eureka!' idea. I went over to Charlie Herzfeld's office and told him about it. And he pretty much instantly made a budget change within his agency and took a million dollars away from one of his other offices and gave it to me to get started. It took about 20 minutes." Keenan Mayo & Peter Newcomb, *How the Web Was Won*, VANITY FAIR (Jan. 7, 2009), <https://www.vanityfair.com/news/2008/07/internet200807>.

<sup>217</sup> Michael Hauben, *Behind the Net: The Untold History of the ARPANET and Computer Science*, <http://www.columbia.edu/~rh120/ch106.x07> (last updated Oct. 15, 1995).

digital network, i.e., the early Internet.<sup>218</sup> As a “packet-switched” network, it relied on a fundamentally different model of communication from the “circuit-switched” model used by telephone networks at the time.<sup>219</sup> Thus, it was internationally designed in explicit *contrast* to what existed in the private sector at the time because of national security communication needs. Because the new network could dynamically alter the flow of packets, it created both internally redundant methods of transmission and a redundant architecture to AT&T’s centralized network.<sup>220</sup> A positive externality of this new structure was its resiliency to attack. Because of its distributed structure, it was likely to better withstand adversary attacks on United States communications infrastructure—an important national security advantage. Ultimately, ARPANET gave birth to the Internet as we know it today.

The part of the story that often remains unanalyzed, however, was a private sector dynamic happening in tandem—what might be termed the problem of “stagnovation.”<sup>221</sup> The OECD defines “stagnovation” as the condition where a technological problem is temporarily postponed, delaying the systematic search for a new technology vision.<sup>222</sup> In other words, the life span of existing dominant technologies is artificially prolonged without adequate planning for the development of next generation technologies.<sup>223</sup>

In reviewing the strategic business choices made by AT&T in the first decades of the Internet’s existence and their relationship to the Computer I, II, and III FCC

---

<sup>218</sup> The initial nineteen nodes on ARPANET included UCLA, SRI, UCSB, University of Utah, BBN, MIT, RAND, SDC, Harvard, Lincoln Lab, Stanford, University of Illinois (Urbana), Case Western Reserve, CMU, NASA-Ames. *Id.*

<sup>219</sup> See Lee Copeland, *Packet-Switched vs. Circuit-Switched Networks*, COMPUTERWORLD (Mar. 20, 2000), <https://www.computerworld.com/article/2593382/networking-packet-switched-vs-circuit-switched-networks.html> (explaining generally the differences between packet-switched and circuit-switched networks).

<sup>220</sup> *Id.*

<sup>221</sup> As explained by the Organisation of Economic Co-Operation and Development (“OECD”), “the greatest danger of stagnovation is that it masks the relation between postponing a problem and exacerbating it.” Meinolf Dierkes et al., OECD, *Technological Development and Organisational Change: Differing Patterns of Innovation*, 1ST CENTURY TECHNOLOGY PROMISES AND PERILS OF A DYNAMIC FUTURE 97, 106–07 (1998).

<sup>222</sup> *Id.*

<sup>223</sup> *Id.*

inquiries,<sup>224</sup> a story of stagnation arguably becomes visible.<sup>225</sup> In the early days of the commercialization of APRANET, AT&T appears to have chosen to focus on short-term returns, seeking to maximize and exploit its incumbency in existing telephony. Consequently, the company appears to have misjudged the future impact of the next generation of technology—the looming commercial explosion of computing and the Internet.<sup>226</sup> Indeed, according to some histories of ARPANET, AT&T's shortsightedness was quite epic: DoD apparently offered to sell ARPANET to AT&T, remaining as an anchor tenant.<sup>227</sup> Allegedly, AT&T refused the deal, saying that the network was incompatible with its existing infrastructure and,

---

<sup>224</sup> FED. COMM'N COMM'N, OET BULL. 93-62, UNDERSTANDING THE FCC REGULATIONS FOR COMPUTERS AND OTHER DIGITAL DEVICES (1996); Ameritech Petition for Waiver of Computer III Rules for Reverse Search Capability, 13 FCC Rcd. 8762 (1997); see generally Note, *The FCC Computer Inquiry: Interfaces of Competitive and Regulated Markets*, 71 MICH. L. REV. 172 (1972).

<sup>225</sup> As explained by ARPA pioneer Bob Kahn:

AT&T probably said, Look, maybe we would have 50 or a hundred organizations, maybe a few hundred organizations, that could possibly partake of this in any reasonable time frame. Remember, the personal computer hadn't been invented yet. So, you had to have these big expensive mainframes in order to do anything.

Mayo & Newcomb, *supra* note 216.

<sup>226</sup> As explained by ARPA pioneer Paul Baran:

The one hurdle packet switching faced was AT&T. They fought it tooth and nail at the beginning. They tried all sorts of things to stop it. They pretty much had a monopoly in all communications. And somebody from outside saying that there's a better way to do it of course doesn't make sense. They automatically assumed that we didn't know what we were doing.

*Id.*

<sup>227</sup> As explained by ARPA pioneer Larry Roberts:

They wouldn't buy it when we were done. I went to AT&T and I made an official offer to them to buy the network from us and take it over. We'd give it to them basically. Let them take it over and they could continue to expand it commercially and sell the service back to the government. So they would have a huge contract to buy service back. And they had a huge meeting and they went through Bell Labs and they made a serious decision and they said it was incompatible with their network. They couldn't possibly consider it. It was not something they could use. Or sell.

Janus Rose, *AT&T Could Have Bought the Internet in 1971*, VICE (Jan. 17, 2012), [https://www.vice.com/en\\_us/article/vvv3qy/remember-that-time-at-t-almost-bought-the-internet](https://www.vice.com/en_us/article/vvv3qy/remember-that-time-at-t-almost-bought-the-internet).

therefore, not immediately commercializable.<sup>228</sup> As explained by one ARPANET pioneer, “[AT&T] said, There’s no business there, and why should we waste our time until we can see that there’s a business opportunity? That’s why a place like ARPA is so important.”<sup>229</sup>

AT&T’s missed long-term opportunities were arguably not limited to external offers. During the early Internet era, AT&T also appears to have missed some opportunities for commercialization of internally-developed computing products coming out of its formidable research laboratory, Bell Labs.<sup>230</sup> For example, the creation of the UNIX operating system<sup>231</sup> appears to have been largely financially unexploited by AT&T.<sup>232</sup> But, what then explains AT&T’s willingness to absorb the expense of operating Bell Labs—a research lab producing Nobel Prize-level basic

---

<sup>228</sup> *Id.* As explained by ARPA pioneer Bob Taylor:

Working with AT&T would be like working with Cro-Magnon man. I asked them if they wanted to be early members so they could learn technology as we went along. They said no. I said, Well, why not? And they said, Because packet switching won’t work. They were adamant. As a result, AT&T missed out on the whole early networking experience.

Mayo & Newcomb, *supra* note 216.

<sup>229</sup> *Id.* Indeed, the story of the Minitel arriving in the United States offers perhaps a parallel historical example. Julien Mailland, *Minitel, the Open Network Before the Internet*, ATLANTIC (June 16, 2017), <https://www.theatlantic.com/technology/archive/2017/06/minitel/530646/>. Unlike in France, the state operated Minitel and remained agnostic about uses, in the United States a company in the private sector attempted to popularize the device. *Id.* Although the technology was identical to the French version, “when the private sector was fully in charge of administering the platform, it chose to limit rather than facilitate the marketplace.” *Id.* The technology failed to become popularized. *Id.*

<sup>230</sup> The arrival of the Internet could have potentially reinvigorated prior AT&T product lines such as the “picture phone,” which was previously prohibitively expensive for average consumers but arguably an impressive example of forward-looking technology that was ahead of its time in terms of United States innovation. PORTICUS CENTER, *Western Electric Products—Picturephone*, <https://beatriceco.com/bti/porticus/bell/telephones-picturephone.html> (last visited Apr. 8, 2019).

<sup>231</sup> Interestingly, and perhaps unexpectedly, at least one author asserts that even the creation of UNIX was not due to a proactive attempt by AT&T to develop and launch new products, rather, it was due to regulatory pressure. Steve Chen, *The Dissemination of Unix, with a Focus on What Went on Within Bell Labs*, <http://www.princeton.edu/~hos/frs122/unixhist/chen.htm> (“[T]he New York Public Service Commission and other such regulatory bodies began putting pressure on AT&T to solve what was termed as a ‘service crises.’ This pressure led AT&T in search of technological advances that would make its support operations more efficient. This search eventually led to Unix.”).

<sup>232</sup> *Id.* (“Because AT&T was not in the business of selling operating systems, Unix soon became readily available to academic institutions at a very small charge.”).



scientific research<sup>233</sup>—if its parent company engaged in only limited commercialization of the research emerging from it? From the perspective of some researchers who worked at Bell Labs at the time and other observers, Bell Labs' existence sometimes appeared to function primarily as a cost center—a way to demonstrate business expenses to the FCC and other regulators in the name of being able to charge existing telephone consumers higher rates.<sup>234</sup> Again, the primary goal appears to have been short-term revenue maximization without an eye on the future of innovation. Similarly, the company sold off corporate assets that, in hindsight, may have proven useful to its own future business lines.<sup>235</sup> In short, history appears to caution us to be wary of private sector stagnation: Private sector companies will not always lead in innovation. Instead, sometimes they will lag behind and choose short-term wins, even at the expense of their own long-term future revenue streams.<sup>236</sup>

Stagnation is also arguably visible in ISPs' conduct today, and it potentially explains a portion of ISPs' contract breaches and delays in infrastructure buildout.<sup>237</sup> A stagnation-driven strategy could be similarly consistent with ISPs' filing lawsuits against local communities who seek to launch competitive network infrastructure. Indeed, in 2008, an ISP sued the city of Chattanooga, Tennessee to prevent it from building out its own municipal fiber network to offer faster Internet access to citizens and expand coverage for rural areas.<sup>238</sup> Meanwhile, when looking

---

<sup>233</sup> NOKIA BELL LABS, *Global Recognition for Groundbreaking Discovery*, <https://www.bell-labs.com/about/recognition/> (last visited Nov. 12, 2019) (listing awards won by Bell Labs researchers).

<sup>234</sup> Robert Buderl, *Bell Labs is Dead, Long Live Bell Labs*, MIT TECH. REV. (Sept. 1, 1998), <https://www.technologyreview.com/s/400241/bell-labs-is-dead-long-live-bell-labs/> (“Bell Labs was a regulated monopoly allowed to fold a ‘research tax’ into every phone call and sale. But the Bell System’s 1984 court-ordered breakup into seven regional operating companies, AT&T’s dramatic decentralization five years later into a series of business units, and then trivestiture, which saw roughly one-fourth of its researchers assigned to the new AT&T, forced a dramatic change in that outlook.”).

<sup>235</sup> Daryl R. Gibson, *AT&T Long Lines Microwave Towers*, <http://www.drgibson.com/towers> (last updated 2003); Jordan Teicher, *The Abandoned Microwave Towers That Once Linked the US*, WIRED (Mar. 10, 2015), <https://www.wired.com/2015/03/spencer-harding-the-long-lines>.

<sup>236</sup> Social psychologists view this as a form of bias against creativity. See generally JENNIFER S. MUELLER, CREATIVE CHANGE: CREATIVE CHANGE: WHY WE RESIST IT. . . HOW WE CAN EMBRACE IT (2017).

<sup>237</sup> Having successfully extracted short-term concessions from municipalities to buttress quarterly returns, ISPs may be employing legal entrenchment and delay tactics as a strategy to postpone the need for incurring and reporting capital expenditures on their balance sheets, improving profitability in the short term. See *supra* notes 175–94 and accompanying text.

<sup>238</sup> *Comcast Sues EPB in Hamilton County on Eve of Bond Issue*, CHATTANOOGAN (Apr. 22, 2008), <https://www.chattanooga.com/2008/4/22/126367/Comcast-Sues-EPB-In-Hamilton-County.aspx>. The

at deployment strategies used by the major telecommunications companies, the most robust experimentation with future alternative network deployment structures such as mesh networks,<sup>239</sup> white space usage,<sup>240</sup> and other novel methods<sup>241</sup> usually originate from outside voices—civil society advocates,<sup>242</sup> university academics,<sup>243</sup> and companies who have traditionally not been part of the Internet infrastructure “pipes.”<sup>244</sup> In other words, private sector stagnation may be obstructing the creation of redundant infrastructure—a dynamic that harms both competition and national security.

Thus, the time has come for past to serve as prologue: in a manner parallel to USPS’s creation of package delivery and DoD’s creation of ARPANET in collaboration with universities, a governmental initiative appears to be required to

---

ISP lost in court and years later offered competitive Internet service to the fiber service offered by the City of Chattanooga since 2009. Jon Brodtkin, *Comcast Brings Fiber to City That it Sued 7 Years Ago to Stop Fiber Rollout*, ARS TECHNICA (Apr. 30, 2015), <https://arstechnica.com/information-technology/2015/04/comcast-brings-fiber-to-city-that-it-sued-7-years-ago-to-stop-fiber-rollout>. After the city fiber network was installed, Amazon opened a regional facility in Chattanooga, potentially due to the high quality of Internet connectivity. Mike Pare, *Amazon’s Chattanooga Distribution Center Plans to Expand*, TIMES FREE PRESS (Jan. 8, 2012), <https://www.timesfreepress.com/news/news/story/2012/jan/08/amazons-chattanooga-distribution-center-plans-expa/67750>. The municipal network is credited with revitalizing the local economy. David Z. Morris, *Private Telecoms Get Another Win Over Municipal Broadband in Tennessee*, FORTUNE (Apr. 15, 2017), <https://fortune.com/2017/04/15/private-telecom-chattanooga-gig>.

<sup>239</sup> Tim Fisher, *What Is a Mesh Network?*, LIFEWIRE (July 15, 2019), <https://www.lifewire.com/mesh-network-4175202>.

<sup>240</sup> FED. COM’N COMM’N, *White Space*, <https://www.fcc.gov/general/white-space> (last visited Apr. 8, 2019); MICROSOFT WHITESPACES DATABASE, <http://whitespaces.microsoftspectrum.com/> (last visited Apr. 8, 2019).

<sup>241</sup> For example, Google Project Loon has experimented with balloons to deliver internet connectivity. Alastair Westgarth, *Turning on Project Loon in Puerto Rico*, MEDIUM (Oct. 20, 2017), <https://medium.com/loon-for-all/turning-on-project-loon-in-puerto-rico-f3aa41ad2d7f>.

<sup>242</sup> Mark Kaufman, *Mesh Networks: An Alternative Way to Connect to the Internet Gains Steam*, MASHABLE (Jan. 9, 2018), <https://mashable.com/2018/01/09/mesh-networks-provide-alternative-intenet-connection/>.

<sup>243</sup> David Coldewey, *A Mesh Network Spontaneously Erupts in the US and Helps Connect Puerto Rico*, TECHCRUNCH (Nov. 14, 2017), <https://techcrunch.com/2017/11/14/a-mesh-network-spontaneously-erupts-in-the-us-and-helps-connect-puerto-rico/>.

<sup>244</sup> Paul Garnett & Sid Roberts, *Overview of Internet Service Provider Technology Considerations for Rural Broadband Deployments*, MICROSOFT (June 2018), [http://download.microsoft.com/download/6/C/9/6C955541-5053-4A1C-BF0E-22F3BA34CE0F/Microsoft\\_Rural\\_ISP\\_Technology\\_Considerations.pdf](http://download.microsoft.com/download/6/C/9/6C955541-5053-4A1C-BF0E-22F3BA34CE0F/Microsoft_Rural_ISP_Technology_Considerations.pdf).

stimulate the next generation of Internet infrastructure creation. The first step in this initiative involves accurately assessing the full scope of the availability problem.

#### IV. STATUS 303<sup>245</sup>: SEE OTHER—THE NEW METRIC OF “INTERNET ACCESS INSECURITY”

“The issue is, what is chicken?”<sup>246</sup>

As the last section explained, the Internet now constitutes a component of our critical infrastructure. This evolution has fundamentally recast Internet access availability as an economic necessity and national security issue. Yet, the present state of United States Internet availability is comparatively suboptimal, and the full extent of the technology hatching problem remains under-quantified. Indeed, the United States currently lacks even basic, trusted metrics on point. Current FCC tallies of the number of United States residents living without reliable, high-quality Internet access are viewed by experts as potentially suspect.<sup>247</sup> While the FCC suggests that the number is approximately 25 million Americans who lack access to a broadband connection, other studies using multiple different sources of data put the figure as high as 128 million.<sup>248</sup>

Despite inventing the Internet, the United States has steadily fallen behind other countries in both Internet access quality and technology workforce development.<sup>249</sup> The average United States Internet speed in 2017 was only 18.7 megabytes per second—only the tenth fastest in the world.<sup>250</sup> While the FCC and telecoms are

---

<sup>245</sup> *HTTP Status Code Registry*, *supra* note 18.

<sup>246</sup> *Frigalment Importing Co. v. B.N.S. Int’l Sales Corp.*, 190 F. Supp. 116, 117 (S.D.N.Y. 1960) (finding the meaning of chicken to be ambiguous).

<sup>247</sup> Kahan, *supra* note 4.

<sup>248</sup> *Id.*

<sup>249</sup> Our markets, regulatory structures, and the venture capital ecosystem have often rewarded technology business models that ship product fast and extract maximum short-term financial revenue, instead of rewarding those companies that help build a technologically sustainable, more secure society through encouraging long-term benefits and safer products. *See, e.g.*, Matwyshyn, *supra* note 17, at 127 (discussing the costs of current technology business models).

<sup>250</sup> Gaby Galvin, *Countries Where People are the Most Wired In*, U.S. NEWS & WORLD REP. (Aug. 22, 2017), <https://www.usnews.com/news/best-countries/slideshows/10-countries-with-the-fastest-Internet-speeds?onepage>. According to the FCC, the United States ranked tenth out of twenty-eight countries for download speed in 2018. FED COMM’N COMM’N, *2018 Broadband Deployment Report* (Feb. 2, 2018),

currently heralding the arrival of 5G networks<sup>251</sup> that promise average speeds of 50Mbps or higher,<sup>252</sup> the implemented reality of this improvement in Internet access quality will be a boon to only a limited number of households.<sup>253</sup> Most consumers will not be able to benefit from this access improvement for years, if ever; the roll-out of 5G has been slow and limited to densely-populated areas.<sup>254</sup> As these new generations of 5G technology are starting to be rolled out, South Korea leads on deployment,<sup>255</sup> not the United States. And, the history of prior Internet service rollouts is a harbinger of the need for tempered expectations.<sup>256</sup> Indeed, the schedule and scope of availability of 5G to United States users is not publicly well-known,<sup>257</sup> and concerns about underinvestment by Internet Service Providers in developing United States Internet infrastructure persist.<sup>258</sup>

We have also fallen behind on computer security concerns in our Internet infrastructure. Because of multiple security vulnerabilities, all 4G<sup>259</sup> and 5G

---

<https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2018-broadband-deployment-report>.

<sup>251</sup> *FCC's 5G Fast Plan*, FED. COMM'N COMM'N, <https://www.fcc.gov/5G> (last visited Apr. 8, 2019).

<sup>252</sup> Simon Hill, *Is 5G as Fast as They're Saying? We Break Down the Speeds*, DIGITAL TRENDS (Jan. 22, 2019), <https://www.digitaltrends.com/mobile/how-fast-is-5g>.

<sup>253</sup> Jacob Kastrenakes, *AT&T's 5G Network Goes Live in 12 Cities—But You Can't Use It Yet*, VERGE (Dec. 18, 2018), <https://www.theverge.com/2018/12/18/18146246/att-5g-us-launch-hotspot-service-plan-price>.

<sup>254</sup> Aaron Pressman, *Data Sheet—Are the First Customers of 5G the Winners or Losers?*, FORTUNE (Dec. 18, 2018), <http://fortune.com/2018/12/18/data-sheet-5g-wireless-verizon-att-tmobile>.

<sup>255</sup> Elaine Ramirez, *In the Race for 5G, South Korea Shows Off Its Tech Prowess at the Winter Olympics*, FORBES (Feb. 23, 2018), <https://www.forbes.com/sites/elaineramirez/2018/02/23/in-the-race-for-5g-south-korea-shows-off-its-tech-prowess-at-the-winter-olympics/#366add6f2853>.

<sup>256</sup> Matthew Miller, *Verizon Announces 4G Rollout, but Are Any of These US Systems Really 4G?*, ZDNET (Dec. 1, 2010), <https://www.zdnet.com/article/verizon-announces-4g-rollout-but-are-any-of-these-us-systems-really-4g>.

<sup>257</sup> Elizabeth Zima, *What Is 5G, and Why Will It Take So Long to Arrive*, GOV'T TECH. (Apr. 12, 2018), <https://www.govtech.com/network/What-is-5G-and-Why-Will-it-Take-So-Long-to-Arrive.html>.

<sup>258</sup> James Titcomb, *Scientists Create Internet Cables 50,000 Times Faster Than Superfast Broadband*, TELEGRAPH (Feb. 11, 2016), <https://www.telegraph.co.uk/technology/2016/02/11/scientists-create-Internet-cables-50000-times-faster-than-superf>.

<sup>259</sup> Zack Whittaker, *Security Flaw Shows 3G, 4G LTE Networks Are Just as Prone to Stingray Phone Tracking*, ZDNET (July 26, 2017), <https://www.zdnet.com/article/stingray-security-flaw-cell-networks-phone-tracking-surveillance>.

communications suffer from the possibility of adversary interception.<sup>260</sup> The more we connect our society, the more vulnerable we become to national security threats from this Internet connectivity; our adversaries will inevitably seek to disrupt our communications networks, our economy, and our population's safety.

While debates over network neutrality may have been predicated on the appropriate mental model for 2002's Internet, the technical reality and attack vectors of 2020's Internet look starkly different. Professor Wu's original model of network neutrality was focused on

giv[ing] users the right to use non-harmful network attachments or applications, and giv[ing] innovators the corresponding freedom to supply them . . . [because s]uch a regime avoids some of the costs of structural regulation by allowing for efficient vertical integration so long as the rights granted to the users of the network are not compromised.<sup>261</sup>

While this model engages with a portion of the relevant Internet availability issues today, it ultimately falls short. It neglects to expressly consider the technology hatching problem—the potentially devastating national security and economic consequences of the mismatch between our current (unwise) structural (over)reliance on always-on Internet availability and the existing inadequacies of Internet infrastructure.<sup>262</sup>

To wit, this section offers a new framework: The model of “Internet Access Insecurity.” Inspired by the USDA and FDA's concept of food insecurity,<sup>263</sup> the term Internet Access Insecurity refers to a household-level economic and social condition of limited or uncertain Internet access. The model explicitly blends national security and human safety concerns with considerations of next generation commerce into a single metric aimed at tracking Internet availability and redundancy. Effective implementation of an Internet Access Insecurity model will require congressional action—an act that might be called the Internet Infrastructure Availability Act

---

<sup>260</sup> Catalin Cimpanu, *New Security Flaw Impacts 5G, 4G, and 3G Telephony Protocols*, ZDNET (Jan. 31, 2019), <https://www.zdnet.com/article/new-security-flaw-impacts-5g-4g-and-3g-telephony-protocols>.

<sup>261</sup> Wu, *supra* note 28, at 143 (emphasis omitted).

<sup>262</sup> Goodman, *supra* note 59, at 84. As Professor Goodman argues, a conception of innovation focused on the provider edge of networks “overlooks digital divide issues and user economic constraint.” *Id.*

<sup>263</sup> See *infra* note 268 and accompanying text.

("IIAA"). The IIAA should (1) authorize the creation of a blue ribbon commission for next generation infrastructure planning and information security vulnerability correction, (2) direct that multiple agencies outside the FCC engage in enforcement activity to ensure market transparency in Internet availability, and (3) direct the appropriation of funds to the Department of Homeland Security ("DHS") and other agencies to collaborate with state, municipal, and citizen groups in efforts to maximize deployment (and maintenance) of redundant networks on the local level for national security and workforce development purposes.

A. *Error 426*<sup>264</sup>: *Terminology Upgrade Required*

As explained in the introduction, the technology hatching problem refers to the disconnect between the frenetic pace of technology development and the deficit of sufficient technological infrastructure in the United States to support this development in the long term. A critical component of this disconnect involves the availability of reliable and affordable Internet access across the United States, particularly in rural and de-industrializing areas. While even telephone penetration does not reach a perfect 100%,<sup>265</sup> current Internet access in the United States does not meet the benchmarks for availability and redundancy expected of critical infrastructure. Indeed, the metrics for reliably measuring the extent of Internet access inadequacy have not been formalized even for national security purposes.

Therefore, a new metric of "Internet Access Insecurity" will assist with tracking progress toward the goal of fully redundant, universally available, reliable Internet access throughout the United States. As Section III explained, this type of redundancy and availability are essential pre-requisites both for the next stage of innovation in the United States and our national defense. Specifically, inspired by the USDA's and FDA's concept of "food insecurity,"<sup>266</sup> the term "Internet Access Insecurity" refers to the condition where an Internet (human or corporate) end user is forced to reduce Internet use or normal use patterns are disrupted<sup>267</sup> because of

---

<sup>264</sup> HTTP Status Code Registry, *supra* note 18.

<sup>265</sup> FED. COMM'N COMM'N, TELEPHONE PENETRATION BY INCOME BY STATE (May 2010), <https://www.fcc.gov/reports-research/reports/telephone-penetration-reports/telephone-penetration-report-through-march>.

<sup>266</sup> Economic Research Service, *Definitions of Food Security*, U.S. DEP'T OF AGRIC., <https://www.ers.usda.gov/topics/food-nutrition-assistance/food-security-in-the-us/definitions-of-food-security.aspx> (last updated Sept. 4, 2019).

<sup>267</sup> A specific availability minimum and uptime should be attached to the meaning of "disrupted" as context requires.

(1) the lack of high-quality, reliably-available<sup>268</sup> Internet access as a technical matter, (2) unfair surprise arising from the terms of service or other business conduct of the provider,<sup>269</sup> or (3) because of the inability to pay for high-quality, reliably-available access.

Internet Access Insecurity provides an explicitly broader reframing of the various (legitimate) consumer and entrepreneur protection concerns raised by net neutrality advocates. Yet, it offers two key implementation differences. First, it quantifies Internet deployment success based on end user reality, instead of the current structure of ISP self-reporting,<sup>270</sup> eliminating at least a portion of the current opportunities for gaming in Internet deployment statistics.<sup>271</sup> Second, it acknowledges the role that the Internet plays in critical infrastructure, national defense, and the continued success of our economy. As such, it does not rely on the FCC alone but, instead, relies on an effort across the public and private sector to correct the current Internet infrastructure inadequacies of the United States. Regardless of where the policy and legal battles over the FCC's authority over net neutrality end, a broader approach driven by the technology hatching problem is complementary. In other words, monitoring Internet Access Insecurity will assist in the creation of a robust, redundant Internet infrastructure. However, this new model of Internet Access Insecurity requires an implementing statute—the Internet Infrastructure Availability Act.

*B. Status 300<sup>272</sup>: Multiple Choices—The Internet Infrastructure Availability Act*

To implement the goal of universally available, redundant, reliable Internet access in the United States, the proposed Internet Infrastructure Availability Act

---

<sup>268</sup> “Availability” is a term of art in computing that means “ensuring timely and reliable access to and use of information.” Computer Security Resource Center, *Availability*, NAT'L INST. OF STANDARDS & TECH., <https://csrc.nist.gov/glossary/term/availability> (last visited Apr. 8, 2019).

<sup>269</sup> The use of “unfair surprise” here is an intentional linkage to the long-standing doctrines of unconscionability, which are due for resuscitation in light of the unsustainable trajectory of end user license agreements. *See, e.g.*, Pascuale, *supra* note 59, at 72.

<sup>270</sup> *Who Must File Form 477?*, FED COMM'N COMM'N, <https://transition.fcc.gov/form477/WhoMustFileForm477.pdf> (last visited Apr. 8, 2019).

<sup>271</sup> Karl Bode, *Big ISPs Lobby to Kill Attempts at More Accurate Broadband Mapping*, TECHDIRT (Oct. 18, 2017), <https://www.techdirt.com/articles/20171017/10292938419/big-isps-lobby-to-kill-attempts-more-accurate-broadband-mapping.shtml>.

<sup>272</sup> *HTTP Status Code Registry*, *supra* note 18.

should contain at least three separate components. First, the IIAA should create a blue ribbon commission of academic, technical, legal, and policy experts with the explicit instruction of Internet “futures planning”—an exercise that is commonplace among other countries’ governments.<sup>273</sup> Second, the IIAA should explicitly direct agencies beyond the FCC to become involved in aspects of ensuring improved market transparency around the provision of private sector Internet access. Specifically, the FDA, Federal Trade Commission (“FTC”), Department of Justice (“DOJ”), DHS, Consumer Financial Protection Bureau (“CFPB”), Securities Exchange Commission (“SEC”), and Government Accountability Office (“GAO”) should be directed to contribute toward the goal of improving market transparency and fair business practices in Internet access in a manner consonant with their respective traditional missions. Third, Congress should appropriate a local infrastructure innovation fund administered by DHS. The goal of this fund would be to explicitly collaborate with state and local governments and community groups to encourage as many different deployments of redundant Internet infrastructure as possible.

### 1. The Blue-Ribbon Commission: Improving Sustainability and Security

In the Internet Infrastructure Availability Act (IIAA), Congress should borrow historical insights from ARPA’s successful engagement with universities and academic experts.<sup>274</sup> Specifically, the IIAA should direct the creation of a blue ribbon commission composed of two academic<sup>275</sup> expert teams—a technical experts team on the one hand, and legal and policy experts on the other. Working consecutively and then merging their visions jointly, these teams’ charge should focus on planning a trajectory for the United States to achieve universally available, reliable, affordable, maximally redundant Internet access by 2030, coast to coast.

The explicit charge to the technology experts should include initially exploring all technically possible options—those currently known and those theoretically possible with future research—without concern for legal and policy implementation challenges. For example, forms of white space usage and mesh network deployment have not been exhaustively investigated as potentially viable options for large-scale, redundant network deployment on the local level. In other words, the explicit charge is blue sky technological planning, and the report should be made publicly available

---

<sup>273</sup> See, e.g., EUROPEAN COMM’N, *White Paper on the Future of Europe* (Mar. 1, 2017), [https://ec.europa.eu/commission/sites/beta-political/files/white\\_paper\\_on\\_the\\_future\\_of\\_europe\\_en.pdf](https://ec.europa.eu/commission/sites/beta-political/files/white_paper_on_the_future_of_europe_en.pdf) (explaining Europe’s five goal areas for achievement by 2025).

<sup>274</sup> See *supra* notes 216–38 and accompanying text (discussing ARPANET).

<sup>275</sup> Academics continue to lead research in Internet infrastructure. See, e.g., Titcomb, *supra* note 258.



to allow for civil society engagement and oversight. After this stage, the legal and policy team should convene, review the technical team's work product and identify implementation obstacles to each proposed technical pathway, develop solutions, and contribute additional ideas. Finally, jointly, the experts of the blue-ribbon commission might debate the results of these two reports, and provide a set of shared findings on paths forward. For example, the experts might debate the merits of a "Best Minus X%" minimum floor of Internet quality—where the floor of slowest permissible speed legally categorized as "broadband" continually increases as the fastest top speeds sold at a premium also increases.

In particular, the blue-ribbon commission should conduct a comparative international assessment of Internet access availability and deployment models outside the United States. In light of the severity of the technology hatching problem in the United States, the commission should explore unconventional directions for building and repurposing existing human and technical capacity in novel directions. For example, in addition to determining the best method for collecting accurate household-level data on Internet Access Insecurity, the commission should develop a new set of national labs, modeled on those run by the Department of Energy,<sup>276</sup> whose mission will focus on civic interests and the technology hatching problem in an interdisciplinary manner.<sup>277</sup> Similarly, in light of USPS's commitment to universal service<sup>278</sup> and its current role in bioterrorism defense, perhaps USPS could also be reimagined as a scale-free network<sup>279</sup> of hubs to assist with local network deployment in Internet infrastructure defense. Perhaps every mail truck and mailbox could be turned into a node in a national mesh network. Perhaps the postal carrier recruitment program might be expanded to create a set of "technical carrier" roles

---

<sup>276</sup> U.S. DEP'T OF ENERGY, *National Laboratories*, <https://www.energy.gov/national-laboratories> (last visited Apr. 8, 2019).

<sup>277</sup> See *supra* notes 216–38 and accompanying text (discussing interdisciplinary cooperation in the creation of ARPANET). Again, the United States lags has fallen behind other countries in the creation of this type of national research structure. See, e.g., FRENCH NATIONAL CENTRE FOR SCIENTIFIC RESEARCH (CNRS), <http://www.cnrs.fr/en> (last visited Apr. 8, 2019).

<sup>278</sup> Rubio, *supra* note 201 ("Today the nation relies on a vast mailing industry that operates primarily for profit. But that network is underpinned by the United States Postal Service—a self-supporting quasi-corporate government agency that remains committed to universal service by constitutional and congressional mandate.").

<sup>279</sup> For a discussion of scale-free networks, see, for example, Albert Laszlo-Barabasi & Eric Bonabeu, *Scale-Free Networks*, SCIENTIFIC AMERICAN (May 2003), <http://barabasi.com/f/124.pdf>; see also generally Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129 (2005).

who simultaneously obtain training to maintain the mesh network as they deliver (snail)mail and parcels during their routes. Or perhaps a “junior postal inspector” program could build a corps of vetted, trained youths in their late teens and early twenties to make house calls and operate a “help-desk” to assist older populations and others in their communities with Internet problems, helping to protect them from fraud.<sup>280</sup> Perhaps USPS could evolve to become an entry-level technology workforce development program for youth from communities where access to technology mentorship and training are unavailable.<sup>281</sup> Just as USPS solved the “last mile” problem for people in rural areas for their catalog deliveries, perhaps USPS can reprise its historical role as the catalyst for another information network’s expansion.

## 2. The Agencies: Improving Transparency and Suitability

A wise adage cautions, “don’t put all your eggs in one basket.”<sup>282</sup> Yet, historically, we have left Internet availability enforcement solely in the hands of the FCC.<sup>283</sup> But, the FCC is not the only possible arbiter of Internet access deployment and practice.<sup>284</sup> Indeed, the single-minded policy focus on the FCC as the legal lynchpin of Internet availability for United States end users is misplaced. Particularly because of the FCC’s paralysis, the creation, maintenance, and policing of a robust Internet infrastructure is a task too formidable for a single regulator. In light of the changed role of the Internet as part of our national security and critical infrastructure, through the IIAA, Congress should specifically empower agencies and government offices outside of the FCC to contribute to enforcement activity and oversight of deployment, marketing, and trade practices in connection with Internet access. In particular, the FDA, FTC, DOJ, DHS, CFPB, SEC, and GAO should be

---

<sup>280</sup> Indeed, the postal inspector service is interested in youth outreach initiatives, even sponsoring a television program in a cost-effective manner—using asset forfeiture revenue and not tax dollars. David Robb, *U.S. Government Spending Millions to Fund “The Inspectors”*; *Kids Show Airs on CBS*, DEADLINE (Aug. 15, 2016), <https://deadline.com/2016/08/the-inspectors-government-spends-millions-to-fund-cbs-kids-show-1201803819>. Future asset forfeiture revenue could be directed toward the new junior inspectors program.

<sup>281</sup> Peer and adult technology mentorship have been demonstrated to be significantly correlated with teen interest in technology entrepreneurship and careers. *See* Matwyshyn, *supra* note 9, at 73.

<sup>282</sup> *Don’t Put all Your Eggs in One Basket*, DICTIONARY.COM, <https://www.dictionary.com/browse/don-t-put-all-your-eggs-in-one-basket> (last updated 2005).

<sup>283</sup> *See supra* note 268 and accompanying text.

<sup>284</sup> Although “someone should mediate conflicts over alleged deviations from abstract neutrality principles,” it is not clear whether “that arbitrator [should] be an inherently political body like FCC” or an “independent, apolitical arbitrators like the Internet Engineering Task Force.” Berin Szoka & Adam Thierer, *Net Neutrality, Slipper Slopes & High-Tech Mutually Assured Destruction*, PROGRESS & FREEDOM FOUND. 1, 5 (Oct. 2009), <http://www.pff.org/issues-pubs/ps/2009/pdf/ps5.11-net-neutrality-MAD-policy.pdf>.

congressionally directed to contribute to the mission of mitigating and, ultimately, eliminating Internet Access Insecurity.

a. FDA

The United States FDA is responsible for oversight of medical devices and their safety.<sup>285</sup> As part of this mission, the FDA has issued both pre-market and post market “cybersecurity guidance” creating minimum standards of care to which manufacturers attest they adhere prior to releasing a medical device into the market.<sup>286</sup> Because the next generation of IoB medical devices rely on the Internet for key aspects of their functionality, whether the devices can function as designed without consistently available Internet access is a key safety consideration. Therefore, Congress should instruct the FDA to borrow from its model from the USDA’s food security labeling system<sup>287</sup> and to create a new labeling system for medical device Internet access requirements. Device manufacturers would then include this labeling information with their devices, indicating to consumers the minimum availability and quality of Internet access required for safe operation of the device. ISPs would then need to make affirmative representations to consumers about whether their services map to the new FDA standards. The FDA should also be instructed to provide an annual report to Congress regarding collaborations with medical device manufacturers, hospitals, and ISPs, describing what steps are in progress to ensure that patient care is not impacted due to unavailability of Internet access.

b. FTC

Although the Federal Trade Commission has historically been the agency leading enforcement activity with respect to businesses’ Internet conduct, this leadership has not occurred in the context of Internet availability because of the FCC’s overlapping authority. However, FCC Chairman Ajit Pai recently asserted that the FTC should step in to become the primary enforcer for questions of ISP conduct,<sup>288</sup> Congress should heed this advice and direct the FTC to begin robust

---

<sup>285</sup> FOOD & DRUG ADMIN., *What Does FDA Regulate?*, <https://www.fda.gov/about-fda/fda-basics/what-does-fda-regulate> (last updated Mar. 28, 2018).

<sup>286</sup> U.S. FOOD & DRUG ADMIN., DRAFT GUIDANCE: CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES (Oct. 18, 2018), <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices>.

<sup>287</sup> See Economic Research Service, *supra* note 266.

<sup>288</sup> *FCC Chairman Responds to Critics of Net Neutrality Rollback, Vows to Stop “Bad Apples”*, CBS NEWS (June 11, 2018), <https://www.cbsnews.com/news/fcc-ajit-pai-net-neutrality-rollback-vows-consumers-will-be-protected/>.

enforcement activity (and appropriate initial resources accordingly). Specifically, Congress should instruct the FTC to create a new technology practices group, whose mission will be to oversee, among other things, the business conduct of ISPs in offering Internet access to consumers. The new FTC technology practices group should also be granted express fining and rulemaking authority and directed to take such action as needed to stimulate more robust competition among Internet Service Providers and more truthful advertising practices in Internet access.

The new FTC technology practices group should write rules explaining that selective throttling can constitute an unfair and deceptive practice actionable under section 5 of the FTC Act or an anticompetitive practice under antitrust law. The group should also be explicitly instructed by Congress to write rules for use of the word “unlimited” in marketing and advertisements,<sup>289</sup> rules extending requirements of substantiation for any assertions of Internet speed,<sup>290</sup> and such other rules as consumer protection and competition stimulation may require. An ISP’s unexpected throttling should be construed as cause for possible enforcement action and to be an admission of the ISP’s selling access in excess of its capacity—a type of conduct that would be considered potentially a form of consumer fraud in non-Internet contexts or an unfair and deceptive trade practice.

c. DOJ (and FTC)

The IIAA should further direct DOJ to enter into a memorandum of understanding with the FTC around behaviors by Internet Service Providers that may constitute presumptive violations of antitrust laws, such as throttling of websites offering competing content services. Similarly, throttling behavior that knowingly endangers human life should be deemed worthy not only of enforcement action but also potentially worthy of criminal sanction. DOJ and the FTC have already entered into similar memoranda of understanding on other categories of antitrust

---

<sup>289</sup> Each of these techniques has been used by the FTC in other contexts with success; for example, the FTC has standing guidance around the use of the word “free” in marketing. 16 C.F.R. § 251.1 (2018). A parallel approach would make sense for Internet access marketing.

<sup>290</sup> In cases where technical medical claims are made, the FTC requires that an advertiser making those claims previously conduct such tests as to generate a record of substantiated results to back up the veracity of the claims made in the advertisements. FED. TRADE COMM’N, *Advertising Substantiation Principles*, <https://www.ftc.gov/sites/default/files/attachments/training-materials/substantiation.pdf> (last visited Mar. 23, 2019).

enforcement, in particular in the context of corporate information sharing practices and information security.<sup>291</sup> As such, the model is a familiar one to both agencies.<sup>292</sup>

d. DHS

Because of its reclassification by presidential policy directive, United States Internet infrastructure now exists under the supervision of DHS and not merely the FCC.<sup>293</sup> Again, this change highlights the need for a recalibration of the FCC's historically outsized role in Internet availability oversight. DHS, the agency primarily responsible for defense of our domestic critical infrastructure, should more aggressively embrace its new role as steward of Internet infrastructure for national security purposes. In particular, the IIAA should appropriate funds and instruct DHS to create a program that matches municipal and private dollars allocated to local Internet deployment initiatives. Similarly, through IIAA, Congress should direct DHS to launch and appropriate funds for a new program that allows community groups to apply for infrastructure development grants in their communities. For example, imagine a local Girl Scout troop that decided to sell and help deploy mesh network kits alongside its usual cookie initiative.<sup>294</sup> Such a program would assist the community in launching a redundant network and simultaneously assist teens in developing professional skills in technology deployment.<sup>295</sup>

e. CFPB

The IIAA should also instruct the CFPB to issue guidance creating classifications of Internet availability suitable for financial transactions, requiring

---

<sup>291</sup> FED. TRADE COMM'N, *FTC, DOJ Issue Antitrust Policy Statement on Sharing Cybersecurity Information* (Apr. 10, 2014), <https://www.ftc.gov/news-events/press-releases/2014/04/ftc-doj-issue-antitrust-policy-statement-sharing-cybersecurity>.

<sup>292</sup> See *Guidelines and Policy Statements*, DEP'T OF JUSTICE, <https://www.justice.gov/atr/guidelines-and-policy-statements-0> (last updated Dec. 11, 2018).

<sup>293</sup> Directive on Critical Infrastructure Security and Resilience, 1 PUB. PAPERS 112 (Feb. 12, 2013). As a result of this presidential directive, the FCC was instructed to work collaboratively with the Department of Homeland Security. *Id.*

<sup>294</sup> Andrea Matwyshyn (@amatwyshyn), TWITTER (Mar. 13, 2019, 3:32 PM), <https://twitter.com/amatwyshyn/status/1105959813132050432>.

<sup>295</sup> Additionally, the Library of Congress might serve an important collaborative role, assisting DHS and private sector groups in building online educational materials and resources and connecting learners to resources in their local libraries.

that entities under its supervisory authority<sup>296</sup> maintain and provide substantiation documentation explaining all Internet outages impacting consumer access to their services. CFPB should then require annual reporting on these outages and publish the reports on its website. Similarly, this CFPB guidance should require that all of its regulated entities insert contractual “throttling riders” into contracts with Internet Service Providers to prohibit their business partners from degrading the quality of Internet access for their consumers. Failure by a regulated entity to do so should be classified by the IIAA to qualify as an abusive act under the CFPB’s unfair, deceptive and abusive acts and practices authority.<sup>297</sup>

f. SEC

Historically many ISPs have been unwilling to disclose their network management and other traffic practices to shareholders, asserting that net neutrality is not “a significant policy issue.”<sup>298</sup> However, the largest Internet Service Providers are publicly traded companies, and investors appear to view this information as material to their investment decisions. This high level of investor interest in understanding Internet traffic practices,<sup>299</sup> in turn, will potentially have a material impact on market perception of ISPs and their share price. As such, the SEC should be instructed by Congress in the IIAA to issue guidance that requires specific disclosures by ISPs in their annual 10K filings about their traffic management practices (and how they deviate from a zero-throttling baseline), historical data on service interruptions, and such other matters as the SEC believes investors may require.

g. GAO

Finally, the GAO should be instructed by the IIAA to provide an annual report to Congress tracking the status of Internet Access Insecurity in the United States, both in terms of individual agencies’ initiatives and levels of access insecurity experienced by end users. The report should summarize all enforcement activity by agencies intended to improve the quality and extent of Internet access in the United States. It should also provide an international comparative assessment of United

---

<sup>296</sup> CONSUMER FIN. PROT. BUREAU, CFPB DEPOSITORY INSTITUTIONS (BASED ON 9/30/18 TOTAL ASSETS) (2018).

<sup>297</sup> 12 U.S.C. § 5491 (2018).

<sup>298</sup> As explained by one publicly traded Internet service provider: “The proponents of prior proposals on net neutrality issues have argued that net neutrality is a significant public policy issue . . . the Company continues to believe it is not and reserves its right to challenge such an assertion.” AT&T Inc., SEC No-Action Letter, 2013 WL 11080762 (Jan. 15, 2013).

<sup>299</sup> *Id.*

States progress on eliminating Internet Access Insecurity and on remediating the larger technology hatching problem in the United States. This GAO report should also be made public to allow for third-party scrutiny and debate.

### 3. The State and Local Level: Improving Competition and Redundancy

The third component of the IIAA involves congressional clarification of the importance of municipal Internet access as a national security redundancy measure. Redundant networks ensure that critical communications about national security and public safety reach local communities expeditiously. These life-and-death communications should not be contingent on a single company or a single point of failure, such as whether a particular end-user has purchased the “correct” Internet access plan from a private sector entity. Therefore, IIAA should explicitly preempt state authority to take actions that prevent municipalities or citizens from taking (otherwise lawful) steps to improve Internet availability.

Congress’ mandate in Section 706 of the Telecommunications Act of 1996, which aimed to encourage broadband deployment, has been undercut by Internet Service Providers on the local level as part of legal efforts that appear to be intended to restrain local competition. For example, ISPs battled to prevent the City of Chattanooga from expanding its highly successful municipal fiber known as The Gig to surrounding rural areas.<sup>300</sup> In particular, in 2016, the states of Tennessee and North Carolina sued to prevent the FCC from assisting municipalities with broadband expansion.<sup>301</sup> The Sixth Circuit sided with Tennessee and North Carolina, stating the following:

The legislatures of Tennessee and North Carolina have passed laws either forbidding or putting onerous restrictions on such expansion by municipal telecommunications providers. The Federal Communications Commission (FCC), citing its statutory mandates to remove barriers to broadband service and to promote competition in the telecommunications market, has issued an order purporting to preempt these state statutory provisions. Tennessee and North Carolina now seek review of the FCC’s order. The FCC order essentially serves to re-allocate decision-making power between the states and their municipalities. This is shown by the fact that no federal statute or FCC regulation requires the municipalities to expand or otherwise to act in contravention of the preempted

---

<sup>300</sup> Tenn. v. FCC, 832 F.3d 597, 600 (6th Cir. 2016).

<sup>301</sup> *Id.*

state statutory provisions. This preemption by the FCC of the allocation of power between a state and its subdivisions requires at least a clear statement in the authorizing federal legislation. The FCC relies upon § 706 of the Telecommunications Act of 1996 for the authority to preempt in this case, but that statute falls far short of such a clear statement. The preemption order must accordingly be reversed.<sup>302</sup>

Thus, the IIAA should clearly amend Section 706 of the Telecommunications Act of 1996 to expressly preempt state and local restrictions that anti-competitively hinder Internet infrastructure deployment. As a precautionary measure, Congress should also expressly limit the FCC's ability to engage in acts that hinder local deployment, as decided by the FTC and DOJ (while preserving the FCC's ability to assist with this deployment).<sup>303</sup>

## V. CONCLUSION

The Internet is now part of our critical infrastructure and the absence of national redundancy—meaning the existence of “backup” Internet availability uniformly across the United States—presents a real and avoidable national security risk. Our (highly Internet-reliant) economy<sup>304</sup> and governance structures<sup>305</sup> are prime targets for attackers sponsored by other countries, and public safety breakdowns have already occurred due to particular ISPs' throttling of Internet access.<sup>306</sup> As explained above, the current rate of deployment and availability are unlikely to be adequate to sustain the next generation of innovation, particularly as human bodies increasingly

---

<sup>302</sup> *Id.*

<sup>303</sup> As explained by Professor Tejas N. Narechania, Section 706 of the Telecommunications Act of 1996 “explicitly vests state commissions with the authority to encourage the deployment of broadband to all Americans . . . [and t]his concurrent grant of jurisdiction to the FCC and to state commissions has important implications . . . [because it] allows local regulators to act where the FCC has declined to do so.” Tejas N. Narechania, *Federal and State Authority for Broadband Regulation*, 18 STAN. TECH. L. REV. 456, 456, 495 (2015). In this way, he argues, “states may exercise their own section 706 authority to promote ‘infrastructure investment’” through net neutrality regulations. *Id.* at 495–96.

<sup>304</sup> Alice M. Rivlin & Robert E. Litan, *The Economy and the Internet: What Lies Ahead?*, BROOKINGS INST. (Dec. 1, 2001), <https://www.brookings.edu/research/the-economy-and-the-Internet-what-lies-ahead>.

<sup>305</sup> AARON SMITH, GOVERNMENT ONLINE, PEW RESEARCH CTR. (Apr. 27, 2010), <https://www.pewInternet.org/2010/04/27/government-online>.

<sup>306</sup> Matt Stevens, *Verizon Throttle California Firefighters' Internet Speeds Amid Blaze*, N.Y. TIMES (Aug. 22, 2018), <https://www.nytimes.com/2018/08/22/us/verizon-throttling-california-fire-net-neutrality.html>.



rely on Internet access for portions of their functionality. This Article has presented a theoretical reframing of the network neutrality conversation rooted in maximizing availability and network redundancy for economic and national security reasons—the new metric of Internet Access Insecurity. It has also proposed a statutory embodiment of this new paradigm by proposing an implementation statute—the Internet Infrastructure Availability Act. This shifted focus to questions of Internet availability and redundancy is critical to the next generation of our country’s economic and national securing progress. It is also overdue. And chickens eventually come home to roost.<sup>307</sup>

---

<sup>307</sup> BYC Support, *Common Chicken Sayings Idioms Other Funny Things We Say*, BACKYARDCHICKENS.COM (Mar. 18, 2012), <https://www.backyardchickens.com/articles/common-chicken-sayings-idioms-other-funny-things-we-say.47662/>.