EDITOR'S NOTE

The *Federal Communications Law Journal* is proud to present the second Issue of Volume 76. FCLJ is the nation's premier communications law journal and the official journal of the Federal Communications Bar Association (FCBA). We are excited to present the second Issue of this Volume showcasing the diverse range of issues encompassed by technology and communications law. This Issue explores novel approaches to legal questions in areas of trivial computer use and the FCC's network resiliency efforts, as well as an analysis of federal obligations to Tribal Nations.

This Issue begins with an article from Christopher S. Yoo, the John H. Chestnut Professor of Law, Communication, and Computer & Information Science and Founding Director of the Center for Technology, Innovation & Competition at the University of Pennsylvania, and Alex Mueller, a CTIC Research Fellow at the University of Pennsylvania Carey Law School. Their Article considers China's growing Internet standard-setting ambitions and what this could mean for the future of a unified, global Internet.

This Issue also features four student Notes, all of which explore innovative ways to apply existing frameworks to novel technology issues.

First, Angela M. Gasca explores how Amazon's acquisition of One Medical revealed gaps in health data regulation and how those gaps might be filled.

In our second Note, Benjamin A. Soullier argues for a more equitable treatment of trivial computer use by narrowing the Computer Fraud and Abuse Act (CFAA).

In our third Note, Benjamin Duwve proposes the FCC borrow from the Department of Energy's proactive framework to bolster its network resiliency efforts.

Finally, Morgan Gray analyzes Tribal Nations' claims to wireless spectrum based on treaty obligations and the Federal Trust Responsibility.

The Editorial Board of Volume 76 would like to thank the FCBA and The George Washington University Law School for their continued support of the Journal. We also appreciate the hard work of the authors and editors who contributed to this Issue.

The Federal Communications Law Journal is committed to providing its readers with in-depth coverage of relevant communication law topics. We welcome your feedback and encourage the submission of articles for publication consideration. Please direct any questions or comments about this Issue to fclj@law.gwu.edu. Articles can be sent to fcljarticles@law.gwu.edu. This Issue and our archive are available at http://www.fclj.org.

Catherine Ryan
Editor-in-Chief

FEDERAL COMMUNICATIONS LAW JOURNAL

GW LAW

FCBA
FEDERAL COMMUNICATIONS BAR ASSOCIATION

VOLUME 76

Published by the GEORGE WASHINGTON UNIVERSITY LAW SCHOOL and the FEDERAL COMMUNICATIONS BAR ASSOCIATION

Federal Communications Law Journal

The *Federal Communications Law Journal* is published jointly by the Federal Communications Bar Association and The George Washington University Law School. The *Journal* publishes three issues per year and features articles, student notes, essays, and book reviews on issues in telecommunications, the First Amendment, broadcasting, telephony, computers, Internet, intellectual property, mass media, technology, privacy, communications and information policymaking, and other related fields.

As the official journal of the Federal Communications Bar Association, the *Journal* is distributed to over 2,000 subscribers, including Association members as well as legal practitioners, industry experts, government officials and academics. The *Journal* is also distributed by Westlaw, Lexis, William S. Hein, and Bloomberg Law and is available on the Internet at www.fclj.org.

The *Journal* is managed by a student Editorial Board, in cooperation with the Editorial Advisory Board of the FCBA and two Faculty Advisors.

Federal Communications Bar Association

The Federal Communications Bar Association (FCBA) is a volunteer organization of attorneys, engineers, consultants, economists, government officials and law students involved in the study, development, interpretation, and practice of communications and information technology law and policy. From broadband deployment to broadcast content, from emerging wireless technologies to emergency communications, from spectrum allocations to satellite broadcasting, the FCBA has something to offer nearly everyone involved in the communications industry. That's why the FCBA, more than two thousand members strong, has been the leading organization for communications lawyers and other professionals since 1936.

Through its many professional, social, and educational activities, the FCBA offers its members unique opportunities to interact with their peers and decision-makers in the communications and information technology field, and to keep abreast of significant developments relating to legal, engineering, and policy issues. Through its work with other specialized associations, the FCBA also affords its members opportunities to associate with a broad and diverse cross-section of other professionals in related fields. Although the majority of FCBA members practice in the metropolitan Washington, D.C. area, the FCBA has eleven active regional chapters, including: Atlanta, Carolina, Florida, Midwest, New England, New York, Northern California, Southern California, Pacific Northwest, Rocky Mountain, and Texas. The FCBA has members from across the U.S., its territories, and several other countries.

The George Washington University Law School

Established in 1865, The George Washington University Law School (GW Law) is the oldest law school in Washington, D.C. The Law School is accredited by the American Bar Association and is a charter member of the Association of American Law Schools. GW Law has one of the largest curricula of any law school in the nation with more than 275 elective courses covering every aspect of legal study.

GW Law's home institution, The George Washington University, is a private institution founded in 1821 by charter of Congress. The Law School is located on the University's campus in the downtown neighborhood familiarly known as Foggy Bottom.

The *Federal Communications Law Journal* is published by The George Washington University Law School and the Federal Communications Bar Association three times per year. Offices are located at 2028 G Street NW, Suite LL-020, Washington, D.C. 20052. The *Journal* can be reached at fclj@law.gwu.edu, and any submissions for publication consideration may be directed to fcljarticles@law.gwu.edu. Address all correspondence with the FCBA to the Federal Communications Bar Association, 1020 19th Street NW, Suite 325, Washington, D.C. 20036-6101.

Subscriptions: Subscriptions are $30 per year (domestic), $40 per year (Canada and Mexico), and $50 per year (international). Subscriptions are to be paid in U.S. dollars and are only accepted on a per-volume basis, starting with the first issue. All subscriptions will be automatically renewed unless the subscriber provides timely notice of cancellation. Address changes must be made at least one month before publication date, and please provide the old address or an old mailing label. Please direct all requests for address changes or other subscription-related questions to the journal via email at fclj@law.gwu.edu.

Single and Back Issues: Each issue of the current volume can be purchased for $15 (domestic, Canada and Mexico) or $20 (international), paid in U.S. dollars. Please send all requests for single or back issues to fclj@law.gwu.edu.

Manuscripts: The *Journal* invites the submission of unsolicited articles, comments, essays, and book reviews mailed to the office or emailed to fcljarticles@law.gwu.edu. Manuscripts cannot be returned unless a self-addressed, postage-paid envelope is submitted with the manuscript.

Production: The citations in the *Journal* conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia L. Rev. Ass'n et al. eds., 21st ed., 2021). Variations exist for purposes of clarity and at the editors' discretion. The *Journal* is printed by Sheridan.

Citation: Please cite this issue as 76 FED. COMM. L.J. ___ (2024).

FEDERAL COMMUNICATIONS LAW JOURNAL
THE TECH JOURNAL
GW LAW VOLUME 76 ISSUE 2 fcba THE TECH BAR
JANUARY 2024

ARTICLES

Crouching Tiger, Hidden Agenda? The Emergence of China in the Global Internet Standard-Setting Arena

China is making an active push to enlarge its role in the development of Internet-related technical standards. The prevailing narrative surrounding this trend suggests that Beijing is aiming to uproot the liberal, democratic values embedded in the Internet's technical foundation and governance arrangements in favor of authoritarian-friendly alternatives. For many, these fears were fully realized when Chinese tech giant Huawei came to the UN-affiliated International Telecommunications Union (ITU) and proposed the development of a future core Internet protocol called "New IP." This proposal allegedly sought to redesign the architecture of the Internet in a way that would both enhance and export the Chinese government's capacity for digital repression. Informed by the understanding of Chinese standards influence as a geopolitical and ideological threat, many are now calling for a more aggressive response to countering Chinese engagement in Internet standards bodies. Yet, the conventional narrative seems to be missing something. Specifically, it overlooks the fact that the sophisticated Internet control apparatus China has developed over the years can already censor and surveil quite effectively at present and that shifting responsibility for core protocol development to the more state-driven ITU would not necessarily enhance its ability to do so. A more comprehensive understanding of this trend is needed.

Using New IP as the primary case study, this article examines China's standard-setting push, its potential motivations, and its implications for the future of the global Internet. We conclude that it is far from clear that New IP was indeed intended as a trojan horse for digital authoritarianism. Observing that technical evolution of the Internet—particularly the type endorsed in Huawei's proposal—plays a prominent role in China's long-term industrial policy strategy, we find it equally plausible that New IP was motivated by economic considerations, something that has largely been absent from the debate over China's standards ambitions. We thus caution against the presumption that Chinese-developed standards are intended to advance the cause of digital repression as well as against politically driven opposition to growing Chinese participation at Internet standard-setting bodies. This insight is crucial, as the way American policymakers and Internet stakeholders respond to this trend will undoubtedly impact both the future of the global Internet and U.S. technological leadership in this domain.

NOTES

Amazon's Acquisition of One Medical: The Lack of Health Data Regulation in the Age of Big Tech

On February 22, 2023, Amazon acquired One Medical, a membership-based primary health care provider. Both Amazon and One Medical claim that patient data is protected under the Health Insurance Portability and Accountability Act, but this statement is misleading: HIPAA as it exists today does not adequately protect or regulate patient health information in the context of a non-clinical entity subsuming a provider of health care services. Personal health data generated from Amazon customers, and from Big Tech users in general, falls outside the scope of HIPAA protection. But where HIPAA falls short, Section 5 of the FTC Act provides a gap filler. This Note will discuss how existing law—specifically the FTC's Section 5 authority, the Hart-Scott-Rodino Act, and elements from the California Consumer Privacy Act—could be used in the future to regulate health data acquired by non-clinical entities through mergers and acquisitions at the pre-merger stage.

Decriminalizing Trivial Computer Use: The Need to Narrow the Computer Fraud and Abuse Act (CFAA) After *Van Buren*

This Note focuses on the potential for overbroad application of the 18 U.S.C. § 1030(a)(2)(C) felony enhancements for hacking to further another crime or tort, specifically as applied to car theft and the use of car GPS computer systems. The Supreme Court's decision in *United States v. Van Buren* implied a "gate" was necessary for someone to breach authorized access to a protected computer and such gates could potentially be physical barriers. Additionally, the decisions in *United States v. Steele* and *United States v. Yücel* determined there was no double jeopardy issue with the CFAA felony enhancements and a protected computer can be considered any device connected to the Internet or another interstate or international cyber network, respectively. After these decisions, prosecutors now have the discretion to charge the statute much more broadly. As necessary everyday lifestyle becomes more dependent on computer processing capabilities and network connections, there is also a necessity for a change in the statutory language or at minimum, implement a narrower legal standard in courts to avoid improper enforcement. Therefore, this Note will argue the felony enhancements for § 1030(a)(2)(c) should be applied under a new "Substantial Furtherance Test," based on Federal attempt law, to determine if the defendant's unauthorized computer use knowingly and substantially furthered a separate crime or tort. The amended statute will specifically and exclusively apply to computer use that is critical to the attempt or completion of another crime or tort. Finally, this would serve to prevent the federal government from ascribing the enhancements to computer use that, if isolated, would not be a crime under the CFAA, while continuing to enforce criminal liability for actions that align with the original purposes of the CFAA.

Crouching Tiger, Hidden Agenda? The Emergence of China in the Global Internet Standard-Setting Arena

Christopher S. Yoo & Alex Mueller*

TABLE OF CONTENTS

* Christopher S. Yoo is the John H. Chestnut Professor of Law, Communication, and Computer & Information Science and Founding Director of the Center for Technology, Innovation & Competition at the University of Pennsylvania. Alex Mueller is a CTIC Research Fellow at the University of Pennsylvania Carey Law School.

I. INTRODUCTION

In March of 2020, the *Financial Times* reported that China had introduced a new proposal at the International Telecommunications Union (ITU), an independent treaty-based organization acting as a U.N. Specialized Agency, purportedly seeking to initiate a radical, top-down re-design of the Internet.[1] The proposal revolved around something called "New IP," a new core Internet protocol that Chinese tech giant Huawei was reportedly pushing to develop at the ITU's Telecommunications Standardization sector (ITU-T).[2] The *Financial Times* article proceeded to explain that New IP would equip networks with built-in "tracking features" and a "shut up command" for blocking communications, leading it to declare that the future protocols would "bake authoritarianism" into the technical foundation of the Internet.[3] News of Huawei's proposal elicited further criticism from other Western media outlets as well as from various civil society and industry groups that urged ITU Member State delegations to oppose it.[4] Many even cited New IP as evidence of the dangers an unchecked China and/or ITU could pose to the free and open Internet.[5]

In the end, Huawei's efforts proved unsuccessful. Though it attempted to frame the initiative as a necessary technical evolution—arguing the existing

1. *See generally* Anna Gross & Madhumita Murgia, *China and Huawei propose reinvention of the internet*, FIN. TIMES (Mar. 27, 2020), https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2 [https://perma.cc/8KUH-GWHQ].

2. *Id.*

3. *Id.*

4. *See, e.g.*, Margi Murphy, *Internet pioneer Vint Cerf says China's plans to rewrite the web are a "dog's breakfast,"* TELEGRAPH (July 2, 2020 4:06 PM), https://www.telegraph.co.uk/technology/2020/07/02/internet-pioneer-vint-cerf-says-chinas-plans-rewrite-web-dogs/ [https://perma.cc/X32F-PU2H]; Stephen Shankland, *China has big ideas for the internet. Too bad no one else likes them*, CNET (July 17, 2020 2:13 PM), https://www.cnet.com/tech/computing/china-has-big-ideas-for-the-internet-too-bad-no-one-else-likes-them/ [https://perma.cc/F5Z9-V4DP]; Jon Fingas, *China, Huawei propose internet protocol with a built-in killswitch*, ENGADGET (Mar. 30, 2020), https://www.engadget.com/2020-03-30-china-huawei-new-ip-proposal.html [https://perma.cc/47HF-T8R5]; *see also, e.g.*, Letter from Mallory Knodel, CTO, Ctr. for Democracy & Tech. & Heather West, Head of Pub. Pol'y, Mozilla, to Off. of Int'l Affs,, Nat'l Telecomm. and Info. Admin., U.S. DEP'T OF COM. (June 8, 2020), https://ntia.gov/sites/default/files/publications/cdt-mozilla-06082020_0.pdf [https://perma.cc/VU8N-JUNG] (urging U.S. delegates to the ITU-T to oppose New IP activities due in part to its centralized, top-down development approach).

5. *See, e.g.*, Tom Wheeler, *The most important election you never heard of*, BROOKINGS TECHTANK (Aug. 12, 2022), https://www.brookings.edu/blog/techtank/2022/08/12/the-most-important-election-you-never-heard-of/ [https://perma.cc/79DM-STMR] (citing China's push of standards like New IP, which would "give governments more control over internet activities," as a reason why the 2022 ITU Secretary General election is pivotal.); Lindsay Gorman, *Why Biden and Blinken Are Backing a Candidate for a Little-Known U.N. Internet Agency*, LAWFARE (Sept. 28, 2022 3:01 PM), https://www.lawfareblog.com/why-biden-and-blinken-are-backing-candidate-little-known-un-internet-agency [https://perma.cc/XS4X-ACZZ] (arguing that if countries like China and Russia succeed in pushing their agenda at the ITU, then technical proposals like New IP "could provide states the ability to control access to the internet itself.").

Internet architecture was ill-equipped for supporting network use cases anticipated in the future—many were unpersuaded.[6] When it came time to decide whether New IP standardization activities should be initiated at the ITU-T, objections raised by several participating Member States effectively killed the proposal.[7]

Following its unceremonious demise, one might be tempted to let the New IP fade into the annals of Internet history without thinking twice about it. However, the New IP saga offers a valuable case study, one that highlights an important ongoing development in the world of Internet governance. As in many other domains across the global governance system, China is widely regarded as making concerted efforts to increase its role and influence in the development of international technical standards, particularly those involving the Internet and other information and communications technologies (ICTs).[8] This push is typically viewed as part of the broader Chinese project to enhance its position within the international order and to strengthen its "discourse power"—its ability to shape global governance institutions and norms.[9] However, disagreement remains over the specific ends to which China intends to use this discursive power within the standards development system as well as the extent to which it seeks to disrupt the status quo.

An increasingly common understanding of this trend sees China's foray into the standard-setting arena as a Trojan Horse whose true purpose is to uproot the liberal values embedded in the Internet's technical design and governance arrangements.[10] In their place, China intends to install alternatives the enable greater state control and thus align with the concept of "Internet sovereignty," the principle said to represent China's normative position on

6. *See* Int'l Telecomm. Union, Telecomm. Standardization Sector [ITU-T], "*New IP, Shaping Future Network": Propose to initiate the discussion of strategy transformation for ITU-T*, TSAG-C83 (Sept. 10, 2019), https://www.itu.int/md/T17-TSAG-C-0083 [https://perma.cc/6WFE-4UYH [hereinafter TSAG-C83].

7. *See infra* note 188 and accompanying text.

8. *See infra* Part I.B (discussing how China is increasing engagement within the ICT standards ecosystem).

9. *See* Nadège Rolland, *China's Vision for a New World Order* 7-11 (Nat'l Bureau Asian Rsch., Special Rep. No. 83, Jan. 2020) https://www.nbr.org/wp-content/uploads/pdfs/publications/sr83_chinasvision_jan2020.pdf [https://perma.cc/K2AQ-LEUE]; Toni Friedman, *Lexicon: 'Discourse Power' or the 'Right to Speak' (话语权, Huàyǔ Quán)*, DIGICHINA (Mar. 17, 2022), https://digichina.stanford.edu/work/lexicon-discourse-power-or-the-right-to-speak-huayu-quan/ [https://perma.cc/4CE5-P7QD].

10. *See, e.g.*, U.S.-CHINA ECON. & SEC. REV. COMM'N, 2022 REPORT TO CONGRESS 459 (Nov. 2022), https://www.uscc.gov/sites/default/files/2022-11/2022_Annual_Report_to_Congress.pdf [https://perma.cc/4A2K-CBJM] [hereinafter USCC 2022 Report]; DEMOCRATIC STAFF OF S. COMM. ON FOREIGN RELS., 116TH CONG., THE NEW BIG BROTHER: CHINA AND DIGITAL AUTHORITARIANISM 1-2 (July 21, 2020), https://www.govinfo.gov/content/pkg/CPRT-116SPRT42356/pdf/CPRT-116SPRT42356.pdf [https://perma.cc/8T2J-QHZ4] [hereinafter THE NEW BIG BROTHER]; Melanie Hart & Baline Johnson, *Mapping China's Global Governance Ambitions*, CTR. AM. PROGRESS 15-16 (2019), https://www.americanprogress.org/wp-content/uploads/sites/2/2019/02/China-Global-Governance-2.pdf [https://perma.cc/CBG9-6TK5].

the governance of global cyberspace.[11] In other words, Beijing intends to use the country's growing standard-setting influence to design a future Internet that is more regulable, inscribing authoritarian norms of information control and surveillance into its technical foundation.[12] If successful, critics warn it would empower world governments to commit human rights violations at unprecedented scale, lead to the widespread diffusion of Chinese-style digital authoritarianism, and potentially even bifurcate the global Internet along multipolar lines.[13] Although most of these concerns predate New IP, some regard the events at the ITU as the moment China tipped its hand.[14]

At the same time, there are reasons to question the conventional account of China's standard-setting push. The United States' foreign policy apparatus, and its so-called "Internet freedom" agenda, has long regarded the Internet as a type of unstoppable, emancipatory force that would inevitably democratize the societies in which it was embedded.[15] Meanwhile, in having maintained a firm grasp over its domestic Internet for nearly three decades, China has

---

11. *See* USCC 2022 Report, *supra* note 10, at 460; Samm Sacks, *Beijing Wants to Rewrite the Rules of the Internet*, THE ATLANTIC (June 18, 2018), https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/ [https://perma.cc/P7YL-Z5LE]; Kenton Thibaut, *Chinese Discourse Power: Aspirations Reality and the Digital Domain*, THE ATL. COUNCIL (Aug. 24, 2022), at 22-23, https://www.atlanticcouncil.org/in-depth-research-reports/report/chinese-discourse-power-ambitions-and-reality-in-the-digital-domain/ [https://perma.cc/KRA9-WZ2X].

12. *See* Daniel F. Runde & Sundar R. Ramanujam, *Digital Governance: It Is Time for the United States to Lead Again*, CTR. STRATEGIC & INT'L STUD. 2 (Aug. 2, 2021), https://www.csis.org/analysis/digital-governance-it-time-united-states-lead-again [https://perma.cc/F7PY-NSZL] (stating China wants to reinvent the Internet in the name of regulating it); Paul Scharre, *The Dangers of the Global Spread of China's Digital Authoritarianism*, CTR. NEW AM. SEC. (May 4, 2023), https://www.cnas.org/publications/congressional-testimony/the-dangers-of-the-global-spread-of-chinas-digital-authoritarianism [https://perma.cc/A5SQ-K2JP] (cautioning that China's growing standard-setting influence risks spreading standards that enable "Chinese-style surveillance and repression").

13. *See* Douglas W. Arner et al., *The Transnational Data Governance Problem*, 37 BERKELEY TECH. L.J. 623, 681 (2022) (arguing China is attempting to internationalize its centralized Internet structure and, consequently, create a parallel digital market dominated by Chinese firms and technologies); Joshua Kurlantzick, *How China Is Attempting to Control the "Information Pipes,"* THE DIPLOMAT (Mar. 3, 2023), https://thediplomat.com/2023/03/how-china-is-attempting-to-control-the-information-pipes/ [https://perma.cc/Y26Y-U38D] (suggesting the pursuit of influence over ICT infrastructure would enable China to export its "vision of a closed and controlled domestic internet"); Stacie Hoffman et al., *Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet*, 5 J. CYBER POL'Y 241, 252-53 (2020) (warning that proposals like New IP could splinter the global Internet).

14. *See, e.g.*, Emily Taylor et al., *Technical Standards and Human Rights: The Case of New IP*, *in* RECLAIMING HUMAN RIGHTS IN A CHANGING WORLD ORDER 185, 186 (Christopher Sabatini ed., 2022) (arguing New IP reveals a lot about China's ambitions and serves as a wake-up call about its potential impact on global Internet governance and standards).

15. *See* Jack Goldsmith, *The Failure of Internet Freedom*, 18-03 KNIGHT FIRST AMEND. INST. 2-4 (June 13, 2018), https://knightcolumbia.org/content/failure-internet-freedom [https://perma.cc/KQE4-NY5G] (examining the Internet freedom agenda that first emerged during the Clinton administration and its two main attributes: commercial non-regulation and anti-censorship); EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM xii-xiv (2012) (defining this belief in the inherently democratizing nature of the Internet as a naïve "cyber-utopianism").

succeeded at a task once regarded as so futile that former-President Bill Clinton famously analogized it to "nail[ing] Jell-O to the wall."[16] China's existing Internet control capabilities—the complex legal and technical architectures that enabled it to do so—beg the question: does China need to highjack the global standard-setting process and push through protocols like New IP just to make the Internet more regulable? To be sure, legal scholarship has long recognized how design choices underlying the Internet's technical architecture can function as the "law of cyberspace," shaping and constraining how individuals use the network much like a traditional regulatory regime.[17] Still, the nearly insurmountable difficulty of replacing the global Internet's common foundation makes it natural to ask why China would attempt to do so in the name of greater control despite having largely achieved this through other means.

As ICT standard-setting bodies become increasingly seen as sites of ideological and geopolitical contention, calls grow louder for a more aggressive approach to countering Chinese influence in this sphere.[18] Yet, if the trojan horse narrative is going to inform how policymakers and participants in the global standard-setting process respond to the growing involvement of Chinese actors, it is clear that a more comprehensive understanding of the trend is needed.

This Article thus sets out to answer two primary questions. First, we ask whether China's growing standard-setting ambitions are indeed motivated by a desire to fundamentally change the Internet's technical architecture and the institutional arrangements through which it is shaped, re-aligning both

---

16. President William J. Clinton, Remarks at the Paul H. Nitze School of Advanced International Studies (Mar. 8, 2000), http://www.presidency.ucsb.edu/ws/index.php?pid=87714 [https://perma.cc/5EZZ-4FRS]; *see also* Goldsmith, *supra* note 15, at 9 ("[A] decade after Bill Clinton's presidency had ended, China was doing a pretty good job of nailing the Jell-O of undesirable speech to the wall of Party control.").

17. For leading early statements, *see generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999) [hereinafter LESSIG, CODE]; Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998). For later discussions, Daniel Benoliel, *Technological Standards, Inc.: Rethinking Cyberspace Regulatory Epistemology*, 92 CALIF. L. REV. 1069 (2004); Kevin Werbach, *Higher Standards Regulation in the Network Age*, 23 HARV. J.L. & TECH. 179 (2009); Deirdre K. Mulligan & Kenneth A. Bamberger, *Saving Governance by Design*, 106 CALIF. L. REV. 697 (2018).

18. *See, e.g.*, U.S.-CHINA ECON. & SEC. REV. COMM'N, 2020 REPORT TO CONGRESS 537 (Dec. 2020), https://www.uscc.gov/sites/default/files/2020-12/2020_Annual_Report_to_Congress.pdf [https://perma.cc/HQE9-LCQC] [hereinafter USCC 2020 Report] (recommending the creation of a government committee that would coordinate the activities of private sector participants at standards bodies in order to compete with China); Sophie Faaborg-Andersen & Lindsay Temes, *The Geopolitics of Digital Standards*, HARV. KENNEDY SCH. BELFER CTR. SCI. & INT'L AFFS. (July 2022), at 1-2, https://www.belfercenter.org/sites/default/files/files/publication/geopolitics-of-digital-standards.pdf [https://perma.cc/UTL5-FDC7] (arguing that market-driven standards development is not equipped to repel the creep of digital authoritarianism and that the U.S. should reverse its historically hands-off approach); Bradley A. Thayer & Lianchao Han, *We cannot let China set the standards for 21st century technologies*, THE HILL (Apr. 16, 2021 1:00 PM), https://thehill.com/opinion/technology/548048-we-cannot-let-china-set-the-standards-for-21st-century-technologies/ [https://perma.cc/FGD4-SKE6].

with its state-centric normative orientation. Second, we inquire into what the trend of increasing Chinese engagement holds for the future of a unified, global Internet. In attempting to answer these questions, we draw primarily on a case study of New IP. Although a more measured analysis of Huawei's proposal reveals several flaws, we ultimately find reason to doubt that its sole motivations were to embed authoritarian values and to expand state control over the Internet. Instead, most of the features discussed by the proposal align closely with the type of future network capabilities China has deemed necessary for supporting its lofty industrial policy goals as well as Huawei's own financial interests. This leads us to argue that New IP may well have been motivated by economic considerations, something frequently overlooked in the broader debate over China's growing role in standards development and requires a more nuanced than countenanced by the conventional account. In other words, it cannot be assumed that every Chinese-produced technology or technical standard is intended to enable digital repression or undermine liberal, democratic values. This will become an increasingly important lesson as Chinese actors continue to grow their presence within mainstream Internet standards development bodies; the American response will undoubtedly have implications for both the future of the global Internet and U.S. technological leadership.

The remainder of this Article is organized as follows: Part I better situates our discussion by providing an overview of the Internet standards development landscape and China's evolving role therein, as by well examining China's alternative vision for the global Internet and digital governance organized around the concept "cyber sovereignty." In Part II, we shift our focus to the Article's primary case study, the New IP proposal, and construct a clearer picture of what Huawei was proposing to help better understand its possible motives. New IP was alleged to propose fundamental changes to the way the Internet works, but *how*? Part III grapples with the conventional explanation of China's standards push as a trojan horse for a more state-centric Internet architecture and standards development model. It identifies several of the theoretical shortcomings behind this framing and demonstrates how they manifest prominently in the case of New IP. Part IV then offers an alternative account of China's standard-setting ambitions, arguing they are motivated to a significant extent by economic factors. Finally, Part V explores what this trend means for the future of the global Internet and standards development. Contrary to predictions of an impending global "splinternet" or an ITU Internet takeover, we find that China has grown increasingly accepting of the existing industry-led, bottom-up, incremental approach to shaping the Internet's architecture. Our conclusion thus offers a warning that coordinated and politically motivated opposition to Chinese engagement risks undermining the standards development model that has contributed to the Internet's extraordinary success.

II. CHINA'S STANDARD-SETTING AMBITIONS: A BACKGROUNDER

Protocols are the lifeblood of the Internet. They are standardized rules for formatting, interpreting, and reacting to a communication, thereby establishing a common language that enables components of a communications system to interoperate and exchange data.[19] The overall architecture of the Internet is comprised of many protocols spread across different functional "layers" into which the various tasks of the communications process are divided. The vertical combination of protocols at each layer, all of which work together to provide a full communications service, is known as the protocol stack. Protocols at the bottom layers of the stack are responsible for managing the physical transmission of data, while those in the upper layers provide features for supporting specific applications (e.g., email or web) without needing to worry about how lower-layer functions have been implemented.

However, the most fundamental protocol resides in the very middle and is simply called the Internet Protocol (IP). When data is transmitted over the Internet, it is divided into smaller packets that a system of interconnected routers then forwards along to the intended destination based on an address specified in each packet's header. It is IP that defines the structure and format of both these packets and addresses. Although there are a variety of protocols that can be used in the upper layers (e.g., HTTP for web, SMTP for email) and bottom layers (e.g., Ethernet or Wi-Fi), virtually every communication over the Internet relies on IP in the middle.[20] The centrality of IP, along with that of another important protocol called TCP at the layer above, is why the Internet as we know is said to run on the TCP/IP suite.

As implied by its name, Huawei's New IP initiative sought to undertake the modernization of this crucial Internet Protocol. Yet, before diving fully into the case of New IP, there is some important background information needed to understand why the proposal was so controversial and to fully appreciate the larger trend at the heart of this Article. The remainder of this Part will set the stage for our subsequent discussion on the underlying motives and future implications of China's Internet standards ambitions. It will do so first by introducing the system that has emerged for developing protocols and other Internet technical standards, then by outlining how China's role within this system has been quickly evolving, and finally by examining the concept cyber sovereignty which is said to inform China's goals and engagement in this sphere.

19. Christopher S. Yoo, *Protocol Layering and Internet Policy*, 161 U. PA. L. REV. 1707, 1716 (2013).

20. Due to the wide diversity of protocols at the upper and lower layers but with just one core protocol in the middle, the Internet architecture is often said to resemble an hourglass figure.

A. A Condensed Overview of the Internet Standards Development Landscape

The development of standards is an essential function of Internet governance, a term which refers to the different activities for coordinating and managing the Internet's technical infrastructure to ensure it remains operational, stable, and secure.[21] The existing system of global Internet governance is considered to be polycentric; its constituent functions are spread out across multiple different institutions, each with a unique configuration and makeup.[22] Moreover, though the term "global governance" may be commonly associated with multilateralism (i.e., state-actors engaging in collective decision-making at intergovernmental bodies like the U.N.), some of the most important functions of global *Internet* governance are performed with limited to no government involvement.[23] Instead, these functions are carried out through institutions that embody a multistakeholder governance approach, engaging a wide range of non-state actors including those from industry, civil society, and academia.[24] These defining characteristics of the Internet governance system as a whole—its polycentricity and the prominent role afforded to non-state actors—can also be found in the Internet standards development ecosystem, which consists of several primarily industry-driven, private standards development organizations (SDOs).

As mentioned above, the Internet architecture consists of many protocols spread across different functional layers of the Internet stack. The scope of responsibilities among different SDOs in the ecosystem tends to reflect the modularity of the Internet's layered architecture, with each SDO limiting their focus to a specific layer or layers of the stack. The Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA), for example, develops lower-layer protocols and physical infrastructure standards, most recognizably the IEEE 802.3 series (Ethernet) and IEEE 802.11 series (Wi-Fi). Similarly, a consortium of regional telecom SDOs called the Third-Generation Partnership (3GPP) defines wireless communications protocols (e.g., 5G-NR) that perform lower-layer functions in mobile broadband networks. At the topmost layer, typically referred to as

---

21. Although the precise definition of Internet governance is still somewhat contested, the way we use the term here is consistent with the relatively narrow definition offered by Laura DeNardis which focuses on issues unique to the Internet's technical infrastructure. *See* LAURA DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE 18-20 (2014) [hereinafter DENARDIS, GLOBAL WAR]; *see also* Mark Raymond & Laura DeNardis, *Multistakeholderism: Anatomy of an Inchoate Global Institution*, 7 INT'L THEORY 572, 588-92 (2015) (providing a taxonomy of the different activities that fall underneath the umbrella of Internet governance).

22. *See* DENARDIS, GLOBAL WAR, *supra* note 21, at 22-23 (describing the distributed nature of Internet governance); *see also* Joseph S. Nye, Jr., *The Regime Complex for Managing Global Cyber Activities*, CTR. INT'L. GOVERNANCE INNOVATION (May 2014), at 7, https://www.cigionline.org/static/documents/gcig_paper_no1.pdf [https://perma.cc/DHG4-9E9N] (locating Internet governance within the broader "cyber regime complex," a collection of loosely connected, non-hierarchical norms and institutions for governing cyberspace).

23. Raymond & DeNardis, *supra* note 21, at 585.

24. *See id.* at 586.

the Application Layer, the World Wide Web Consortium (W3C) focuses on protocols and other standards related to web technologies.

However, the most important SDO in the Internet standard-setting ecosystem is the Internet Engineering Task Force (IETF). The IETF is an open, international community of volunteers that has traditionally been responsible for maintaining and evolving the core protocols towards the middle of the stack—including both the IP and TCP in the TCP/IP suite—as well as a significant number of different Application Layer protocols. The organization's history is closely tied to that of the Internet itself, having evolved out of the same community of U.S. government-funded network researchers and engineers that laid the foundation of what would eventually become the modern Internet.[25]

While most of the other SDOs described above could be considered "open" to varying degrees, the IETF is notoriously so.[26] All IETF standards, published in the form of documents called RFCs, are made publicly available online along with just about every other conceivable piece of information produced within the organization.[27] The IETF also has no formal membership and thus no membership fees.[28] Any individual who wishes to participate can do so in full.[29] This includes attending any of the three annual in-persons meetings, submitting an Internet Draft (i.e., a proposed standard or informational document), or joining one of the Working Group mailing lists where much of the discussion takes place. Though a large share of participants tends to be affiliated with network operators, equipment vendors, or other companies that implement IETF standards, many also come from civil society organizations, universities, and even government agencies. That said, participants are expected to act in their individual capacities rather than as representatives of corporations or governments.[30]

The IETF is also renowned for its informal, collaborative ethos. Participants openly debate the technical merits of a proposed standard based

---

25. *See* DENARDIS, GLOBAL WAR, *supra* note 21, at 67-71 (providing an overview of the IETF's historical origins).

26. *See* A. Michael Froomkin, *Habermas@discourse.net: Toward a Critical Theory of Cyberspace*, 116 HARV. L. REV. 749, 799 (2003); Werbach, *supra* note 17, at 199.

27. *See* DENARDIS, GLOBAL WAR, *supra* note 21, at 71.

28. *The Tao of the IETF: A Novice's Guide to the Internet Engineering Task Force*, INTERNET ENG'G TASK FORCE (last updated Nov. 17, 2022), https://www.ietf.org/about/participate/tao/ [https://perma.cc/BEQ2-SQ6H] ("The IETF has no members and no dues.").

29. *Id.*

30. Harald Tveit Alvestrand, *A Mission Statement for the IETF* (IETF Network Working Grp., RFC No. 3935, 2004), http://www.ietf.org/rfc/rfc3935.txt [https://perma.cc/9YNM-7LL2] ("The IETF has found that the process works best when focused around people, rather than around organizations, companies, governments or interest groups."). Although norms strongly discourage individual participants from representing the interests of their employers, that does not mean commercial interests do not find their way into the IETF. This can have an impact on the standard-setting process, as one empirical analysis found a statistically significant relationship between the concentration of private-sector participants in a working group—a so-called "beard-to-suit ratio"—and lengthier delays in reaching consensus. *See generally* Timothy Simcoe, *Standard Setting Committees: Consensus Governance for Shared Technology Platforms*, 102 AM. ECON. REV. 305 (2012).

on its real-world implementations, advancing it along the standards track only if there is widespread agreement among the group.[31] A famous adage from Internet pioneer David Clark perhaps best captures the spirit of the organization's modus operandi: "We reject kings, presidents and voting; we believe in rough consensus and running code."[32] Though certainly not without criticism, the IETF has remained the preeminent Internet standards body for nearly forty years. It is the organization's participatory and radically transparent nature to which many attribute its enduring legitimacy.[33]

It is important to keep in mind when discussing the Internet standards ecosystem that, even though a division of responsibility has emerged among the different SDOs, this has largely been the result of private self-ordering.[34] For example, there was never an inter-governmental agreement granting the IETF exclusive authority over the middle layers of the Internet stack.[35] Instead, these polycentric arrangements are informal and took shape organically over time.[36] There is often nothing preventing one SDO from engaging in standards work that has traditionally fallen under the purview of another. Nonetheless, SDOs tend to respect each other's remits and coordinate in order to avoid inefficiently duplicating work, creating of incompatible standards, or causing uncertainty in the marketplace.[37]

There is one SDO, however, that has somewhat of a history of encroaching on others' technical mandates while attempting to enlarge its

---

31. *See* Scott Bradner, *IETF Working Group Guidelines and Procedures § 3.3* (IETF Network Working Grp., RFC No. 2418, 1998), http://www.ietf.org/rfc/rfc2418.txt [https://perma.cc/84S4-MEAQ].

32. David D. Clark, *A Cloudy Crystal Ball: Visions of the Future*, PROC. 24TH INTERNET ENG'G TASK FORCE 543 (Megan Davies et al. eds. 1992), https://www.ietf.org/proceedings/24.pdf [https://perma.cc/SJK3-JW45].

33. *See, e.g.*, Froomkin, *supra* note 26, at 798-805 (examining the IETF through the lens of Habermas's discourse ethics, arguing that it satisfies the procedural conditions the generate legitimacy.).

34. *See id.* at 755-56 (describing the Internet, a largely self-regulating system that emerged in the absence of an international legal framework, as a type of "orderly anarchy").

35. Joseph Liu, *Legitimacy and Authority in Internet Coordination: A Domain Name Case Study*, 74 IND. L.J. 587, 588 (1999) (noting that working groups have no formal legal authority, not do the standards they produce have legally binding effects).

36. *See* MILTON MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE 217 (2010) [hereinafter MUELLER, NETWORKS AND STATES] (using the term "organically developed Internet institutions" to refer to the transnational groups of actors that took shape with the Internet outside of the nation-state system.).

37. *See* NIZAR ABDELKAF ET AL., UNDERSTANDING ICT STANDARDIZATION: PRINCIPLES AND PRACTICE 62 (2018), https://www.etsi.org/images/files/Education/Understanding_ICT_Standardization_LoResWeb_20190524.pdf [https://perma.cc/XQ6Q-5S4D] (describing this coordination as "inherent to the spirit of standardization"). By uncertainty, we refer to situations in which the market hesitates to adopt either of two competing standards due to fears of selecting the loser and stranding one's investment. *See* CARL L. SHAPIRO & HAL R. VARIAN, INFORMATION RULES 230 (1998).

own.[38] We are talking of course about ITU-T, the Geneva-based venue where Huawei presented its controversial New IP proposal. Although ITU-T and its standards were instrumental in enabling international interoperability among public switched telephone networks, this did not translate into a significant role within the modern Internet standards ecosystem.[39] Instead, its involvement has been mostly limited to lower-layer Internet access technologies such as Digital Subscriber Line (DSL), which uses standard telephone lines as a transmission medium, as well as the optical fiber used in carrier networks.[40]

To get a more complete picture of ITU-T, one of the three sectors of the ITU, it is helpful to know a bit of its history. The ITU was established in 1865, when twenty predominantly European states signed a treaty intended to facilitate policy coordination and technical interoperability among the Continent's telegraph networks.[41] It then gradually expanded over the next eighty years, admitting new member states[42] and adding new forms of telecommunications, such as radio and telephony to its remit.[43] This continued until 1947, when it became officially recognized as a specialized agency of the United Nations.[44] It now consists of 193 Member States (i.e., countries that acceded to the ITU Constitution and Convention) that are typically represented by their respective national telecommunications administrations.[45]

As an international multilateral body with roots in pre-war Europe, the ITU and its standardization sector unsurprisingly embody a much more formal, top-down style of governance than the IETF.[46] Participation in ITU-T is restricted to its members, a category which includes both Member States

38. The New IP proposal is far from the only example of the ITU-T entertaining possible standards work that would have overlapped with another SDO. *See, e.g.*, Stanley M. Besen & George Sadowsky, *The Economics of Internet Standards*, *in* HANDBOOK ON THE ECONOMICS OF THE INTERNET 211, 220 (Johannes M. Bauer & Michale Latzer eds., 2017); Iljitsch van Beijnum, *ITU bellheads and IETF netheads clash over transport networks*, ARS TECHNICA (Mar. 3, 2011, 10:25 AM), https://arstechnica.com/tech-policy/2011/03/itu-bellheads-and-ietf-netheads-clash-over-mpls-tp/ [https://perma.cc/PG99-DXTF]; Jorge L. Contreras, *Divergent Patterns of Engagement in Internet Standardization: Japan, Korea and China*, 38 TELECOMM. POL'Y 914, 920 (2014).

39. *See* Scott J. Shackelford & Amanda N. Craig, *Beyond the New Digital Divide: Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119, 125 (2014).

40. The ITU-T's limited role is not for a lack of trying. Throughout its history, the institution has been involved in multiple attempts at developing data networking standards as alternatives to TCP/IP. However, each of these failed to gain significant long-term adoption. *See infra* Part III.A.

41. *The 1865 International Telegraph Conference*, INT'L TELECOMM. UNION (last accessed May 25, 2023), http://handle.itu.int/11.1004/020.2000/s.138 [https://perma.cc/4F4L-SZPA].

42. Ernest K. Smith, *The History of the ITU, with Particular Attention to the CCITT and the CCIR, and the Latter's Relations with URSI*, 11 RADIO SCI. 497, 498-99 (1976).

43. *Overview of ITU's History (3)*, INT'L TELECOMM. UNION (last accessed May 25, 2023), http://handle.itu.int/11.1004/020.2000/s.210 [https://perma.cc/9X3W-RWZD].

44. *Id.*

45. Raymond & DeNardis, *supra* note 23, at 598-99.

46. Patrick S. Ryan, *The ITU and the Internet's Titanic Moment*, 2012 STAN. TECH. L. REV. 8 ¶ 26 (2012).

as well as any companies, civil society groups, or academic institutions that have been formally admitted as dues-paying "sector members."[47] However, the participation rights granted to non-state sector members come with limitations, as there are certain privileges within ITU-T enjoyed exclusively by Member States. This hierarchical membership structure is not reflected much in the day-to-day standardization work taking place within ITU-T Study Groups, but it does exclude these sector members from involvement in major internal governance decisions.[48]

Another area of sharp contrast between the IETF and ITU-T is with regards to transparency.[49] While final versions of approved ITU-T standards (called "Recommendations") are made public, all other working documents are stored in an internal database accessible only to its members.[50] This effectively prevents any visibility into ongoing developments within ITU-T, making it difficult for both civil society and the general public to play an oversight role. When paired with the superior decision-making authority it grants to government actors, the behind-closed-doors nature of the ITU thus appears to be more amenable to the style of governance preferred by states like China. In fact, we need not even speculate here, as China itself has been quite vocal in its support for expanding the ITU's role within the global Internet governance system.[51]

B. International Standardization with Chinese Characteristics

Having arrived at the subject of China, it is useful to see how its own role within Internet-related SDOs and the broader ICT standard-setting environment has been evolving. Despite having boasted the world's largest number of Internet users for quite some time, the influence of Chinese actors here has historically been limited. This is largely due to China's status as a latecomer.[52] When many modern ICTs and their corresponding SDOs were first beginning to take shape, China was still undergoing major economic

---

47. *See* Raymond & DeNardis, *supra* note 21, at 598-99. In 2023, the standard ITU-T annual membership fee was 31,800 CHF for sector members and 3,975 CHF for academic members. *Fees*, INT'L TELECOMM. UNION, https://www.itu.int/en/ITU-T/membership/Pages/Categories-and-Fees.aspx#:~:text=The%20annual%20fee%20for%20Sector,fee%3A%203%2C975%20CHF%20per%20year.&text=Focus%20your%20resources%20on%20a,for%20Associate%20is%2010%2C600%20CHF [https://perma.cc/DP5M-ELYR] (last visited Feb. 26, 2023).

48. Raymond & DeNardis, *supra* note 21, at 599.

49. Ryan, *supra* note 46, ¶ 40 ("[T]he IETF's philosophy of access and transparency could not be more different than that of the ITU.").

50. *Id.* ¶ 39.

51. *See, e.g.*, *Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development*, KREMLIN.RU (Feb. 4, 2022), http://en.kremlin.ru/supplement/5770 [https://perma.cc/FS5V-TWNS] ("The sides support the internationalization of Internet governance . . . [and] are interested in greater participation of the International Telecommunication Union in addressing these issues.").

52. *See* Lennart Schott & Kerstin J. Schaefer, *Acceptance of Chinese Latecomers' Technological Contributions in International ICT Standardization — The Role of Origin, Experience and Collaboration*, 52 RSCH. POL'Y 1-2 (2023).

reforms and lacked much of a domestic technology sector.[53] As a result, Chinese actors were forced to play catch-up with those from the U.S., EU, and Japan who had already established themselves.[54]

During this catching up period, China often distanced itself from the global standards development system. Instead, it tended to focus on the development of its own homegrown standards, a strategy intended to promote indigenous technologies, gradually build up innovation capacity, and reduce dependence on foreign proprietary standards.[55] From the perspective of Western market economies, however, this approach to standardization had a clear protectionist agenda.[56]A prime example of this indigenous standards strategy in action can be found in the WLAN Authentication and Privacy Infrastructure (WAPI), an alternative Wi-Fi security standard developed in China during the early 2000s.[57] The Chinese government made adoption of the WAPI standard compulsory for wireless network-enabled devices and equipment sold within its market, a requirement that would have forced foreign firms to license the underlying IP from a select group of Chinese companies. Since mandating this indigenous standard threatened to significantly impede foreign vendors' access to the Chinese market and even splinter the global wireless networking market, the U.S., EU, and others raised concerns that China was flouting some of its World Trade Organization (WTO) obligations, specifically the Technical Barriers to Trade agreement that will be discussed at greater length *infra* Part III.A.[58] The U.S. et al. ultimately pressured China into suspending the mandate and, following several years of unsuccessfully pushing WAPI at international standards

53. Contreras, *supra* note 38, at 924.

54. *Id.*

55. *See* DIETER ERNST, INDIGENOUS INNOVATION AND GLOBALIZATION: THE CHALLENGE FOR CHINA'S STANDARDIZATION STRATEGY 19-27 (2011) (analyzing China's technical standardization strategy during this "catching-up" phase and the goals it serves).

56. *See e.g.*, *2003 Report to Congress on China's WTO Compliance*, U.S. TRADE REPRESENTATIVE (Dec. 11, 2003), at 36-37, https://ustr.gov/archive/assets/Document_Library/Reports_Publications/2003/asset_upload_file425_4313.pdf [https://perma.cc/9VD8-8XVP] ("China is actively pursuing the development of unique requirements, despite the existence of well-established international standards. This course of action will create significant barriers to entry into its markets . . . .").

57. For a more in-depth background and analysis of the WAPI dispute, *see* Christopher S. Gibson, *Globalization and the Technology Standards Game: Balancing Concerns of Protectionism and Intellectual Property in International Standards*, 22 BERKELEY TECH. L.J. 1403, 1434-45 (2007).

58. *See* Committee on Technical Barriers to Trade, *G/TBT/M/32, Minutes of the Meeting of 23 March 2004*, WORLD TRADE ORG. (Apr. 19, 2004), at ¶¶ 8-12, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/G/TBT/M32.pdf&Open=True [https://perma.cc/A2QT-JKSN].

venues and attempting to defend subsequent iterations of the mandate, China eventually abandoned the standard altogether.[59]

It was also around the late 2000s that some began to observe China's strategy beginning to shift towards a greater focus on global standards influence.[60] Perhaps disputes such as those over WAPI forced China to acknowledge that this indigenous standards strategy was becoming increasingly untenable as the country deepened its integration into the world economy. On the other hand, perhaps China simply believed it had arrived at a point where it possessed sufficient innovation capacity and standards development experience to be competitive in the global standards arena. In any case, the last decade and a half has seen the government of China—led by and inextricably entwined with the Chinese Communist Party (CCP)—accelerate its efforts to transform the country into a global standards leader.

Much has already been written about the strategic framework China has adopted for expanding its international technical standards footprint, so we intend only to summarize it briefly here.[61] The strategy, whose focus is not just limited to ICT standards, has been described as comprising two tracks.[62] Each of these tracks represents a separate avenue through which Chinese-developed standards are to be proliferated.

The first track focuses on international SDOs, seeking to increase both the representation of Chinese actors and the competitiveness of their

---

59. *See* Gibson, *supra* note 57, at 1439-43 (recounting China's unsuccessful efforts to get WAPI approved as an ISO-recognized international standard). In 2009, China resurrected the mandate for mobile handset devices, which would be required to support WAPI and in addition to the widely the standard 802.11 (Wi-Fi) specification. As was quite predictable, this mandate faced a similar level of resistance as the original before it was ultimately dropped. *See* Committee on Technical Barriers to Trade, *G/TBT/M/48*, *Minutes of the Meeting of 25-26 June 2009*, WORLD TRADE ORG. (Sep. 29, 2009), at ¶¶ 49-50, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/G/TBT/M48.pdf&Open=True [https://perma.cc/9CHQ-FX6E].

60. *See e.g.*, Contreras, *supra* note 38, at 30 (observing significant growth in Chinese engagement at the IETF during this time which suggests China has "left behind its role of 'catching up'").

61. *See generally* John Seaman, *China and the New Geopolitics of Technical Standardization*, FRENCH INST. OF INT'L RELS. NOTES (Jan. 27, 2020), https://www.ifri.org/en/publications/notes-de-lifri/china-and-new-geopolitics-technical-standardization [https://perma.cc/9FGF-YGCS]; Sorina Teleanu, *The geopolitics of digital standards: China's role in standard-setting organisations*, DIPLOFOUNDATION (Dec. 2021). https://www.diplomacy.edu/resource/report-the-geopolitics-of-digital-standards-chinas-role-in-standard-setting-organisations/ [https://perma.cc/4SY6-ZSAE]; Tim Rühlig, *Chinese Influence through Technical Standardization Power*, 32 J. CONTEMPORARY CHINA 54 (2023); Julia Voo & Rogier Creemers, *China's Role in Digital Standards for Emerging Technologies - Impacts on the Netherlands and Europe*, LEIDEN ASIA CTR. (May 2021), https://leidenasiacentre.nl/wp-content/uploads/2021/05/Chinas-Role-in-Digital-Standards-for-Emerging-Technologies-1.pdf [https://perma.cc/CBX2-GDAJ]; Emily de la Bruyère, *Setting the Standards: Locking in China's Technological Influence*, *in* CHINA'S DIGITAL AMBITIONS: A GLOBAL STRATEGY TO SUPPLANT THE LIBERAL ORDER 49 (Nat'l Bureau Asian Rsch., NBR Special Rep. No. 97, Emily de la Bruyère et al. eds., 2022); Daniel R. Russel & Blake H. Berger, *Stacking the Deck: China's Influence in International Technology Standards Setting*, ASIA SOC'Y POL'Y INST. (2021), https://asiasociety.org/sites/default/files/2021-11/ASPI_StacktheDeckreport_final.pdf [https://perma.cc/J4EK-TLZT].

62. Seaman, *supra* note 61, at 20.

contributions. To do so, China has been known to offer financial support and incentives intended to boost engagement at prioritized SDOs.[63] This includes subsidizing participation costs (e.g., membership fees, travel, training, etc.) as well as providing monetary awards to those who submit contributions or secure leadership positions.[64] Within these SDOs, there are many reports of Chinese participants acting in a highly coordinated manner such as by voting blocs.[65] The precise mechanism for achieving this coordination is not entirely known, but most assume it involves some degree of direction from the party-state.[66]

The second track of China's strategy operates outside the conventional institutional framework for global standard-setting and instead facilitates international adoption of Chinese-developed standards through its various bilateral trade and investment relationships.[67] This approach can be characterized as a de facto standardization strategy, wherein Chinese domestic standards are elevated to global status through widespread market acceptance rather than formal recognition by an international body. Though the diffusion of Chinese standards might initially be focused on those countries with whom China has close economic linkages, the rest of the world may begin to quickly follow once the level of global adoption reaches a critical mass.[68]

This de facto standardization track is closely related to China's Digital Silk Road (DSR), which has become a component of its larger Belt and Road Initiative.[69] The DSR seeks to enhance digital connectivity and trade between China and other partner countries through ICT infrastructure construction

63. Rühlig, *supra* note 61, at 66-67.

64. de la Bruyère, *supra* note 61, at 57.

65. *Id.* at 59 (quoting one interviewed SDO participant as saying "other countries' delegates act like individuals. China's act like a group"); Russel & Berger, *supra* note 61, at 12 (stating that Chinese firms flood SDOs with large volumes of standards proposals and vote in a single bloc). *But see infra* notes 77-79 and accompanying text (finding that China's use of manipulative tactics has been overstated and that its growing success at SDOs is more attributable to improvements in standards proposal quality).

66. Rühlig, *supra* note 61, at 67-68 (explaining that party-state's level of involvement and control makes it possible for a strategy in which Chinese actors "speak with one voice" at SDOs); de la Bruyère, *supra* note 61, at 60 (indicating that the party-state is uniquely positioned to influence how Chinese firms engage with SDOs).

67. Seaman, *supra* note 61, at 24-25; de la Bruyère, *supra* note 61, at 61.

68. *See* SHAPIRO & VARIAN, *supra* note 37, at 13-14 (explaining that adoption of technologies subject network effects can begin to experience explosive growth once it reaches the point where demand-side economies of scale begin to kick in).

69. *See* Alex He, *The Digital Silk Road and China's Influence on Standard Setting*, CTR. INT'L. GOVERNANCE INNOVATION (Apr. 4, 2022), at 2-3, https://www.cigionline.org/publications/the-digital-silk-road-and-chinas-influence-on-standard-setting/ [https://perma.cc/34PN-R8YE] (providing an overview of how digital "standards connectivity" fits into the DSR initiative).

projects.[70] The financing for these projects, typically offered on generous terms by one of China's state-owned development banks, is conditioned on the use of Chinese-manufactured components.[71] The DSR thus helps externalize Chinese domestic ICT standards by facilitating the export of products that adhere to them.[72]

The results of China's efforts thus far have been mixed but trending upwards. Whether the expanded international market for Chinese ICTs enabled by the DSR will provide a durable source of de facto standards power still remains to be seen.[73] When looking at the global ICT standards environment in general, China's influence is still overshadowed by that of the U.S. and some other Western counterparts. However, there has been an observed increase in Chinese participation and submissions across several SDOs.[74] This participation is not just limited to venues endorsed by China, such as ITU-T, but includes those like the 3GPP, IEEE-SA, and—as we will highlight later—the IETF.[75] Further, as demonstrated by the success enjoyed by Chinese firms like Huawei during the 5G standardization process, there is mounting evidence that China's impact within these SDOs is growing.[76]

It would be a mistake to dismiss these recent successes as the product of tactics like packing SDOs with participants or flooding them with high volumes of standards proposals.[77] Quantity alone does not necessarily translate to influence within SDOs, especially since most of them utilize

70. Unlike most major Chinese political initiatives, the DSR is not the result of the CCP's top-down planning. Instead, it evolved out of the natural efforts of Chinese multi-national tech companies to begin expanding into relatively untapped international markets. The party-state eventually embraced this trend and began to promote it as a formal initiative under the BRI. *See* Robert Greene & Paul Triolo, *Will China Control the Global Internet Via its Digital Silk Road?*, CARNEGIE ENDOWMENT INT'L PEACE (May 08, 2020), https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857 [https://perma.cc/Q2K5-JG6E].

71. Matthew S. Erie & Thomas Streinz, *The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance*, 54 N.Y.U. J. INT'L L. & POL. 1, 53 (2021).

72. *Id.* at 45.

73. *See* Teleanu, *supra* note 61, at 63.

74. *See id.* at 7 (summarizing the report's analysis of trends in Chinese engagement at ICT SDOs).

75. *See id.*; *see also infra* Part IV.B (discussing Chinese actors' increasing engagement at the IETF).

76. *See* Voo & Creemers, *supra* note 61, at 11-13.

77. Matt Sheehan & Jacob Feldgoise, *What Washington Gets Wrong About China and Technical Standards*, CARNEGIE ENDOWMENT INT'L PEACE (Feb. 27, 2023), https://carnegieendowment.org/2023/02/27/what-washington-gets-wrong-about-china-and-technical-standards-pub-89110 [https://perma.cc/D55J-7GSZ] (finding that the general belief among the peers of Chinese SDO participants is that manipulative tactics are the exception rather than the rule).

consensus-based decision-making.[78] Instead, there seems to be an emerging consensus that Chinese actors have made steady improvements in the quality of their contributions at ICT-related SDOs.[79] The competitiveness of Chinese standards contributions has also benefited—even if indirectly—from China's large investments into developing national technical expertise and innovation capacity in areas it deems strategically important.[80] Since standards influence remains a major priority for the CCP, such progress should only be expected to continue.

C. China's Alternative Vision for Cyberspace

As China has turned its strategic focus towards the development global technical standards and provided an increasingly formidable source of competition for Western participants, the perception of standards bodies as a type of political battlegrounds has become more common. However, this is unlikely to be much of a revelation to those who have long studied the field. There is a vast body of literature, spanning several decades and different academic disciplines, examining the political nature of technical standards and standardization. To summarize it in just a few words, protocols are political.[81]

The Internet standard-setting process brings together a diverse collection of actors with disparate goals and interests. There is often a tremendous amount at stake in the outcome, as decisions here can tilt entire markets in a company's favor and/or have consequences in the form of millions of dollars.[82] At a more macro level, standards power can promote

78. Giulia Neaher et al., *How Can the United States Navigate the Geopolitics of International Technology Standards?*, ATL. COUNCIL (Oct. 2021), at 16, https://www.atlanticcouncil.org/wp-content/uploads/2021/10/Standardizing-the-future-How-can-the-United-States-navigate-the-geopolitics-of-international-technology-standards.pdf [https://perma.cc/LK68-GKLK]; Naomi Wilson, *China Standards 2035 and the Plan for World Domination—Don't Believe China's Hype*, COUNCIL ON FOREIGN RELS. (June 3, 2020) https://www.cfr.org/blog/china-standards-2035-and-plan-world-domination-dont-believe-chinas-hype [https://perma.cc/RJ6N-JDY5].

79. Rühlig, *supra* note 61, at 60 (reporting that most interviewed SDO participants acknowledged an improvement in the quality of Chinese proposed standards); Teleanu, *supra* note 61, at 41 (noting there has been an observed increase in the quality of Chinese proposals over time as resources have been allocated to training); Riccardo Nanni, *Digital Sovereignty and Internet Standards: Normative Implications of Public-Private Relations Among Chinese Stakeholders in the Internet Engineering Task Force*, 16 INFO. COMMC'N & SOC'Y 2342, 2355 (2022) (finding that interviewed IETF participants generally agreed that Chinese actors have grown more effective within the IETF as they have gained experience).

80. *See* Voo & Creemers, *supra* note 61, at 7; Rühlig, *supra* note 61, at 66.

81. LAURA DENARDIS, PROTOCOL POLITICS: THE GLOBALIZATION OF INTERNET GOVERNANCE 71 (2009) [hereinafter DENARDIS, PROTOCOL POLITICS]; *see also* JANET ABBATE, INVENTING THE INTERNET 179 (1999) ("The debate over network protocols illustrates how standards can be politics by other means."); SHAPIRO & VARIAN, *supra* note 37, at 240 (describing the formal standard-setting process as a "wild mix of politics and economics"); LAWRENCE LESSIG, CODE VERSION 2.0 62, 78 (2006) [hereinafter LESSIG, CODE 2.0].

82. *See* Froomkin, *supra* note 26, at 795 ("Decisions regarding standards now have important financial consequences for would-be providers of Internet hardware and software, and tempers can flare when tens of millions of dollars are at stake.").

domestic industries and bolster national prestige by signaling a country's technological prowess.[83] The standards arena thus serves as a site of mediation among these many competing interests, where the different stakeholders vying for influence must engage in a series of tradeoffs and compromises over choices that have the potential to shift the balance of economic power.[84] In this sense, the process is political.[85]

Yet, there is a different way in which Internet standard-setting might be understood as political, one that resonates more with the dominant narrative of China's standards ambitions. Beyond the economic interests at stake, the standards process often involves choices over the values that should inform and be prioritized in the design of a protocol.[86] Not only does a protocol reflect these normative choices made by its designers, but the values embedded in its design can have important implications for civil liberties (e.g., privacy, free expression) as well as the distribution of power and authority in society.[87] Similarly, as legal scholars such as Lawrence Lessig and Joel Reidenberg observed over two decades ago, the technical design and implementation of the Internet's architecture is capable of serving a regulatory function that supplements or even supplants law in cyberspace.[88] A logical extension of this metaphor is that those who control the development of protocol standards—the common blueprints for implementing different parts of the Internet's

83. *See* ABBATE, *supra* note 81, at 147-48.

84. *See* SHAPIRO & VARIAN, *supra* note 37, at 240 (describing the "logrolling" that can take place in formal standardization venues.); *see also* Colin J. Kiernan & Milton L. Mueller, *Standardizing Security: Surveillance, Human Rights, and the Battle Over TLS 1.3*, 11 J. INFO. POL'Y 2-4 (2021) (offering the term "political economy of standardization" to capture the political nature of this process more accurately).

85. Kiernan & Mueller, *supra* note 84, at 2.

86. *See* Mulligan & Bamberger, *supra* note 17, at 707 (explaining that decisions in the design process have become sites for resolving value disputes).

87. DENARDIS, PROTOCOL POLITICS, *supra* note 81, at 71; Ian Brown et al., *Should Specific Values Be Embedded in the Internet Architecture?*, PROC. RE-ARCHITECTING INTERNET WORKSHOP (Art. No. 10) (Nov. 30, 2010), https://conferences.sigcomm.org/co-next/2010/Workshops/REARCH/ReArch_papers/10-Brown.pdf [https://perma.cc/4KWA-49XN]. It should be noted that this claim about protocols, embedded values, and their social impact is not uncontested. Milton Mueller and Farzaneh Badiei direct several challenges at this notion, pointing out both the voluntary nature of protocol adoption and the difficulty of knowing *a priori* how a given design choice will impact a set of values once introduced into a complex real-world setting. *See generally* Milton Mueller & Farzaneh Badiei, *Requiem for a Dream: On Advancing Human Rights via Internet Architecture*, 11 POL'Y & INTERNET 61 (2019). Even those who generally accept the premise nonetheless acknowledge that translating values into technical designs that uphold or enforce those values is not always straightforward, often leading to unforeseen or unintended consequences. *See* Helen Nissenbaum, *From Preemption to Circumvention: If Technology Regulates, Why Do We Need Regulation (and Vice Versa)?*, 26 BERKELEY TECH. L.J. 1367, 1370 (2011); Mulligan & Bamberger, *supra* note 17, at 710.

88. Reidenberg, *supra* note 17, at 568 ("Rules established in this fashion form a legal regulatory regime. In the context of information flows on networks, the technical solutions begin to illustrate that network technology itself imposes rules for the access to and use of information."); LESSIG, CODE, *supra* note 17, at 89 ("The code or software or architecture or protocols . . . constrain some behavior by making other behavior possible or impossible. The code embeds certain values or makes certain values impossible. In this sense, it too is regulation . . . .").

architecture—assume the role of lawmakers.[89] Hence, the competition over influencing Internet standards might be framed as a struggle over a private, transnational regulatory power and the values that should guide its use.[90]

According to the prevailing narrative, the impetus behind China's growing presence in the global standards arena is the goal of contesting the Western liberal values.[91] In their place, China intends to install a set of norms and values that reflects it competing vision for the global Internet, the alternative it offers to the "free and open" version historically championed by the United States. At the center of this vision is a new guiding principle for governing and building order in international cyberspace, a concept China refers to as cyber sovereignty (*wangluo zhuquan*).[92]

The starting point for any discussion of Chinese cyber sovereignty should be to recognize that China's own articulation of the concept, found across various policy documents and speeches by Party officials, has been vague and even logically inconsistent at times.[93] China has insistently characterized cyber sovereignty as the natural extension of national sovereignty—a "basic norm in contemporary international relations"—into the domain of cyberspace.[94] Yet, these explanations offer little in the way of clarification, as the principle of sovereignty itself frequently takes on different meanings and is invoked by states to advance a wide range of political

89. LESSIG, CODE, *supra* note 17, at 60; Mulligan & Bamberger, *supra* note 17, at 713.

90. *See* LESSIG, CODE, *supra* note 17, at 60 ("How the code regulates, who the code writers are, and who controls the code writers . . . reveal how cyberspace is regulated."); DENARDIS, PROTOCOL POLITICS, *supra* note 81, at 91 (analogizing power over standards to the ability to enact public policy that directly impacts individuals who use a technology).

91. *See supra* notes 10-12 and accompanying text.

92. This term is often translated as Internet sovereignty or network sovereignty.

93. *See* Rogier Creemers, *China's Conception of Cyber Sovereignty: Rhetoric and Realization*, *in* GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY 107 (Dennis Broeders & Bibi van den Berg eds., 2020) [hereinafter Creemers, *China's Conception of Cyber Sovereignty*] (noting official documents tend to define cyber-sovereignty in broad, vague terms); Katharin Tai & Yuan Yi Zhu, *A Historical Explanation of Chinese Cyber-Sovereignty*, 22 INT'L RELS. ASIA-PAC. 469, 484-86 (2022) (arguing that cyber sovereignty's "seeming lack of coherence" is due to its origin as a domestic propaganda device rather than part of a clear, comprehensive vision.).

94. *International Strategy of Cooperation on Cyberspace*, MINISTRY FOREIGN AFFS. PEOPLE'S REPUBLIC CHINA (Mar. 1, 2017), http://www.xinhuanet.com//english/china/2017-03/01/c_136094371.htm [https://perma.cc/M2QD-WYQA] [hereinafter *International Strategy of Cooperation*] (describing cyberspace as a "new domain of state sovereignty"); *Full Text: Jointly Build a Community with a Shared Future in Cyberspace*, CHINA DAILY (Nov. 2022 10:49 AM), at § IV, https://www.chinadaily.com.cn/a/202211/07/WS63687246a3105ca1f2274748.html [https://perma.cc/F8RY-GT88] [hereinafter *SCIO, Shared Future in Cyberspace*] (reprinting white paper issued by the China's State Council Information Office) ("China advocates . . . that a just and rational international order in cyberspace be built on the basis of national sovereignty.").

objectives.[95] Multiple commentators who have undertaken the task of deciphering China's conception of cyber sovereignty have instead observed that it consists of at least three separate dimensions: a national security dimension, a domestic governance dimension, and international governance dimension.[96]

The national defense dimension implicitly links cyber sovereignty to territorial integrity, a widely accepted norm derived from the principle of sovereignty under international law.[97] From this perspective, respect for cyber sovereignty as a primary rule of international law would prohibit a state from promoting, supporting, or condoning cyber-activities that harm ICT infrastructure located within another state's territorial borders.[98] This dimension is thus consistent with the way cyber sovereignty has been frequently discussed in the American legal-academic context over the last decade, where the discourse has concentrated on how sovereignty and derivative norms should apply to cyber-conflict and state conduct in cyberspace.[99] However, China has tended to emphasize this dimension far less than the others, perhaps understandably given the history of Chinese state-sponsored extraterritorial cyber-operations.[100]

China's conception of cyber sovereignty is much more concerned with ideological security than it is with the security of cyber-infrastructure residing within its territory.[101] Beijing sees the West's idealization of an open, borderless global Internet that permits the unimpeded flow of information as a threat to domestic stability and Party rule.[102] As a direct response, the second dimension of Chinese cyber sovereignty—the domestic governance

95. *See* Henning Lahmann, *On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace*, 32 DUKE J. COMP. & INTL. L. 61, 91 (2021); HARRIET MOYNIHAN, THE APPLICATION OF INTERNATIONAL LAW TO STATE CYBERATTACKS: SOVEREIGNTY AND NON-INTERVENTION ¶ 62 (2019), https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf [https://perma.cc/U943-DC3T].

96. Sarah McKune & Shazeda Ahmed, *The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda*, 12 INT'L J. COMMC'N 3835, 3837 (2018); *see also* Anqi Wang, *Cyber Sovereignty at Its Boldest: A Chinese Perspective*, 16 OHIO ST. TECH. L.J. 395, 403 (2020) (presenting a similar yet slightly modified tri-dimensional framework).

97. *International Strategy of Cooperation*, *supra* note 94 (asserting that states "exercise jurisdiction over ICT infrastructure, resources and activities within their territories" and have the right to protect them from "from threat, disruption, attack and destruction"); *see also* Anupam Chander & Haochen Sun, *Sovereignty 2.0*, 55 VAND. J. TRANSNAT'L L. 283, 294 (2022) (noting the emphasis on territoriality appears to be a nod to international law).

98. President Xi Jinping, President of the People's Republic of China, Remarks at the Opening Ceremony of the Second World Internet Conference (Dec. 16, 2015), http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml [https://perma.cc/E2EG-X6X2] [hereinafter Xi WIC speech] (stating that no country should "connive at or support cyber activities that undermine other countries' national security").

99. *See generally* Eric Talbot Jensen, *Cyber Sovereignty: The Way Ahead*, 50 TEX. INT'L L.J. 275 (2014); Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. L. REV. 1639 (2017); Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AM. J. INT'L L. UNBOUND 207 (2017).

100. *See* Lahmann, *supra* note 95, at 80-81.

101. *See id.* at 82; Creemers, *China's Conception of Cyber Sovereignty*, *supra* note 93, at 130.

102. Wang, *supra* note 96, at 406.

dimension—asserts that all sovereign states have the right to choose their own "path of cyber development, model of cyber regulation, and Internet public policies" without foreign interference.[103] If a country wants to restrict certain information flows or pursue technological independence in the name of security, it should be able to do so without being undermined from the outside (e.g., by foreign states providing locals with circumvention tools).[104]

Having been described as a "cyber-Westphalia,"[105] China thus envisions a global cyberspace where states have exclusive control over deciding how Internet infrastructure and activities within their territories are regulated.[106] To lend legitimacy to this interpretation of cyber sovereignty, China again appeals to widely accepted international legal principles, this time those of non-intervention and self-determination. Yet, as many have noted, the widespread acceptance of these principles has never been invitation for states to disregard other international legal commitments, namely the rights to free expression and access to information enshrined in international human rights law.[107] This is what China is ostensibly trying to justify when it asserts cyber sovereignty.[108]

The use of cyber sovereignty as a pretext for censorship and other forms of Internet control is why China's global promotion of the principle has many alarmed. When concerns are raised over China's purported strategy to re-organize the global Internet around cyber sovereignty, it is this second dimension that is typically being referenced. Understood this way, modifying the Internet's technical architecture to better align with cyber sovereignty would seem to entail equipping networks with features that provide states the option to exert greater control over information flows or to identify users so they can be held accountable for violations of domestic law. In other words, it would involve the development of a new Internet architecture that, by default, is more regulable.

Finally, China's conception of cyber sovereignty also has an international governance dimension. Citing the principle of sovereign

---

103. *International Strategy of Cooperation*, *supra* note 94; *see also* Adam Segal, *China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace*, *in* AN EMERGING CHINA-CENTRIC ORDER: CHINA'S VISION FOR A NEW WORLD ORDER IN PRACTICE 85 (Nat'l Bureau Asian Rsch., NBR Special Rep. No. 87, Nadège Rolland ed., 2020) (interpreting Chinese cyber-sovereignty as a pushback against the West's insistence on the universality of values like free expression, access to information, and privacy from the state.); Creemers, *China's Conception of Cyber Sovereignty*, *supra* note 93, at 129 (recognizing the concept's defensive, reactive nature).

104. A 2010 speech by then Secretary of State Hillary Clinton, in which she admonished China for its Internet censorship and reaffirmed the U.S.'s commitment to empowering foreign citizens with the tools for bypassing it, is often recognized as a catalyst behind China increasingly assertive stance on cyber sovereignty. *See* Tai & Zhu, *supra* note 93, at 490. Segal, *supra* note 103, at 91; Goldsmith, *supra* note 15, at 4-6.

105. *See, e.g.*, Chris C. Demchak, *Uncivil and Post-Modern Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age*, 1 CYBER DEF. REV. 49, 55-64 (2016).

106. *See, e.g.*, Lahmann, *supra* note 95, at 77.

107. *See id*. at 105-106; McKune & Ahmed, *supra* note 96, at 3849.

108. *See* Tai & Zhu *supra* note 93, at 491-92 (illustrating how China will invoke cyber sovereignty as a reaction to those provoking the tension between its system and human rights, the latter of which it believes are subordinate to national sovereignty).

equality enshrined in the U.N. Charter, China maintains that all countries have the right to participate on equal footing in the governance of the Internet and global cyberspace.[109] It has stated that no state should pursue or maintain "cyber-hegemony" and that decisions in this sphere "should not be made with one party calling the shots."[110] As suggested by these subtle jabs at a particular unnamed country, this dimension was heavily influenced by China's discontentment with how the existing system of Internet governance privileges the United States and reflects its preferences for a multistakeholder, limited-government model.[111] Although the alternative China offers to this system would allow industry and civil society to participate in consultative role, it would—for all intents and purposes—represent a much more state-centric form of governance.[112]

Equally notable is the rhetorical move China makes when promoting this international governance dimension of cyber sovereignty. Here, it characterizes cyberspace as a shared, global commons for which all countries bear the responsibility of preserving together.[113] On its face, this depiction of cyberspace appears to directly contradict the highly territorialized version it uses to justify its Internet control regime.[114] Although the contradiction could theoretically be reconciled by introducing a principle that clearly demarcates common cyberspace from national cyberspace, there has yet to be a serious attempt at doing so. Some have argued that contradictions like these are why China has struggled thus far to gain international acceptance for its interpretation of cyber sovereignty.[115] However, this early lack of success has certainly not stopped China from continuing to try.

---

109. *SCIO, Shared Future in Cyberspace*, *supra* note 94, § III.3 ("It has been China's consistent view that all countries, big or small, strong or weak, rich or poor, are equal members of the international community and are entitled to equal participation in developing a global order and international rules, to ensure that the future development of cyberspace is decided by people of the world").

110. Xi WIC speech, *supra* note 98.

111. *See* Creemers, *China's Conception of Cyber Sovereignty*, *supra* note 93, at 130; Wang, *supra* note 96, at 44-46.

112. *See* Xi WIC speech, *supra* note 98 (describing China's envisioned governance model as a "multilateral approach with multi-party participation").

113. *Id.* ("The Internet is the common home of mankind. Making it better, cleaner and safer is the common responsibility of the international community."); *International Strategy of Cooperation*, *supra* note 94 ("Cyberspace is the common space of activities for mankind, hence needs to be built and managed by all countries.").

114. *See, e.g.*, *The Internet in China*, INFO. OFF. OF THE STATE COUNCIL OF CHINA (June 8, 2010), at § VI, http://www.china.org.cn/government/whitepaper/node_7093508.htm [https://perma.cc/4AMR-TCDU] [hereinafter *Internet in China* whitepaper] ("Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty . . . . [L]egal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China . . .").

115. *See, e.g.*, McKune & Ahmed, *supra* note 96, at 3846-50 (highlighting contradictions of the Internet sovereignty promoted by China and explaining how this has served as a barrier to gaining international acceptance).

III. UNDERSTANDING NEW IP

The New IP proposal involved several elements that caused it to attract an unusual amount of attention: an emerging global superpower, its controversial national tech champion, potential implications for civil liberties, and at the center of it all, alterations to a revolutionary technology that has woven itself into the fabric of everyday life. Given what was potentially at stake, it should come as no surprise that along with this attention, the proposal attracted a great deal of speculation. Yet, if we are to draw any valuable conclusions about New IP, its purpose, and what it spells for the future direction of the global Internet, it is necessary to first separate hype from reality.

In this section, we offer a clearer, more precise picture of what was being proposed using internal ITU-T documents along with other Huawei-authored research and SDO contributions. Despite some reports to the contrary, nothing contained in the New IP proposals approximated an actual technical standard, at least not the type capable of being adopted and implemented.[116] The proposals instead sought to initiate preliminary, high-level planning activities for the future protocols. Thus, our goal here is not to make predictions about what New IP would have looked like in its final form, as it is impossible to predict how the full process would have played out. However, the high-level solutions and underlying technical justifications contained in the proposal materials still provide valuable insights into the problems New IP is attempting to solve as Huawei understands them. This, in turn, sheds light on what Huawei and China might hope to accomplish. The remainder of this section will examine the three main functional features advanced by the proposal.

A. Better-than-Best Effort Service

Transmission of data packets over the IP-based public Internet typically occurs on a "best effort" basis. This means the network provides neither a guarantee that traffic will reach its destination within a certain amount of time, nor that it will get there at all. A data packet traveling over the public Internet typically passes through several intermediate routers, each one of which decides where to forward the packet next based on the destination address specified in its header.[117] When a packet arrives at an intermediate router, it is placed in a queue where it typically waits until all the packets arriving earlier have been processed and forwarded. Under the best effort delivery

116. *See, e.g.*, Madhumita Murgia & Anna Gross, *Inside China's controversial mission to reinvent the internet*, FIN. TIMES (Mar. 27, 2020), https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f [https://perma.cc/5QJ6-NSH7] (suggesting that ITU participants would decide whether to adopt New IP at the 2020 World Telecommunications Standardization Assembly).

117. *See generally What is routing?*, CLOUDFLARE, https://www.cloudflare.com/learning/network-layer/what-is-routing/#:~:text=Cloudflare%20Argo%20uses%20smart%20routing,the%20online%20experience%20for%20users [https://perma.cc/V54L-CYC8] (last visited Feb. 19, 2023).

model, packets in a router queue are effectively treated equally, meaning no packet is given special priority.[118] Longer queues translate to longer waiting times, and when a queue becomes too long, the router may be forced to beginning dropping excess packets. Thus, when the network load increases, it is not unusual to experience higher levels of packet loss, delay (latency), and delay variation (jitter).

This best effort service model has worked well for traditional applications like email, while modern applications like real-time video have also managed to adapt. However, Huawei argues that best effort service will be inadequate to meet the needs of many future network use cases that have uniquely high sensitivity to different quality of service (QoS) dimensions like latency, jitter, and packet loss.[119] Such use cases include telemedicine operations (i.e., remote surgeries), autonomous vehicle traffic management, and most prominently, the industrial Internet.[120] Consider an industrial automation scenario where machinery is remotely monitored and controlled in real time through Internet-connected sensor and actuator devices, a use case that routinely appears in New IP documents.[121] Here, the consequences of packet loss or severe latency could be costly, leading to disruptions in the manufacturing process, product defects, or damage to machinery. Hence, one of the proposed requirements for New IP is the ability to achieve deterministic QoS—end-to-end transmission of data flows with guaranteed maximum/minimum levels of reliability, latency, and/or jitter—over large-scale networks.[122]

Huawei is far from the first one to take an interest in these capabilities, as efforts to enable differentiated QoS in packet switched networks have been taking place for well over three decades. The IETF has undertaken two major initiatives aimed at defining new QoS models as alternatives to best effort

---

118. LARRY L. PETERSON & BRUCE S. DAVIE, COMPUTER NETWORKS: A SYSTEMS APPROACH 492-94 (5th ed. 2012) (providing an overview of the first-in, first-out queuing associated with best effort delivery).

119. Richard Li et al., *New IP: A Data Packet Framework to Evolve the Internet*, PROC. 2020 IEEE 21ST INT'L CONF. ON HIGH PERFORMANCE SWITCHING & ROUTING (HSPR) 3 (2020), https://doi.org/10.1109/HPSR48589.2020.9098996 [https://perma.cc/DY8F-5NYL] [hereinafter Li et al., *New IP Data Packet Framework*].

120. *See, e.g.*, Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Tutorial on C83 - New IP: Shaping the Future Network*, TSAG-TD598/GEN, at 7 (Sept. 2019), https://www.itu.int/md/T17-TSAG-190923-TD-GEN-0598 [https://perma.cc/MBN8-YTVX] [hereinafter TSAG Tutorial].

121. *See, e.g.*, *id.* at 7; Richard Li, Chief Scientist, Huawei R&D, New IP and Market Opportunities, Keynote Address at the IEEE International Conference on High Performance Switching and Routing (HSPR) 8 (May 12, 2020), https://hpsr2020.ieee-hpsr.org/wp-content/uploads/sites/118/2020/05/Richard-HPSR-2020-v1.0.pdf [https://perma.cc/LR3Z-GPCZ] [hereinafter Li, *Market Opportunities*].

122. This "large-scale networks" part is important because it is how Huawei distinguishes what it is proposes from similar ongoing work at other SDOs, such as the IEEE's Time Sensitive Networking and IETF's Deterministic Networking working groups. *See* Richard Li, *Some Notes on "An Analysis of the "New IP" Proposal to the ITU-T,"* INTERNET EVOLUTION (June 2, 2020), https://internet4future.wordpress.com/; Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Proposal of text amendments to the Terms of Reference of the proposed new Question F (Q.F) for the next study period of SG13*, SG13-C994, at 2 (July 7, 2020), https://www.itu.int/md/T17-SG13-C-0994 [https://perma.cc/9CL7-PEZC].

delivery. The first attempt came in the form of Integrated Services (*IntServ*), which was initiated in 1994.[123] *IntServ* enables users/applications to reserve the necessary resources (i.e., bandwidth) from each router along a network path in order guarantee that subsequent packets in a flow receive a particular level of service. *IntServ* was followed by Differentiated Services (*DiffServ*), first proposed in 1998.[124] *DiffServ* involves categorizing network traffic into different pre-defined classes which can be specified in an IP packet header field. A *DiffServ*-enabled router uses this information to determine how to prioritize traffic (something called a per-hop-behavior or PHB), giving preferential treatment to high-priority classes while giving lower-priority classes traditional best effort service.

As suggested by the fact that this QoS discussion is still occurring several decades later, neither of the solutions above have succeeded in gaining significant traction, at least on an Internet-wide scale.[125] Indeed, each of them has proven to face various technical limitations, many of which Huawei notes in its justification for New IP. *IntServ*, for instance, involves complex signaling between endpoints and routers, including the initial setup which itself can contribute to delay.[126] It also requires routers to store and continuously process information about each active flow it has reserved resources for, something that can add significant overhead in large networks and thus limiting its scalability. *DiffServ*, on the other hand, avoids most of these limitations but comes with a major downside in that it cannot provide strict end-to-end QoS guarantees.[127] It offers only to prioritize traffic based on broadly defined classes, which increases the probability that packet will arrive within a certain amount of time rather than provide deterministic guarantees, and the way both classification and prioritization are implemented in different networks often varies considerably.

Despite the aforementioned technical limitations, many maintain that economic and business-related obstacles have played a larger role in the failure of these solutions to achieve widespread implementation across the

123. *See generally* Robert Braden et al., *Integrated Services in the Internet Architecture: An Overview* (IETF Network Working Grp., RFC No. 1633, 1994), http://www.ietf.org/rfc/rfc1633.txt [https://perma.cc/K276-NAJG].

124. *See generally* Steven Blake et al., *An Architecture for Differentiated Services* (IETF Network Working Grp., RFC No. 2475, 1998), http://www.ietf.org/rfc/rfc2475.txt [https://perma.cc/M7NK-V377].

125. KC Claffy & David D. Clark, *Adding Enhanced Services to the Internet*, 6 J. INFO. POL'Y 206 (2016); Geoff Huston, *The elusive nature of QoS in the Internet*, APNIC (Sept. 30, 2021), https://blog.apnic.net/2021/09/30/the-elusive-nature-of-qos-in-the-internet/ [https://perma.cc/GP68-BMYN].

126. *See* PETERSON & DAVIE, *supra* note 118, at 548-49 (explaining the scalability issues of IntServ); Lijun Dong & Lin Han, *New IP Enabled In-Band Signaling for Accurate Latency Guarantee Service*, PROC. 2021 IEEE WIRELESS COMMC'N & NETWORKING CONF 1 (2021), https://doi.org/10.1109/WCNC49053.2021.9417598 [https://perma.cc/PMT3-AHYF] (identifying poor scalability, large overhead, and difficult implementation as main limitations of IntServ).

127. *See* Dong & Han, *supra* note 126, at 2 (citing the raw granularity of traffic class-based differentiation, which prevents precise end-to-end guarantees, as main limitation of *DiffServ*).

public Internet.[128] From this perspective, providing end-to-end QoS guarantees in a multi-operator network environment is more of a coordination problem than an engineering one. Although it is not uncommon for ISPs and large enterprises to use *DiffServ* for prioritizing certain types of traffic within the confines their own networks, end-to-end QoS on an inter-network level requires significant coordination between operators.[129] Negotiating service level agreements and pricing arrangements, already obstacles in their own right, can also entail providing other competing ISPs with greater visibility into one's internal network operations, creating further disincentives to such coordination.[130]

The New IP proposals, on the other hand, make it clear that Huawei sees this primarily as a technical problem rather than a coordination one. The general solution it outlines in various proposal documents and research papers revolves around the idea of altering the IP packet structure to include a "contract," which would be located between the header and payload.[131] The contract would be able to carry in-band signaling information for the setup of resource reservations along a network path as well as richer semantics (aka "contract clauses") for the specification of more granular QoS requirements and PHBs.[132] In simpler terms, Huawei believes the longstanding QoS problem can be overcome with a new model that combines *IntServ*'s fine-grained end-to-end guarantees but with *DiffServ*'s scalability and lack of complicated out-of-band signaling. Yet, none of what is contemplated here

---

128. *See* Claffy & Clark, *supra* note 125, at 227-32 (arguing economic obstacles to widespread QoS implementation have proven to be larger than the technical ones); Hascall Sharp & Olaf Kolkman, *An Analysis of the "New IP" Proposal to the ITU-T* 6-7 (Internet Soc'y, Discussion Paper, 2020), https://www.internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/ [https://perma.cc/KZ2W-D55B] (arguing business and regulatory problems involved in inter-domain deterministic networking will not be solved by a new protocol system).

129. Claffy & Clark, *supra* note 125, at 229 ("[T]he QoS technology developed by the IETF was in use in many IP-based enterprise networks, for example, corporate intranets"); Christopher S. Yoo, *Network Neutrality and the Need for a Technological Turn in Internet Scholarship*, *in* HANDBOOK OF MEDIA LAW AND POLICY: A SOCIO-LEGAL EXPLORATION 539, 543-44 (Monroe E. Price & Stefaan G. Verhulst eds., Routledge 2012) (explaining that operators like Comcast and AT&T use *DiffServ* to prioritize delay-sensitive traffic within their internal networks).

130. *See* Claffy & Clark, *supra* note 125, at 230-32.

131. *See* Richard Li, Chief Scientist, Huawei R&D, Network 2030 and New IP, Keynote Address at the 2019 15th International Conference on Network and Service Management (CNSM) 21 (Oct. 23, 2019), http://www.cnsm-conf.org/2019/files/slides-Richard.pdf [https://perma.cc/2PGE-8STF] [hereinafter Li, *Network 2030 and New IP*] (providing a high-level visual depiction of the New IP packet structure and describing the capabilities of its "contract spec").

132. Lijun Dong & Lin Han, *New IP Enabled In-Band Signaling for Accurate Latency Guarantee Service* (IEEE WCNC 2021), https://ieeexplore.ieee.org/document/9417598 [https://perma.cc/8LZY-M9VT] ("A contract clause describes how the routers treat the packet as it traverses the network based on the predefined triggering event and condition."); Lin Han et al., *A Framework for Bandwidth and Latency Guaranteed Service in New IP Network*, PROC. IEEE INFOCOM 2020 - IEEE CONF. ON COMPUT. COMMC'NS WORKSHOPS (INFOCOM WKSHPS) 85 (2020), https://ieeexplore.ieee.org/document/9162747 [https://perma.cc/3U43-7AP9].

would obviate the need for coordination between operators in order to enable these capabilities at the inter-network level. It is possible, perhaps even likely, that all this would do is equip networks with yet another set of tools for providing differentiated QoS that go largely unused in practice. Thus, despite taking aim at a legitimate problem the technical community has long struggled to solve, questions remain about the potential effectiveness of Huawei's general approach.

B. Intrinsic Security

The most controversial part of the New IP proposal relates to its so-called "intrinsic security" features. Were it not for this component, which included the now notorious "shut up command," it is possible Huawei's proposal receives little outside attention.[133] However, this part of New IP is also the most difficult to appraise, as unlike many of the other proposed features, intrinsic security cannot be traced back to a large body of research published by New IP contributors. It is also notably absent from several of Huawei's New IP presentations outside the ITU.[134] Fortunately, months after Huawei's original presentation to ITU-T, it followed up with a new contribution that provided a slightly more detailed look at New IP's "Intrinsic Security Framework."[135] Here, it claims that security was an oversight in the design of the TCP/IP Internet and that the subsequent patchwork of solutions are no substitute for an Internet architecture with security embedded into its design from the beginning.[136] Huawei identifies the Internet's primary security weakness as the inability to verify the authenticity of a packet's source. It argues that the ability to hide or misrepresent the origin of network traffic through methods like IP spoofing can be used to help carry out DDoS and Man-in-the-Middle attacks as well as to evade accountability for harm and illegal acts online.[137]

In response, proposal documents depict a high-level architecture for verifying source address authenticity and enabling "privacy-preserving" user accountability.[138] Routers within the originating network domain would check that the source identifier included in a packet's header is legitimate and then add a cryptographically verifiable authentication code, which routers in the destination domain would then use to determine the packet's authenticity and integrity.[139] Packets whose source cannot be authenticated are then filtered out by routers in the destination domain, frustrating one's ability to spoof an

133. *See supra* text accompanying note 3.

134. *See generally, e.g.*, Li, *Network 2030 and New IP*, *supra* note 131; Li, *Market Opportunities*, *supra* note 121 (containing no references to New IP's intrinsic security features).

135. Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Overview New IP Networking & Intrinsic Security Framework*, SG17-C788 (Mar. 3, 2020), https://www.itu.int/md/T17-SG17-C-0788 [https://perma.cc/7RQG-PJH9] [hereinafter SG17-C788].

136. *Id.* at 14.

137. *Id.* at 8.

138. *Id.* at 15.

139. *Id.* at 16.

IP address or other identifier. As an additional layer of protection against abnormally large volumes of authenticated traffic making it through the filters, the architecture specifies a feature whereby the destination domain could send a request to an "accountability agent" running in the source domain to cut off the responsible party.[140] This is the source of the widely-reported "shut up command" or "kill-switch," although the feature's purported justification is to prevent and mitigate DDoS attacks.[141] Finally, a separate encrypted value, partially derived from an alpha-numeric identifier tied to an Internet subscriber's real identity, would be included in the packet header and verified by internal routers before leaving the source domain.[142] This would theoretically enable the traceback of illegal or malicious traffic to a particular individual, although the assistance of the source network operator would be necessary in order to reveal the subscriber information linked to a given identifier.

The intrinsic security architecture shown in the proposal does raise legitimate concerns. The shutoff feature is ripe for abuse, as it is conceivable that spurious requests to silence a host on a different network are sent for purposes like censorship rather than terminating a DDoS attack.[143] The embedding of traceable identifiers into the packet header is also problematic, although the concerns raised here should be prefaced by reiterating that these identifiers would be encrypted using a symmetric key possessed only by the network operator. The ciphertext would also change on a per-flow basis to prevent third parties from being able to correlate all of an individual's network activities.[144] Regardless, the simple possibility of tracing traffic back to an individual person comes at the cost of reducing anonymity while likely having only limited effectiveness in deterring malicious actors.[145] This is because a large share of modern cyberattacks are carried out through compromised hosts (e.g., as part of a botnet), meaning the individuals to whom the attacks are directly traceable are not actually responsible.[146]

Simultaneously, there are doubts over just how "intrinsic" these security features are to New IP.[147] The architecture depicted in Huawei's proposal bears a close resemblance to a technology developed in China over a decade earlier called the Source Address Validation Architecture

140. *Id.* at 22-24.

141. SG17-C788, *supra* note 135, at 22-24.

142. *Id.* at 18-19.

143. The proposal documents do not indicate whether granting these shutoff requests would be left to the discretion the network operator or is instead carried out through some automated process.

144. *See* SG17-C788, *supra* note 135, at 18-19.

145. *See* David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SEC. J. 323, 325 (Mar. 16, 2011) (arguing that redesigning the Internet so that all actions can be attributed to an individual person would not help deter sophisticated cyberattacks, though it would raise issues related to privacy and freedom of expression).

146. *See id.* at 334-35 (explaining that many attacks are now multi-stage in nature, meaning the owner of a host to which an attack can be directly traced is not actually the attack's source, but instead a victim).

147. *See* Sharp & Kolkman, *supra* note 128, at 7.

(SAVA).[148] Designed around IPv6, SAVA is also capable of verifying the authenticity of the source IP address and filtering network packets at both the inter and intra-domain level.[149] An enhanced version of this architecture (called Source Address Validation Improvements or SAVI) was successfully implemented on CNGI-CERNET2, the IPv6-only backbone network constructed as part of the "China Next Generation Internet" initiative that began in 2003.[150] The proposed intrinsic security features thus appear to be largely independent of the underlying network architecture, as there is no obvious reason why most of these same capabilities could not be implemented on existing IPv6 networks.[151]

C. Flexible Addressing for the Connection of "ManyNets"

The simplest way to describe the Internet is as "a network of networks," a diverse collection of smaller independently operated networks called autonomous systems that are interconnected via a common protocol (IP) that was designed to prioritize universal connectivity. Yet, Huawei observes that the global network environment is becoming increasingly heterogenous as different network types emerge, such as those connecting new non-traditional devices and/or consisting of more dynamic topologies.[152] It characterizes this trend as a shift from "OneNet" to "ManyNets" and expects it to continue in the future as novel use cases with unique technical demands arise.[153]

Despite IP's emphasis on global connectivity, Huawei contends that the way devices are attached to and identified on the existing IP-based Internet

148. SAVA was developed by researchers from Tsinghua University as part of the state-funded "Research of Future Internet Architecture" project in the early 2000s. *See generally* Jianping Wu et al., *Theoretical Research Progress in New-Generation Internet Architecture*, SCI. CHINA SER. F-INF. SCI. 1634 (Oct. 2008), https://link.springer.com/article/10.1007/s11432-008-0160-8 [https://perma.cc/G68G-9LUY].

149. *See* Ying Liu et al., *Recent Progress in the Study of the Next Generation Internet in China*, 371 PHIL. TRANSACTIONS ROYAL SOC'Y A 20120387, at 13-16 (Mar. 28, 2013), https://doi.org/10.1098/rsta.2012.0387 [https://perma.cc/4K94-W52L].

150. *See* Jianping Wu et al., *CNGI-CERNET2: An IPv6 Deployment in China*, 41 ACM SIGCOMM COMPUT. COMMC'N REV. 48, 50 (2011) (detailing the implementation of SAVA/SAVI on CERNET2); The success of the SAVA/SAVI deployment was even touted in the seminal *Internet in China* whitepaper released by the State Council in 2010. *See Internet in China* whitepaper, *supra* note 114, § 1 (identifying "true IPv6 source address validation" as one of the technologies successfully implemented on "the world largest IPv6 demonstration network.").

151. Huawei researchers seemed to admit as much when they published a research paper months later containing an architecture nearly identical to the "Intrinsic Security Framework" but oriented around IPv6 instead of New IP. *See generally* Weiyu Jiang et al., *Security-Oriented Network Architecture*, SEC. & COMMC'N NETWORKS (May 27, 2021), https://doi.org/10.1155/2021/6694650 [https://perma.cc/8NUT-WJKN].

152. TSAG-C83, *supra* note 6, at 2.

153. Li et al., *New IP Data Packet Framework*, *supra* note 119, at 3 (explaining the phenomenon it refers to as ManyNets and arguing that today's public Internet will eventually be only one such Internet in this collection); Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Report of NSP e-meeting (23 June 2020)*, SG13-TD456/GEN (July 10, 2020), https://www.itu.int/md/T17-SG13-200720-TD-GEN-0456 [https://perma.cc/D2MF-SJJC] (clarifying that ManyNets is an ongoing phenomenon New IP is intended to address, not a goal or end state it is trying to achieve).

will no longer be sufficient to accommodate the "ManyNets" of the future.[154] It identifies two primary limitations. The first is the fixed-length of existing IP addresses, as Huawei holds that IPv6's one-size-fits-all 128-bit addresses create challenges for smaller, less expensive devices with limited memory and processing power.[155] It highlights industrial networks comprised of interconnected low-power devices—part of the Industrial IoT (IIoT)—as an emerging use case for which fixed 128-bit addresses unnecessarily contribute to increased packet overhead and reduced transmission efficiency.[156] The other limitation is that existing IP addresses were originally designed to identify physical devices attached to the network at a fixed location, an assumption that most routing protocols have been built around.[157] Huawei argues this precludes optimal routing in a growing number of scenarios where, for example, the intended destination is not a specific host device but rather a service, person, or piece of content.[158] It also emphasizes the challenges this presents for networks comprised of several moving parts, namely integrated ground/satellite networks.[159]

If these limitations are not addressed by a single holistic solution, Huawei claims that an inconsistent patchwork of solutions will emerge instead, some of which will bypass the Internet altogether.[160] This would push the global network environment further towards fragmentation and risk creating several non-interoperable communication "islands," an outcome Huawei believes should be avoided.[161] Hence, the motivating force behind New IP's changes to Internet addressing, at least on the proposal's face, is accommodating and maintaining interconnectivity among ManyNets by overcoming the aforementioned limitations of IP addressing.

One of the primary functional requirements for New IP would be to provide a common, universal address format capable of supporting variable-length addresses as well as multiple semantics. Whereas the former is fairly self-explanatory, support for multiple address semantics essentially means the

---

154. *See* TSAG-C83, *supra* note 6, (describing the current design of the Internet as "vastly insufficient"); Zhe Chen et al., *NEW IP Framework and Protocol for Future Applications*, PROC. IEEE/IFIP NETWORK OPERATIONS & MGMT. SYMP. 1 (2020), https://doi.org/10.1109/NOMS47738.2020.9110352 [https://perma.cc/PNT7-V7EP] [hereinafter Chen et al., *NEW IP Framework*] ("The current TCP/IP protocols and framework contain limitations for the ManyNets interconnectivity.").

155. Li, *Network 2030 and New IP*, *supra* note 131, at 25 (describing 128-bit addresses as "overkill" for low-power devices).

156. Chen et al., *NEW IP Framework*, *supra* note 154, at 1.

157. *Id.*

158. *Id.*

159. Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Proposal of text amendments to the Terms of Reference of the proposed new Question G (Q.G) for the next study period of SG13*, SG13-C995 (July 7, 2020), https://www.itu.int/md/T17-SG13-C-0995 [https://perma.cc/UDD8-86FP] ("Furthermore, most of the existing interconnection methods are essentially designed based on static physical network topologies. . . . The current addressing and routing schemes were not designed to support such network dynamicity.").

160. *See* TSAG-C83, *supra* note 6, at 2 (arguing that an increasing number of "unilateral and temporary technologies are being deployed" and that a "ubiquitous, universal and better protocolled system" is preferable).

161. *Id.*

ability for network devices to interpret an IP address as something other than a location on the network's topology. For instance, the address format may be defined such that those starting with a certain sequence of bits are interpreted as identifying a piece of content rather than a host.[162] Routers would then use the remaining bits in the address to make a forwarding decision based on the nearest instance of that content.[163] Similarly, a different leading sequence of bits may be designated to signify the address is instead carrying geographic location information, which may be used in Low Earth Orbit satellite networks to calculate the shortest path to a ground destination based on the relative positions of satellites at the time.[164]

Some New IP critics have raised concerns about the use of content or person-based identifiers in the address field.[165] They argue it would facilitate tracking and censorship by exposing information about the requested content or recipient in the packet header for intermediate network elements to see.[166] Yet, it is important to recognize that the proposal does not prescribe or endorse a particular address type, only a format flexible enough to accommodate the many possible address types that could emerge in the future.[167] While New IP could support content or identity-based addressing and forwarding schemes, they would still need to be separately developed and implemented. The extent to which these schemes would be averse to privacy or information freedom would be determined almost entirely by the choices made during the design and implementation processes.[168] Until this actually happens, it would be speculative to draw any conclusions about whether these features were intended to facilitate censorship or surveillance.

That said, this dimension of New IP still leaves some major questions unanswered. The most crucial such question pertains to its intended scope, as it is unclear whether New IP addressing was intended to be a general purpose solution, providing globally-routable and unique identifiers that would supplant IPv6, or if they are intended to have a more limited application to

---

162. *See* Chen et al., *NEW IP Framework*, *supra* note 154, at 2 (describing an address format that would encode information about the size, structure, and semantics into the beginning addresses first 8 bits).

163. *See* TSAG Tutorial, *supra* note 120, at 20.

164. *See id.* at 19 (depicting geography-based addressing and routing in ground-satellite networks); Li et al., *New IP Data Packet Framework*, *supra* note 119, at 8 (explaining the new address format accommodates "the need for geographic address structures for the networks involving satellites.").

165. *See, e.g.*, Taylor et al., *supra* note 14, at 196 (arguing the use of persistent object identifiers "would enable unparalleled tracing over the internet").

166. *Id.*

167. Sharp & Kolkman, *supra* note 128, at 4 ("[T]he New IP framework proposes a flexible length address space to subsume all the possible future types of addresses.").

168. There is nothing inherently privacy compromising about Information-Centric Networking (ICN). Consider, for example, Named Data Networking (NDN), a proposed ICN-based architecture initially developed through the NSF-funded Future Internet Architecture project. Largely due to its stateful forwarding plane, NDN enables content to be anonymously requested and retrieved over a network without any information about the requestor (e.g., a source address) being included in a packet. *See Named Data Networking: Motivation & Details*, NAMED DATA NETWORKING https://named-data.net/project/archoverview/ [https://perma.cc/L9MY-9LVX] (last visited July 7, 2023).

those environments where existing address limitations present issues. This question is of great significance, as if the answer is the former, it would seemingly introduce several new challenges from both a technical and governance perspective. For instance, who would be the entity responsible for managing the new global address space? How would they break up and allocate these addresses? Would requiring every router to support forwarding based on several different address semantics—greatly increasing the amount of routing information that would need to be exchanged and stored—have a detrimental impact on the complexity and scalability of the routing system?[169] Unless the benefits are overwhelming, issues like these, along with the arduous and costly transition process, would make it difficult to justify a new global addressing scheme.

Conversely, it is possible New IP's flexible addressing was not intended to replace IPv6 addresses but to instead serve as a complement whose use is limited to scenarios where conventional addressing is inadequate. Limiting it to smaller special-purpose networks (e.g., industrial, ground-satellite, etc.) would obviate the need for these addresses to be globally unique, although they would be routable only within the smaller network. In order to travel over the public Internet, a packet with a flexible address would either need to be translated into a unique IPv6 address or encapsulated into an IPv6 packet that is then sent over the public Internet and unwrapped when it reaches the destination network (a process called tunneling). Understood this way, New IP's flexible addressing features would function as a Swiss-army knife for connecting special purpose networks to the Internet, providing one standard mechanism for turning packets with heterogenous private addresses into globally routable ones. Although this would avoid many of the challenges associated with a new global addressing scheme, it is uncertain just how strong of a value proposition it offers.

The questions about New IP's intended scope turn out to be a major theme throughout Huawei's proposal. Earlier descriptions of New IP paint a far more ambitious picture and seem to operate on the assumption that the new protocol would indeed act as a successor to IP.[170] Yet, a notable shift in direction can be seen in later New IP materials. Several months after first introducing New IP, Huawei effectively rebranded its initiative within ITU-T with the title Future Vertical Communications Networks (FVCN).[171] While retaining nearly all of the original's proposed features, FVCN emphasized a

169. *See* TSAG Tutorial, *supra* note 120, at 20 (indicating New IP would be capable of direct routing based on diverse IDs through "maintaining diverse ID routing tables in the network").

170. This is on display from the very first substantive slide of Huawei's initial New IP presentation at the ITU-T. Here, it shows a graphic in which TCP/IP and several other non-IP network types all converge into one future network (New IP). *See* TSAG Tutorial, *supra* note 120, at 3.

171. *See generally* Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Encourage study on future network evolution supporting vertical applications including Future Vertical Communication Networks*, SG13-C1062 (July 10, 2020), https://www.itu.int/md/T17-SG13-C-1062/en [https://perma.cc/CH5B-BUCQ].

more limited application of the future protocols within the networks of certain industry verticals (e.g., manufacturing, energy, etc.) rather than globally.[172]

Even in discussions outside of the ITU, Huawei began to advertise a more complementary role for New IP, characterizing it as a fully TCP/IP-compatible solution for connecting industrial networks with unique requirements directly to the Internet.[173] Although none of this was ultimately enough to save New IP, there was still a noticeable pivot away from portraying it as a TCP/IP replacement. Of course, a more cynical interpretation of this pivot might simply dismiss it as a rhetorical strategy in response to the initial public blowback the proposal drew. Yet, it is also possible to see this as an act of pragmatism, whereby Huawei realized the proposal's most important goals could be achieved through less radical changes. This narrowed focus on industrial use cases should thus be kept in mind when debating the underlying motives of New IP, as it arguably provides another hint about what the proposal was really out to accomplish.

IV. CONFRONTING THE "TROJAN HORSE" NARRATIVE

A more robust understanding of the New IP proposal better positions us to address one of this Article's animating questions: Are China's efforts to enhance its position within the international standard-setting landscape really just a trojan horse, a hidden strategy for giving the global Internet's architecture and governance arrangements an authoritarian overhaul? This is indeed the way it has been framed by many predominantly Western actors, and the New IP initiative—having become largely understood as a calculated attempt to expand state control over the Internet—is regularly cited as validation.[174] However, we argue this type of framing provides, at best, a reductive understanding China's Internet standard-setting ambitions, inflating many of the interests involved while neglecting others. This Part addresses

---

172. Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Supporting contribution to the two contributions submitted into the July 2020 SG13 meeting which propose text amendments to the Terms of Reference of, respectively, draft Questions F and G of SG13 (Q.F/13 and Q.G/13) for the next study period of SG13*, SG13-C996 (July 7, 2020) , at 2-5, https://www.itu.int/md/T17-SG13-C-0996 [https://perma.cc/C3J7-AFAV] (clarifying that FVCN protocols "are not meant to replace the existing Internet protocols," but instead to complement them in "business-critical industrial" use cases.).

173. In response to the initial wave of criticism, Dr. Richard Li, chief scientist at Huawei's U.S.-based research arm and one of the central most figures behind New IP, setup a website where he re-iterated this more limited role. Richard Li, *Some Notes on "An Analysis of the "New IP" Proposal to the ITU-T,"* INTERNET EVOLUTION (June 2, 2020), https://internet4future.wordpress.com/ [https://perma.cc/AF4K-SXFE] ("New IP complements IP and is intended to connect to the Internet the networks and their terminals that have not been connected to the Internet for certain types of business-critical industrial use.").

174. *See, e.g.*, Taylor et al., *supra* note 14, at 186 ("China's New IP has an authoritarian flavor. It is designed to capture large amounts of data and enable centralized controls that could be harnessed for government surveillance."); *Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet*, FREEDOM HOUSE (2022), at 16, https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf [https://perma.cc/MKD7-BYRU] (describing New IP as a plan to redesign common protocols to "facilitate greater state control over domestic networks").

two major problems with the trojan horse narrative. The first concerns limitations within ITU-T to the state-centric approach to global standard-setting that China purportedly favors, while the second involves flawed assumptions about the "regulability" of the existing TCP/IP Internet. We find that both issues become particularly glaring when the narrative framework is superimposed onto the case of New IP.

A. The Limits of the ITU-T and Multilateral Approaches to Standard Setting

According to the conventional account, one of the primary goals in China's pursuit of greater influence over the standard-setting process is to reshape the institutional landscape, moving functions away from open, privatized, multistakeholder bodies in favor of those that provide a stronger voice to governments.[175] This type of multilateral approach to standard-setting would be consistent with China's endorsement of cyber sovereignty as an alternative normative foundation for global Internet governance. It has also been suggested that China finds a "one country, one vote" system attractive because it could court like-minded countries to help push through controversial standards that would otherwise fail in an open, consensus-based model.[176]

In terms of a venue, the prevailing assumption has been that China sees ITU-T as an ideal fit. Indeed, China has been quite explicit in its support for expanding the ITU's role within the broader Internet governance system, which can be interpreted as including the development of technical standards.[177] It was thus seen as little coincidence that Huawei brought the New IP proposal to ITU-T instead of a body like the IETF.[178]

On the surface, this part of the trojan horse narrative appears perfectly reasonable. Yet, in reality, shifting Internet standard setting away from a

---

175. *See, e.g.*, USCC 2022 Report, *supra* note 10, at 459-60; Shane Tews, *China's Tech Ambitions Threaten to Fundamentally Change How the Internet Functions*, AM. ENTER. INST. (July 7, 2020), https://www.aei.org/technology-and-innovation/chinas-tech-ambitions-threaten-to-fundamentally-change-how-the-internet-functions/ [https://perma.cc/M384-74G9] (claiming China seeks to "destabilize" existing governance arrangements in favor of a centralized top-down model).

176. *See* Mark Montgomery & Theo Lebryk, *China's Dystopian "New IP" Plan Shows Need for Renewed US Commitment to Internet Governance*, JUST SEC. (Apr. 13, 2021), https://www.justsecurity.org/75741/chinas-dystopian-new-ip-plan-shows-need-for-renewed-us-commitment-to-internet-governance/ [https://perma.cc/WRM2-R9FN]; Russel & Berger, *supra* note 61, at 23-24; Hoffman et al., *supra* note 13, at 253.

177. *See supra* note 51.

178. *See, e.g.*, *The Open Internet on the Brink: A Model to Save Its Future*, TONY BLAIR INST. FOR GLOB. CHANGE (Sept. 30, 2021), at 24, https://institute.global/policy/open-internet-brink-model-save-its-future [https://perma.cc/W8WK-F59R] ("China's proposal provides the opportunity for national governments, which support more tightly censored and regulated models of the internet, to have greater power in shaping its future."); Marco Hogewoning, *Do We Need a New IP?*, RIPE.NET (Apr. 22, 2020), https://labs.ripe.net/author/marco_hogewoning/do-we-need-a-new-ip/ [https://perma.cc/M4P5-ANZF] (arguing New IP is being leveraged as an opportunity to redesign internet governance to have a more "top-down structure").

multistakeholder model towards a more multilateral approach would provide China with much more limited ability to achieve many of the goals attributed to it than is generally realized and thus lacks much of the appeal suggested by most observers. Venues like ITU-T are not a panacea that allow authoritarian-leaning countries magically to overcome Western opposition to controversial proposed standards and ensure their global adoption. Moreover, as China's national champions in the ICT sector grow stronger, moving away from an industry-led standards development model may actually work to its detriment.

1. Adherence to Consensus-Based Decision-Making

First, consider China's purported venue of choice, ITU-T. Despite the numerous differences between ITU-T and bodies like the IETF, the former still largely adheres to consensus-based decision making. Its procedures are not, at least on paper, substantially different from the "rough consensus" of the IETF.[179] During a study period, there are two separate tracks that a Recommendation can travel through to gain approval for final publication.[180] In both such tracks, opposition from a single member state delegation is sufficient to stop a draft from proceeding.[181] The Alternative Approval Process, which despite its name is the track selected for an overwhelming majority of Recommendations, even permits a lone non-state sector member to prevent the requisite "unopposed agreement" from being reached at the final stage.[182]

Concededly, this consensus requirement does not *always* prevent the approval of Recommendations one would ordinarily expect to be met with contention. In recent years, certain ITU-T Study Groups have slowly morphed into de facto East Asia regional standards bodies, as a majority of the contributions here now originate from China, South Korea, and/or Japan.[183] Although Western participants still maintain a modest level of engagement at

179. *See* Bradner, *supra* note 31, § 3.3 (stating working groups make decisions through "rough consensus," some level of agreement between a simple majority and unanimity that satisfies the judgement of the group's chair); *see also* Voo & Creemers, *supra* note 61, at 11 (noting ITU Study Groups also require approval by consensus similar to many other SDOs).

180. *See generally* World Telecomm. Standardization Assembly, *Resolution 1 - Rules of procedure of the ITU Telecommunication Standardization Sector* § 8 (Rev. 2022), https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.1-2022-PDF-E.pdf [https://perma.cc/WVH3-MM3T] [hereinafter WTSA Res. 1]; Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Recommendation A.8 - Alternative approval process for new and revised ITU-T Recommendations* (Rev. 2022), https://www.itu.int/rec/T-REC-A.8-202203-I/en [https://perma.cc/UM36-EMY6] [hereinafter ITU-T Rec. A.8].

181. *See* WTSA Res. 1, *supra* note 180, § 9.5.3 ("[D]ecision of the delegations . . . to approve the Recommendation under this approval procedure must be unopposed").

182. *See* ITU-T Rec. A.8, *supra* note 180, §§ 4.3, 5.3; however, opposition from a lone Sector Member during the final stage may effectively be overridden if there have been repeated attempts to reach unopposed agreement and no more than one Member State present is in opposition. *See id.* § 5.4.

183. *See* Teleanu, *supra* note 61, at 58. This trend of East Asian dominance can also be observed extending to Study Group leadership positions. *See id.* at 36-37 (identifying China, Korea, and Japan as the top three countries in terms of ITU-T Study Group Working Party Chair and Vice-Chair positions during the 2017-2020 study period).

the ITU-T, they—non-state members in particular—tend to devote far more of their attention and resources towards the industry-driven venues that have historically played a greater role in modern ICT standards development (e.g., the 3GPP, IETF, or ETSI). Unfortunately, modest engagement at the ITU-T is not always enough to keep up with the large volume of proposed Recommendations coming out of Asia, opening the door for standards that might otherwise attract opposition from Western actors to gain ITU-T approval simply by flying under the radar.[184]Having said that, an undertaking as ambitious as redesigning the Internet's architecture is not the type that could conceivably go unnoticed by casual ITU-T participants. Individual Study Groups are only able to engage in standardization activities that fall within the scope of the work program they were explicitly authorized to perform by the ITU-T's full governing body, the World Telecommunication Standardization Assembly (WTSA). Before a major new standardization initiative could proceed, it would require WTSA to approve several different proposed work items known in ITU-T parlance as "study questions." However, the process through which Study Groups prepare new questions to submit for WTSA's approval is a highly contentious one that commands a lot of attention from participants.[185] In fact, the development of new study questions, a process that is also subject to consensus-based decision making, was precisely where the New IP initiative stalled.[186] This, in essence, shows how countries like China are still fairly constrained in their ability to leverage U.N.-style voting-bloc politics as a means of forcing radical technical agendas through the ITU-T. Nor is this a limitation that can be changed without consequence. To understand why, one must turn to the law of international

184. It should also be noted that there are limited circumstances in which a draft Recommendation that failed to gain consensus in a Study Group may be deferred to WTSA where it is possible to be adopted through a simple majority vote of Member States. *See* WTSA Res. 1, *supra* note 180, § 9.2.2. However, these circumstances are rare, and to the extent they do occur, almost always involve Recommendations related to economic and policy matters instead of technical ones. At the previous two WTSAs, the only draft Recommendations submitted for consideration were all Series D, which are related to accounting matters, tariffs, and other policy issues. *See* Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], PROC. WORLD TELECOMM. STANDARDIZATION ASSEMBLY V-5 (2016), https://www.itu.int/pub/T-REG-LIV.1-2016/en [https://perma.cc/277F-J9EF].

185. Series of special planning meetings, wherein participants debate the proposed agenda for an upcoming study period, often begin as far out as two years in advance of the next WTSA (which itself is held every four years). *See generally, e.g.*, Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Ad-hoc group on next study period (NSP) preparation for WTSA-24*, SG13-TD62-R1/PLEN (Nov. 14, 2022), https://www.itu.int/md/T22-SG13-221114-TD-PLEN-0062/en.https://www.itu.int/md/T17-SG13-R-0040 [https://perma.cc/E95J-UATN].

186. *See* Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Report of the ITU-T Study Group 13 Meeting*, SG13-R40, at 4 (Dec. 17, 2020), https://www.itu.int/md/T17-SG13-R-0040 [https://perma.cc/6LAM-2WWB] [hereinafter SG13 December 2020 Meeting Report] (recording that Huawei's proposed study questions were not approved due to a "significant number of objections").

trade, or more specifically, the World Trade Organization's Agreement on Technical Barriers to Trade (TBT).[187]

A component of the overall WTO agreement, and thus binding on all WTO Members, the TBT agreement's primary goal is to ensure that standards and standards-based technical regulations do not create unnecessary obstacles to international trade.[188] It requires that Members, to the extent they mandate adherence to a standard through national regulation, base such regulations on "relevant international standards."[189] This provision is intended to prevent countries from using technical regulations to serve protectionist ends, favoring domestic firms by conditioning the market access of their foreign competitors on adherence to unique national standards.[190]

The reason the TBT regime is germane to the ITU and its internal decision-making procedures involves the "relevant international standards" language mentioned above.[191] The ITU is generally considered one of the few recognized "international standardizing bodies" capable of producing standards that meet this definition, which in turn, gives them a (rebuttable) presumption of compliance with the TBT agreement when used as the basis for national technical regulations.[192] Some have hypothesized this special status is part of what China finds attractive about ITU-T as the venue is uniquely positioned to legitimize standards and give them a pre-emptive effect over inconsistent national technical regulations enacted by WTO members.[193]

However, there is an important caveat here. The WTO's Appellate Body has indicated this status is contingent on a standards body's adherence to a number of procedural principles that are outlined in a Decision from the WTO's TBT Committee.[194] Along with familiar principles like transparency

---

187. *See generally* Agreement on Technical Barriers to Trade, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, annex lA, 1868 U.N.T.S. 120 [hereinafter TBT Agreement].

188. DENARDIS, GLOBAL WAR, *supra* note 21, at 83.

189. TBT Agreement, *supra* note 187, art. 2.4.

190. Olia Kanevskaia, *Governance of ICT Standardization: Due Process in Technocratic Decision-Making*, 45 N.C. J. INT'L L. 549, 573 (2020); Panagiotis Delimatsis, *Global Standard-Setting 2.0: How the WTO Spotlights ISO and Impacts the Transnational Standard-Setting Process*, 28 DUKE J. COMP. & INT'L L. 273, 278 (2018).

191. TBT Agreement, *supra* note 187, annex 1.2 (defining "standards" to mean those approved by a "recognized body").

192. *See id.* at 299; Kanevskaia, *supra* note 190, at 605; *see also* TBT Agreement, *supra* note 187, art. 2.5 (stating that technical regulations serving a legitimate objective and that are consistent with relevant international standards are "rebuttably presumed not to create an unnecessary obstacle to international trade").

193. *See, e.g.*, Taylor et al., *supra* note 14, at 188-89; Hoffman et al., *supra* note 13, at 246.

194. Appellate Body Report, *United States - Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products*, ¶ 379, WTO Doc. WT/DS381/AB/R (adopted June 13, 2012) ("[T]he TBT Committee Decision, reflect the intent of WTO Members to ensure that the development of international standards take place transparently and with wide participation. . . . In analyzing whether an entity is an 'international standardizing body,' a panel needs to balance these considerations."); *see also* Delimatsis, *supra* note 190, at 281-84 (explaining how "recognized international body" has come to be interpreted under WTO case law).

and openness to participation, this Decision states that bodies preparing international standards should ensure that "impartiality and consensus" are observed.[195] More specifically, it directs them to establish consensus procedures that "take into account the views of all parties concerned and to reconcile any conflicting arguments."[196] Moving away from consensus-based decision-making—a widely-accepted best practice for standards development—would thus not only damage ITU-T's legitimacy; it would threaten one of the venue's few remaining value propositions by seriously jeopardizing its status as a recognized international standardizing body under the TBT.

2. The Need for Voluntary Adoption

Even if one were to disregard the obstacles presented by consensus-based standards development, any efforts by China to push a controversial new protocol suite through a venue like ITU-T would still face several challenges. The largest such challenge would be getting the manufacturers and operators of Internet infrastructure around the world, most of whom are private actors, to adopt and implement these new standards. The successful standardization of an alternative Internet architecture, even by a multilateral body, far from guarantees its adoption in the real-world. ITU-T knows this all too well, having been behind not one but two unsuccessful attempts in its history.

The first came in the mid-1970s when ITU-T (then known as the CCITT) developed a standard for data networking called X.25.[197] Since ITU-T was dominated by state-owned telephone monopolies at the time, X.25's highly network-centric and connection-oriented design was naturally modeled after the way circuit-switched telephone networks operated. However, as Internet historian Janet Abbate writes, "the 'telephone model' of computer networking did not fit well with the way computer users actually wanted to use networks."[198] The second attempt took place during the so-called "Internet standards wars" of the late 1980s and early 1990s when ITU-T, in collaboration with the International Organization for Standardization, championed the Open Systems Interconnection (OSI) protocol suite.[199] However, OSI's overall architecture proved far more complex than was practical, and its development was prolonged by slow bureaucratic processes that allowed the competing TCP/IP suite enough time to firmly establish itself.[200]

---

195. Comm. on Tech. Barriers to Trade, *Second Triennial Review of the Operation and Implementation of the Agreement on Technical Barriers to Trade*, WTO Doc. G/TBT/9 annex 4, 24-26 (Nov. 13, 2000).

196. *Id.*

197. *See* ABBATE, *supra* note 81, at 154.

198. *Id.* at 152.

199. *See* Andrew L. Russell, *The Internet that Wasn't*, 50 IEEE SPECTRUM 39, 40-42 (Aug. 2013) (providing a history of the Open Systems Interconnection standards).

200. *See* ANDREW S. TANENBAUM, COMPUTER NETWORKS 51-53 (5th ed. 2010) (examining several of the reasons OSI failed).

Although X.25 and the OSI protocols each saw periods of modest adoption, most of that coming outside of the United States, TCP/IP ultimately prevailed.[201] A significant reason these alternative protocol suites were unsuccessful is that they failed to account for the type of network capabilities for which there was legitimate demand at the time and that had been proven to work in practice.[202] This an inherent limitation of developing Internet standards through a top-down, anticipatory approach instead of in a more responsive, bottom-up fashion (*à la* the IETF).[203] Absent a government mandate, the choice to adopt a particular standard will be left up to market actors to decide based on a variety of technical, economic, and political considerations. If an alternative set of core protocols developed by ITU-T or any other multilateral venue is to avoid the same fate as X.25 and OSI, it will need to justify itself to these market actors. History has shown this to be no easy task.

The aforementioned limitations of multilateral Internet standard-setting do not necessarily mean China has no reason to favor this approach over the existing multistakeholder model. Despite having of a fair degree of political control over Chinese firms and thus being able to shape their engagement at multistakeholder SDOs, agency problems still exist. These could effectively be eliminated through a system in which States are involved more directly in the standard-setting process. Given its public support for expanding the ITU's role within the Internet governance ecosystem, China obviously sees *some* benefit in trying to shift functions to Geneva. At the same time, it is important that we focus on China's actions just as much as we focus on its rhetoric. These actions reveal a growing acceptance of the current institutional arrangements for standards development. As explained in Part I, China has been heavily promoting the engagement of domestic firms in the existing industry-driven ICT standards environment. Although it has yet to surpass the United States, the results thus far are fairly promising. As the influence of Chinese actors in this domain continues to grow, China's support for a "one country, one vote" style of multilateralism may become[204] even more difficult to justify.

B. How China Made Its Internet Regulable

The second component of the trojan horse narrative posits that China's standard-setting agenda is motivated by a desire to reinvent the Internet's technical architecture in its own image. Not only might this result in an

201. *See* ABBATE, *supra* note 81, at 167, 176 (summarizing the fates of X.25 and OSI protocols).

202. *See* Russell, *supra* note 199, at 43 (acknowledging that, while OSI's reputation as a total failure is not entirely fair, it is frequently portrayed as a cautionary tale of overly bureaucratic "anticipatory standardization.").

203. *See* Benoliel, *supra* note 17, at 1094-95 (explaining that the limitations of anticipatory standardization are why it eventually gave way to participatory approaches which directly involve stakeholders through a more iterative process).

204. *See* Erie & Streinz, *supra* note 71, at 55 (acknowledging that agency issues even exist between the government and state-owned enterprises).

Internet architecture that streamlines China's ability to censor and surveil its citizens, but fears exist that this architecture would export embedded authoritarian values around the globe in service of legitimizing alternative norms like cyber sovereignty.[205]

The concerns surrounding China's purported interest in radically reshaping core Internet protocols appear consistent with one of early cyberlaw's most influential insights: the capacity of the Internet's technical architecture to regulate user behavior.[206] Scholars such as Lawrence Lessig even predicted that governments of the future would increasingly attempt to alter the Internet's architecture, either directly or indirectly, seeking to transform it from a freedom-enabling un-regulable space towards one that can be easily and effectively controlled.[207] Yet, the proposition that fundamental changes to core protocols are either a necessary or especially compelling means of enabling such control contains shades of Internet exceptionalism, a once common view of the Internet as unique in its transcendence of territorial jurisdiction and thus resistant to traditional forms of regulation.[208] Needless to say, history has not been kind to this perspective which, if not already dead, is still on life-support.[209]

Perhaps no single actor contributed more to the shattering of this exceptionalist paradigm than China, the country that demonstrated that it was indeed possible to "nail[] Jell-O to the wall"—to borrow once again President Clinton's famous metaphor.[210] Many are already familiar with the so-called

---

205. These fears are not unique to the standard-setting context but have accompanied China's general rise as technological power. For example, a 2020 document released by the Trump Whitehouse on its China strategy charged the CPC with attempting to spread its ideology beyond China's borders by actively exporting the tools of its "techno-authoritarian model" around the world. DEP'T OF DEF., EXEC. OFF. OF THE PRESIDENT, UNITED STATES STRATEGIC APPROACH TO THE PEOPLE'S REPUBLIC OF CHINA 5 (2020).

206. *See supra* note 88 and accompanying text.

207. *See* Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net*, 14 BERKELEY TECH. L.J. 759, 763 (1999). It should be noted here that in using the term "architecture," Lessig explicitly clarified he was not necessarily speaking about core protocols but was referring broadly to the design of all the various hardware and software components that makeup cyberspace. LESSIG, CODE 2.0, *supra* note 81, at 62, 72.

208. The most famous enunciation of this exceptionalist position (or at least its descriptive variety) came from EFF co-founder John Perry Barlow, who boldly pronounced that world governments "have no sovereignty" in this newly formed cyberspace and that the legal concepts which govern the physical world do not apply. *See generally* John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence [https://perma.cc/5UVT-SCSM]. However, that Barlow's *Declaration* has become a punching bag for those taking jabs at the naivete of early techno-libertarianism is rather unfair. It was a piece of lyrical prose meant to capture the promethean optimism that surrounded the early Internet, not a nuanced argument about the possibility of public legal order in cyberspace. For a highly-cited attempt at the latter, *see generally* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

209. *See generally* Tim Wu, *Is Internet Exceptionalism Dead?*, *in* THE NEXT DIGITAL DECADE: ESSAYS ON THE FUTURE OF THE INTERNET 179 (Berin Szoka & Adam Marcus eds., 2010).

210. *See supra* note 16 and accompanying text.

Great Firewall surrounding China, the "semipermeable membrane that lets in what the government wants and blocks what it doesn't," but this only begins to scratch the surface.[211] China has built the world's most sophisticated Internet control regime, comprised of complementary legal and technical architectures whose effects extend from the network's physical infrastructure to the content/applications running on top of it. Most of what critics fear that authoritarian-aligned protocols would enable is not only possible with the existing TCP/IP Internet; it is already being done in China.

1. Licensing

First, the Chinese party-state exercises strict control over who can provide Internet-related services within its borders. At the infrastructure level, an entity seeking to provide Internet access or transit services must first obtain the appropriate state-issued operating license.[212] Eligibility for an operating permit is contingent on conforming to certain ownership restrictions: foreign equity in last-mile ISPs and backbone network operators must be no greater than fifty percent and forty-nine percent, respectively, with the latter being at least fifty-one percent state owned.[213] Although the regulations as written appear to permit some degree of foreign ownership, this is not the case in practice as very few foreign invested entities have been successful in obtaining requisite licenses.[214]

None of what China does here is revolutionary. Many other countries limit foreign access to their domestic telecommunications markets, and even more of them impose similar licensing requirements, especially those applicable to the provision of wireless access services as these can be found in virtually every country. However, part of what distinguishes China from the rest is that it extends its licensing regime to the application/content level. Entities seeking to provide commercial information services over the Internet,

---

211. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 92 (2006).

212. Zhonghua Renmin Gongheguo Dianxin Tiaoli (中华人民共和国电信条例) [Telecommunication Regulation of the People's Republic of China] (promulgated by State Council Sept. 25, 2000, effective Sept. 25, 2000, amended Feb. 6, 2016), art. 7, CLI.2.267182 (EN) (PKULaw) [hereinafter Telecommunication Regulation] (establishing licensing requirements for the provision of various telecommunications services). Under China's telecommunications regulatory framework, Internet access services are classified as value-added telecom services, whereas Internet transmission (i.e., backbone) services are categorized as basic telecom services. This classification is what determines the applicable foreign-ownership restrictions. *Id.* Appendix - Catalogue of Telecommunications Business.

213. *See id.* art. 10; *see also* Waishang Touzi Dianxin Qiye Guanli Guiding (外商投资电信企业管理规定) [Provisions on the Administration of Foreign-funded Telecommunications Enterprises] (promulgated by State Council Jan. 1, 2001, effective Jan. 1, 2002, amended May 1, 2022), art. 6, LEXIS CHINA ONLINE, htttp://www.lexiscn.com.

214. STAFF OF PERMANENT SUBCOMM. ON INVESTIGATIONS, S. COMM. ON HOMELAND SEC. & GOVT'L AFFS., 116TH CONG., THREATS TO U.S. NETWORKS: OVERSIGHT OF CHINESE GOVERNMENT-OWNED CARRIERS 19 (2020) (noting that no foreign entity has ever been successful in meeting the requirements for offering basic telecom services, while only a few dozen have successfully secured value-added licenses.).

such as operators of a website or mobile application, must first obtain an Information Content Provider (ICP) license.[215] Further requirements exist for special types of information services, such as those that distribute news or audiovisual content.[216] In both the case of ICPs and ISPs, those operating without a licenses face the risk of receiving large fines as well as closure/termination of their services.[217] In requiring prior authorization to operate such services, placing limitations on foreign and private ownership, and imposing the threat of license revocation for non-compliance with accompanying regulatory obligations, the party-state puts itself in a much stronger position to control domestic Internet activity both directly and indirectly.[218]

2. State Controlled Chokepoints

Second, from the early stages of China's connection to the global Internet, it began taking measures to limit the channels over which information was allowed to flow in and out of its territorial borders. In 1996, the State Council issued a set of administrative regulations mandating that "interconnecting networks," those directly connecting to networks outside China, achieve this interconnection though international Internet gateways designated and supervised by the Ministry of Posts and Telecommunications, a predecessor to what is now the Ministry of Industry and Information Technology (MIIT).[219] Entities are prohibited from connecting internationally through any channels—physical or virtual (i.e., VPNs)—outside of the approved gateways.[220] Moreover, the day-to-day operation of these gateways

---

215. Hulianwang Xinxi Fuwu Guanli Banfa (互联网信息服务管理办法) [Measures for the Administration of Internet Information Services] (promulgated by the State Council, Sept. 25, 2000, effective Sept. 25, 2000, amended Jan. 8, 2011), art. 4, CLI.2.174868 (EN) (PKULaw) [hereinafter Internet Information Service Measures]. Commercial Internet information services are considered value-added telecommunication services, meaning they must comply with foreign-ownership restrictions to obtain a license. *See supra* notes 212-13 and accompanying text. Non-commercial Internet information services—those that operate without compensation and are purely informational—must only submit an ICP filing also known as a "bei'an" (备案). *See id.* at art. 7, 8.

216. Rogier Creemers, *The Privilege of Speech and New Media: Conceptualizing China's Communications Law in the Internet Era*, *in* THE INTERNET, SOCIAL MEDIA AND A CHANGING CHINA 92-93 (Jacques deLisle et al. eds., 2016).

217. *See* Internet Information Service Measures, *supra* note 215, arts. 19-23.

218. *See* Henry Gao, *Data Regulation with Chinese Characteristics*, *in* BIG DATA AND TRADE 245, 258 (Mira Burri ed., 2021) (stating that the threat of having a license revoked or website shut down is what gives the regulations "real teeth").

219. *See* Zixiang Alex Tan et al., *China's New Internet Regulations: Two Steps Forward, One Step Back*, COMMC'N ACM, Dec. 1997, at 11 (analyzing the State Council's [then] newly issued *Interim Regulations on International Interconnection of Computer Information Networks*).

220. Gao, *Data Regulation with Chinese Characteristics*, *supra* note 218, at 248.

must be carried out by state-owned entities that are subject to the supervision, inspection, and guidance of MIIT.[221]

Funneling all internationally inbound and outbound traffic through a small number of state-managed Internet "chokepoints," makes information flows much easier to control than in a flatter, more decentralized network topology.[222] Under this architecture, one can no longer simply "route around" the censorship, as digital pioneer John Gilmore once famously said the TCP/IP Internet permits by default.[223] This is thus one of the biggest reasons why China's Great Firewall is even remotely effective.[224]

Much of what is publicly known about the Great Firewall and how it operates is the result of black box testing conducted by outside Great Firewall. Though we will not expound much on this here, the Great Firewall is believed to employ a variety of techniques, including simple IP address-based blocking, DNS manipulation, and URL/keyword filtering using Deep Packet

---

221. Guoji Tongxin Churukou Ju Guanli Banfa (国际通信出入口局管理办法) [Measures on the Administration of International Communication Accesses] (promulgated by Ministry of Info. Indus. Mar. 14, 2002, effective Oct. 1, 2002) Art. 7, CLI.4.40342 (EN) (PKULaw).

222. This is consistent with the empirical findings of researchers over the years who have attempted to map the topology of China's Internet, observing that traced inbound traffic traveled through just a small number of ASes belonging to state-owned backbone operators like China Telecom and China Unicom, or one of non-commercial networks like CERNET. *See, e.g.*, Hal Roberts et al., *Mapping Local Internet Control* (Oct. 2011) (paper presented at the 25th IEEE Annual Computer Communications Workshop (CCW)), https://cyber.harvard.edu/netmaps/mlic_20110513.pdf [https://perma.cc/9D2G-HDAG]; Guangchao Charles Feng & Steve Zhongshi Guo, *Tracing the Route of China's Internet Censorship: An Empirical Study*, 30 TELEMATICS & INFORMATICS 335 (2013), https://doi.org/10.1016/j.tele.2012.09.002 [https://perma.cc/8U4E-RJ7J].

223. Philip Elmer-Dewitt, *First Nation in Cyberspace*, TIME (Dec. 6, 1993), https://content.time.com/time/subscriber/article/0,33009,979768,00.html [https://perma.cc/HA3Z-KUA8] (quoting John Gilmore as saying "[t]he Net interprets censorship as damage and routes around it"). Although it may be difficult to route around these chokepoints, the emergence of Internet access technologies like low Earth orbit (LEO) satellite broadband could provide a means of going over the top of the Great Firewall. This is because LEO satellite constellations can deliver Internet connectivity directly to end-user terminals without needing to be relayed through an ISP-controlled ground station. Even though the leading provider of this service—SpaceX's Starlink—is not currently available in China (reportedly at the government's request), and China is currently constructing a large State-owned LEO constellation of its own, this technology still has the potential to present serious challenges to China's Internet control regime in the future. *See* Russel Brandom, *China asked Elon Musk not to sell Starlink within the country*, THE VERGE (Oct. 10, 2022), https://www.theverge.com/2022/10/10/23397301/elon-musk-starlink-china-great-firewall-censorship [https://perma.cc/6LMH-XJRA]; *see also* Cate Cadell, *China's military aims to launch 13,000 satellites to rival Elon Musk's Starlink*, WASH. POST (Apr. 6, 2023), https://www.washingtonpost.com/national-security/2023/04/06/elon-musk-china-starlink-pla/ [https://perma.cc/S73R-SYCD].

224. GOLDSMITH & WU, *supra* note 211, at 93.

Inspection (DPI).[225] Just as importantly, it has continued to evolve over time to keep pace with new circumvention techniques, as is demonstrated by its ability to block the use of privacy enhancing technologies such as the Tor network.[226] While far from perfect, it is effective enough against the average Chinese netizen to prevent the spread of unfavorable information from reaching the critical mass where it becomes a serious problem for the Party.[227]

3. Intermediary Liability and Self-Censorship

Third, while the Great Firewall is the primary means of controlling transnational Internet information flows, the approach for regulating domestic ones relies heavily on a form of intermediary liability in which censorship is effectively outsourced to ISPs and ICPs in exchange for their avoidance of license revocation, fines, and other administrative punishments.[228] There are several different sources of law in China that impose obligations on both ISPs and ICPs to record, report, and prevent users' dissemination of prohibited content through their services, either upon discovering it or being given notice.[229] Prohibited content in this context refers to a number of broadly defined categories that appear uniformly across major Internet laws and

---

225. *See* Daniel Anderson, *Splinternet Behind the Great Firewall of China*, ACM QUEUE , Nov. 2012, at 40-42 (describing the use of null routing or "blackholing," in which false routing information is advertised and propagated across border ASes so that routers drop traffic bound for blacklisted IP ranges instead of correctly forwarding it); Richard Clayton et al., *Ignoring the Great Firewall of China*, *in* PRIVACY ENHANCING TECHNOLOGIES 20 (George Danezis & Philippe Golle, eds., 2006) (explaining that the Great Firewall functions like an Intrusion Detection System, analyzing passing traffic out-of-band and, if found to violate policy, sending TCP resets to both endpoints to terminate sessions before data transfer can be completed); Graham Lowe et al., *The Great DNS Wall of China* (2007), https://censorbib.nymity.ch/pdf/Lowe2007a.pdf [https://perma.cc/PM72-VMWW] (demonstrating how the Great Firewall falsifies bad responses to DNS queries).

226. *See* Roya Ensafi et al., *Examining How the Great Firewall Discovers Hidden Circumvention Servers*, IMC'15: PROC. 2015 INTERNET MEASUREMENT CONF. 445, 446-47 (2015), https://dl.acm.org/doi/10.1145/2815675.2815690 [https://perma.cc/2G24-VBBL] (finding the Great Firewall uses "active probing" to discover and block hidden Tor bridges); *see also* Simon Sharwood, *China upgrades Great Firewall to defeat censor-beating TLS tools*, REGISTER (Oct. 6, 2022), https://www.theregister.com/2022/10/06/great_firewall_of_china_upgrades/ [https://perma.cc/8HTT-5WQS].

227. *See* Jyh-An Lee & Ching-Yi Liu, *Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China*, 13 MINN. J.L. SCI. & TECH. 125, 146-47 (2012).

228. *See, e.g.*, REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM 36 (2012) ("[D]omestic companies are the stewards and handmaidens, the tools and enforcers, of China's inner layer of Internet censorship.").

229. In terms of legal authority, the highest-ranking source of these obligations is China's Cybersecurity Law. Zhonghua Renmin Gongheguo Wanglao Anquan Fa (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017), art. 47-48, CLI.1.283838 (EN) (PKULaw) [hereinafter Cybersecurity Law]. However, more detailed articulations can be found in prior administrative regulations. *See* Internet Information Service Measures, *supra* note 215, at 15-16; Telecommunication Regulation, *supra* note 212, arts. 56, 61.

regulations.[230] It ranges from content that undermines state security, public order, social stability, or national honor to content that promotes vulgarity, pornography, gambling, or violence.[231] Some of these categories are noticeably vague, which may be deliberate so as to create chilling effects and induce companies to err on the side of caution by over-censoring.[232]

On top of all this, Internet-related companies sign a public "self-disciplinary" pledge that is administered and enforced by the quasi-governmental Internet Society of China.[233] This pledge, whereby signatories commit to adopting more proactive measures for monitoring and disposing of harmful information, is nominally voluntary. However, it appears as a practical matter to be yet another requisite to operating in China.[234]

Given the sheer number of Chinese netizens, prohibited content still frequently slips through the cracks. For this reason, the government has become increasingly proactive in policing Internet content itself. The Cyberspace Administration of China (CAC), the dual state/Party entity overseen by the Xi Jinping-led Central Cyberspace Affairs Commission, functions as a coordinating body on Internet censorship, and its provincial-level offices are tasked with monitoring and demanding removal of prohibited content online.[235] China has also taken steps to heighten enforcement of Internet companies' legal obligations, granting public security bureaus broad authority to conduct random inspections where they verify, among other things, that satisfactory measures for preventing dissemination of prohibited

230. *See* Gao, *supra* note 218, at 257 (noting that the list has remained largely constant for the past twenty years).

231. *See, e.g.*, Internet Information Service Measures, *supra* note 215, at 15.

232. *See* Bryan Druzin & Jessica Li, *Censorship's Fragile Grip on the Internet: Can Online Speech Be Controlled?*, 49 CORNELL INT'L L.J. 369, 376 (2016) ("Indeed, the genius of this statute is that it is fantastically vague. The precise ambit of permissible speech is left unclear to encourage self-censorship and maximize the range within which people voluntarily restrain their behavior online.").

233. Internet Soc'y China, *Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry*, CHINA DAILY (Mar. 26, 2002), https://govt.chinadaily.com.cn/s/201812/26/WS5c23261f498eb4f01ff253d2/public-pledge-of-self-regulation-and-professional-ethics-for-china-internet-industry.html [https://perma.cc/RFF3-DJHY].

234. *See* Creemers, *supra* note 216, at 94 (noting that compliance with the pledge has become a de facto soft requirement for having one's licensing renewed).

235. *See* Jamie P. Horsley, *Behind the Facade of China's Cyber Super-Regulator*, STAN. DIGICHINA (Aug. 4, 2022), https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/ [https://perma.cc/B345-F99G] (providing an overview of the rapidly ascendent and equally complex Cyberspace Administration of China); *see also* Ryan Fedasiuk, *Buying Silence: The Price of Internet Censorship in China*, JAMESTOWN FOUND. (Jan. 12, 2021), https://jamestown.org/program/buying-silence-the-price-of-internet-censorship-in-china/ [https://perma.cc/YCN8-24KG] (estimating Chinese government's on expenditures on direct censorship activities); Henry L. Hu, *The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration*, 207 CHINA Q. 523, 526-27 (2011) (detailing the of use coordinated, periodic "strikes" against unlawful content carried out through ISPs even before the CAC was established).

content are in place.[236] Internet companies have very little latitude when it comes to responding to demands from Chinese authorities if they intend to retain their operating licenses. When the party-state can simply order an ISP to cut off a subscriber and they have no real choice but to comply, there is only a small amount of value to be derived from a built-in "shutoff" protocol like that shown in the New IP proposal.

4. Real-Name Registration and Record-Keeping

Next, ISPs and ICPs in China have become subject to an increasing number of subscriber/user registration and record-keeping obligations that together have greatly eroded the anonymity enjoyed by Chinese netizens.[237] At the content/application level, virtually any online service that enables users to post, publish, or send information is legally required to register them using authenticated real-identity information.[238] This includes microblogs, forums, instant messaging applications, and websites with comment sections.[239] Failure to comply can lead to large fines, license forfeiture, and even secondary tort liability for acts committed by an anonymous user that the online service provider failed to properly register.[240]

As an additional layer of protection, a similar set of requirements exists at the infrastructure level. Network operators, both fixed line and mobile, are legally required to register subscribers using authentic identity information.[241] The requirement extends to Internet access offered to patrons at places of business, meaning an individual who wishes to connect to the Wi-Fi at their neighborhood Internet café must first show their government-issued ID card

---

236. *See* Gong'an Jiguan Hulianwang Anquan Jiandu Jiancha Guiding (公安机关互联网安全监督检查规定) [Provisions on Internet Security Supervision and Inspection by Public Security Organs] (Promulgated by Ministry of Pub. Security Sept. 5, 2018, effective Nov. 1, 2018), art. 10, CLI.4.322375 (EN) (PKULaw).

237. *See* Jyh-An Lee & Ching-Yi Liu, *Real-Name Registration Rules and the Fading Digital Anonymity in China*, 25 WASH. INT'L L.J. 1, 10-17 (2016) (examining the historical evolution of China's "real-name registration" policy).

238. *See, e.g.*, Cybersecurity Law, *supra* note 229, art. 24; China's real-name registration policy reflects the principle of "foreground voluntary name, background real name." While users must register their legal name with the platform operator, they are still able to choose their public display name on the platform. Samm Sacks & Paul Triolo, *Shrinking Anonymity in Chinese Cyberspace*, LAWFARE (Sept. 25, 2017), https://www.lawfareblog.com/shrinking-anonymity-chinese-cyberspace [https://perma.cc/2BMC-LJE3].

239. *See id.* (discussing several regulations involving real-name registration that were released shortly after China's Cybersecurity Law took effect).

240. *See* Rogier Creemers, *The Pivot in Chinese Cybergovernance: Integrating Internet Control in Xi Jinping's China*, 2015/4 CHINA PERSP. 10 (2015), https://journals.openedition.org/chinaperspectives/6835 [https://perma.cc/92B7-254T] [hereinafter Creemers, *Pivot in Chinese Cybergovernance*].

241. *See, e.g.*, Cybersecurity Law, *supra* note 229, art. 24.

to be verified and recorded.[242] ISPs are further required to keep and preserve detailed records about subscribers, most notably the IP address(es) assigned to them at any given time, and to disclose this information to state authorities upon request.[243] MIIT also maintains a centralized database of IP address blocks assigned to ISPs.[244] ISPs are obligated to promptly update the database whenever this information changes.[245] The database is accessible by the public security bureaus, so that upon discovering illegal content posted by someone who is identifiable only by IP address, they know exactly to which ISP to go in order to compel disclosure of a subscriber's identity. New IP's controversial "intrinsic security" features would do little to streamline this process, as the assistance of ISPs would still be needed to decrypt an embedded identifier and provide the corresponding real-identity information.

5. Promotion of IPv6 Deployment

China has been strongly promoting domestic IPv6 deployment for nearly two decades and has accelerated its efforts in recent years with the hope of achieving 100% adoption by 2025.[246] Some have long suspected that one of the primary motives behind China's IPv6 push is the fact that the expanded address pool would enable every device to have a globally unique identifier, making it easier to trace traffic back to its source.[247] This is because the scarcity of IPv4 addresses led to heavy reliance on Network Address Translation (NAT), which allows several devices share the same public-facing IP address and thus enjoy a degree of practical anonymity. IPv6 has no

---

242. Hulianwang Shangwang Fuwu Yingye Changsuo Guanli Tiaoli (互联网上网服务营业场所管理条例) [Regulations on the Administration of Business Sites of Internet Access Services] (promulgated by State Council, Sept. 29, 2002, effective Nov. 15, 2002, amended Mar. 24, 2019), art. 23, CLI.2.331350 (EN) (PKULaw). However, the thoroughness of this verification process appears to be somewhat inconsistent. It was reported in 2013 that several individuals had been regularly accessing the Internet at a café by using forged IDs that contained the name and image of U.S. President Barack Obama. *See Manager forged ID card to make "Obama" a regular at Chinese Internet café*, GLOB. TIMES (May 30, 2013), https://www.globaltimes.cn/content/785616.shtml [https://perma.cc/6WTQ-EGCE].

243. Hulianwang Anquan Baohu Jishu Cuoshi Guiding (互联网安全保护技术措施规) [Provisions on the Technical Measures for the Protection of the Security of the Internet] (promulgated by Ministry of Public Security Nov. 23, 2005, effective Mar. 1, 2006), art. 8, CLI.4.73057 (EN) (PKULaw).

244. Hulianwang IP Dizhi Beian Guanli Banfa (互联网IP地址备案管理办法) [Measures for the Administration of IP Address Archiving] (promulgated by Ministry of Info. Indus. Feb. 8, 2005, effective Mar. 20, 2005), art. 6, CLI.4.56965 (EN) (PKULaw).

245. *Id.* at 9.

246. *See* Yuedong Zhang, *100% by 2025: China getting serious about IPv6*, APNIC (June 6, 2019), https://blog.apnic.net/2019/06/06/100-by-2025-china-getting-serious-about-ipv6/ [https://perma.cc/6RC2-U6QF] (highlighting some of the goals outlined in the 2017 Party/State-issued IPv6 deployment plan and subsequent progress made towards achieving them).

247. Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 601 (2011) ("Indeed, part of China's push to deploy IPv6 is the country's desire to increase attribution and accountability online.").

such constraints, obviating the need for NAT and enabling a one-to-one mapping between address and device.[248] Ironically, some of the discussion around China's embrace of IPv6 in the mid-2000s is closely reminiscent of that surrounding New IP. For instance, a New York Times article from 2006 described IPv6 as "new technical standard enthusiastically embraced by China [that] will allow greater traceability of Internet users, potentially endangering those expressing views counter to the government's."[249]

Admittedly, the impending exhaustion of the IPv4 address space and the desire to obtain first-mover advantages were likely important motivations for China's IPv6 push.[250] In any case, China has undeniably welcomed the possibilities opened up by each device globally having a globally unique identifier.[251] The development of the aforementioned SAVA, designed with IPv6 in mind, is one illustration of this.[252] Having already been implemented on one of the country's major non-commercial backbone networks, it is still undergoing improvements and appears to remain a large part of China's plans. A new working group within the IETF titled "Source Address Validation in Intra-domain and Inter-domain Networks" was established in 2022, and Chinese participants look to be heavily involved.[253] This would provide much of the same functionality as New IP's end-to-end "intrinsic security," but without the need for an entirely new protocol.

* * *

In summary, while the conventional narrative charges the CCP with wanting to fundamentally change the Internet in order to provide governments

248. The ability to externally track a user by IPv6 address is largely dependent on how frequently an ISP rotates the network prefix (i.e., the assigned series of leading bits that devices then use to derive a full IPv6 address) delegated to a subscriber site. Though IPv6 privacy extensions have been designed to frequently change a device's address, all of these addresses would still have the same network prefix; where this prefix is relatively static and its length is known, the IPv6 address could be used as the basis for tracking. *See* Erik Rye et al., *Following the Scent: Defeating IPv6 Prefix Rotation Privacy*, *in* IMC'21: PROC. 21ST ACM INTERNET MEASUREMENT CONF. 739, 740 (2021), https://arxiv.org/pdf/2102.00542.pdf [https://perma.cc/9G5F-BSCH] ("While privacy extensions protect clients when changing networks, IP-based tracking is still possible via the customer's assigned prefix.").

249. Thomas Crampton, *Innovation may lower Net users' privacy*, N.Y. TIMES (Mar. 19, 2006), https://www.nytimes.com/2006/03/19/business/worldbusiness/innovation-may-lower-net-users-privacy.html [https://perma.cc/M6H2-6N68].

250. *See* DENARDIS, PROTOCOL POLITICS, *supra* note 81, 109-10 (discussing the history of China's IPv6 strategy and its underlying motivations); Li Weitao, *Future of the Internet begins to take shape*, CHINA DAILY (last updated Sept. 25, 2006), http://www.chinadaily.com.cn/china/2006-09/25/content_695792.htm [https://perma.cc/J775-DYAE] (highlighting the opportunities presented by IPv6).

251. Salil Tripathi, *Cash for acquiescence*, THE GUARDIAN (Apr. 4, 2006), https://www.theguardian.com/technology/2006/apr/04/comment.china [https://perma.cc/PQS5-WZQS] ("Hu Qiheng, chair of the Internet Society of China warmly embraced IPv6, which . . . empowers governments like China's to track down individuals who might "misbehave" online.").

252. *See supra* note 148 and accompanying text.

253. *Source Address Validation in Intra-domain and Inter-domain Networks (savnet)*, IETF (2022), https://datatracker.ietf.org/wg/savnet/about/ [https://perma.cc/M7D9-2SJY].

with significant control over how their citizens use it, a careful examination of the legal and technical situation reveals that the existing protocol stack already gives China much of the power needed to accomplish these goals. It is true that China's current system is imperfect, expensive, and dependent on many non-technological forces outside the CCP's direct control.[254] Likewise, control-obsessed regimes like Beijing are not known to grow complacent with the status quo of their surveillance and censorship apparatus. Yet, as has been demonstrated throughout this Section, the type of architectural changes Chinese actors have endorsed through proposals like New IP would not represent a significant improvement over China's existing control regime.

Nor would they be an especially effective vehicle for spreading the so-called "Chinese model" around the world by giving aspiring digital-authoritarian countries tools that enable them to emulate China.[255] The effective use of such tools is dependent on, rather than a viable substitute for, China's sophisticated Internet control architecture. Consider some examples from the New IP proposal. A feature which cryptographically binds a personal identifier to all of a user's packets would be of little utility if the ISPs in a country are not already forced to preserve accurate records about subscribers' real identities and IP address assignments at all times. Similarly, a government hoping to use content-based addressing schemes (which New IP could hypothetically support in the future) as a censorship mechanism would have very limited success unless they possess the power to force the exclusive use of these schemes and the means to control cross-border Internet traffic. This censorship could otherwise be easily circumvented by accessing content the traditional way (i.e., using host-based identifiers like an IP address), especially when that content is hosted outside the country's jurisdictional reach.

More fundamentally, the premise that China threatens to increase international acceptance of authoritarianism by exporting related values through Internet infrastructure warrants greater skepticism. It appears to reflect the same type of soft-technological determinism as the United States' early "Internet Freedom" agenda that saw the Internet an unstoppable vehicle for democracy.[256] Just as the existing Internet failed to liberate China, Russia, and Iran, a cyber-sovereign Internet should be no more likely to increase the

254. *See* Lee & Liu, *supra* note 237, at 26 (recognizing that real-name registration would likely be impossible to enforce without the co-operation of ISPs or other Internet companies.); Druzin & Li, *supra* note 232, at 408-09 (arguing the heavy reliance of China's Internet control regime on self-censorship and private sector enforcement, rather than direct censorship through technological measures, makes it vulnerable to collapse).

255. *See* Erie & Streinz, *supra* note 71, at 14-16 (casting doubt on the ability of Chinse "digital authoritarianism" to be exported because, insofar as a "China model" exists, it is enabled by set of internal power relations, state capacities, and other historically conditioned features relatively unique to China).

256. *See supra* note 15 and accompanying text.

level of digital repression among governments that have not already embraced authoritarianism.[257]

This, of course, should not be construed as defense of authoritarian values or protocols that reflect these values. Nor is it a denial that China is attempting to facilitate the acceptance of cyber sovereignty around the globe. Instead, it is merely a recognition that if China is serious about spreading its alternative vision and enhancing its control capabilities, the realities of ITU-T governance and the private nature of standards adoption mean that re-inventing core Internet protocols through the global standard-setting process hardly represents a foolproof way to accomplishing those goals. The Internet architecture is, after all, just an architecture, and it can be used to support a variety of different implementations.[258] China has already demonstrated how the existing architecture can be implemented and configured in a way that enables state control while still preserving (selective) global interoperability. All of this thus strongly points to the possible existence of something more behind China's Internet standards agenda than the conventional accounts suggest.

V. TOWARDS AN ALTERNATIVE UNDERSTANDING

If the desire for enhanced Internet control capabilities or a more state-centric standards development model cannot fully explain China's advocacy of New IP, then what does? In this Part, we explore the role that economic interests play. This is readily visible in the case of New IP. Even though components such as "intrinsic security" raised some valid concerns, other features such as deterministic QoS appear to be more than just a smokescreen to conceal ulterior purposes. These features and the sector-specific use cases to which they are tailored are better understood in light of China's long-term growth and development planning, which seeks to transform Chinese industry through the deep integration of ICTs. The remainder of Part IV will both examine how Internet infrastructure innovation fits into China's industrial policy strategy as well as another frequently overlooked consideration—the role and economic interests of Chinese companies like Huawei—in order to construct a more compelling explanation of what is driving China's standards push.

257. Jessica Chen Weiss, *A World Safe for Autocracy? China's Rise and the Future of Global Politics*, FOREIGN AFFS., July-Aug. 2019, at 92, 98; *see also* STEVEN FELDSTEIN, THE RISE OF DIGITAL REPRESSION: HOW TECHNOLOGY IS RESHAPING POWER, POLITICS, AND RESISTANCE 48 (2021) (arguing that although Chinese firms make digital surveillance tools available to countries at low costs, domestic factors that generate demand for these tools are the main driver of digital repression); Segal, *supra* note 103, at 88 (offering countries' growing disillusionment over issues like disinformation and security as the primary driver of this demand).

258. David D. Clark, *The Design Philosophy of the DARPA Internet Protocols*, 18 ACM COMPUT. COMMC'N. REV. 106, 111 (1988) ("The Internet architecture tolerates this variety of realization by design.").

A. The Internet in Chinese Industrial Policy

One way to understand China's current campaign to evolve the Internet's architecture is as part of its lofty ambitions to transform the country into both a "cyber great power" and a modern "manufacturing power."[259] For the past decade, the highest levels of both the state and the party have repeatedly emphasized that realization of these goals depends heavily on the development of a new generation of information communication network infrastructure and capabilities. Rather than shape the future direction of the Internet's architecture towards greater state control, it appears much more interested in an architecture that is conducive to achieving its industrial policy goals.[260] In fact, nearly every dimension of Huawei's New IP proposal can be traced back to some economic development priority outlined in China's state-driven planning process.

A good place to start is the Five-Year development plans that the CCC-led government has used to shape the long-term direction of the country since the 1950s by outlining economic and social goals for the next period along with high-level strategies for achieving them.[261] The twelfth such plan was published in 2011. It heavily prioritized the continued development of China's ICT sector, identifying it as one of just a handful of "strategic emerging industries" expected to be a future driver of economic growth.[262] It also listed the improvement of China's science and technology innovation capacity as one of the main objectives for the period.[263] This was to be achieved through accelerating the transition to a predominantly enterprise-driven innovation system, increasing the support and resources available to industry, constructing major technology innovation infrastructure, and

259. These are common English translations of two important buzzwords that have appeared with increasing frequency across official Chinese policy, planning, and strategy documents over the past decade. *See* Rogier Creemers et al., *Lexicon: 网络强国 Wǎngluò Qiángguó*, STAN. DIGICHINA (May 31, 2018), https://digichina.stanford.edu/work/lexicon-%E7%BD%91%E7%BB%9C%E5%BC%BA%E5%9B%BD-wangluo-qiangguo/ [https://perma.cc/QQ5N-EP54]; *制造强国 (zhizao qiangguo): Manufacturing Power*, CHINA DAILY (June 29, 2015), https://www.chinadaily.com.cn/opinion/2015-06/29/content_21128372.htm [https://perma.cc/3H7P-WRRT].

260. Designing a future Internet around the need to support future economic goals is not necessarily an unusual idea. David Clark's work studying proposed future architectures has identified and categorized some of the distinct aspirational goals underlying various proposals. Among them is one that promotes the future Internet as a "platform for innovation," serving as a driver of economic growth by enabling new applications, technology development, and the disruption of industries. *See* DAVID D. CLARK, DESIGNING AN INTERNET 288, 291 (2018).

261. *What is China's five-year plan?*, THE ECONOMIST (Mar. 4, 2021), https://www.economist.com/the-economist-explains/2021/03/04/what-is-chinas-five-year-plan [https://perma.cc/4HE3-9RMA].

262. Robert D. Atkinson, *ICT Innovation Policy in China: A Review*, INFO. TECH. & INNOVATION FOUND. 2 (2014), https://www2.itif.org/2014-china-ict.pdf [https://perma.cc/WPW2-CHTH]

263. Zhonghua Renmin Gongheguo Guomin Jingji He Shehui Fazhan Di Shier Ge Wu Nian Guihua Gangyao (中华人民共和国国民经济和社会发展第十二个五年规划纲要) [The Twelfth Five-Year Plan for National Economic and Social Development of the People's Republic of China], chap. 27, CLI.1.146717 (EN) (PKULaw).

promoting breakthroughs in major areas like, inter alia, information networks.[264]

China's promotion of innovation and investment in the ICT sector is hardly a new development. It has long fallen under the rubric of "informatization" (*xinxihua*), the upgrading of social and economic processes through the application of ICTs.[265] This has been a central pillar of its development strategy for well over two decades.[266] What was new, however, was the elevated importance these goals were given.[267] The Plan was widely understood as an attempt to re-orient China's economy, shifting it away from a resource-dependent export-driven model and towards a more sustainable one fueled by indigenous innovation, specifically within emerging areas like next-generation ICTs.[268] Moreover, the plan made clear that enterprise was to play a leading role in this innovation-driven economy and that the state should strengthen science and technology infrastructure in order to facilitate private innovation in key areas.[269]

Shortly thereafter, the State Council released more detailed implementation plan for carrying out a number of science and technology infrastructure construction projects pursuant to the Twelfth Five-Year Plan.[270] Among the sixteen major projects outlined was one titled "future network test facilities," a large-scale experimental network infrastructure and test

264. *Id.*

265. Creemers, *Pivot in Chinese Cybergovernance*, *supra* note 240, at 2, 6.

266. Informatization has been a crucial component of China's developmental and industrial policy since at least the late 1990s. It is on the back of this informatization agenda that Chinese leaders have pinned their hopes of "leapfrog development" through which it catches up to and eventually surpasses the industrialized West. *See* Xiudian Dai, *ICTs in China's Development Strategy*, *in* CHINA AND THE INTERNET: POLITICS OF THE DIGITAL LEAP FORWARD 8 (Christopher R. Hughes & Gudrun Wacker eds., 2003).

267. *See* Yu Hong, *Reading the 13th Five-Year Plan: Reflections on China's ICT Policy*, 11 INT'L J. COMMC'N 1755, 1758-59 (2017) (stating that the status of ICTs in the 12YP was one of "unprecedented importance").

268. *See, e.g.*, Joseph Casey & Katherine Koleski, *Backgrounder: China's 12th Five-Year Plan*, U.S.-CHINA ECON. & SEC. REV. COMM'N 3-4 (June 24, 2011), https://www.uscc.gov/sites/default/files/Research/12th-FiveYearPlan_062811.pdf [Remove Hyperlink Functionality] [https://perma.cc/P9ZH-7L4S] (suggesting the shift towards a steadier growth model may have been partially motivated by the 2008 financial crisis, which saw the collapse in global demand for Chinese exports, and in turn, Chinese economic growth).

269. ROBERT ASH, ROBIN PORTER & TIM SUMMERS, CHINA, THE EU AND CHINA'S TWELFTH FIVE-YEAR PROGRAMME 88-89 (2012), https://www.chathamhouse.org/sites/default/files/public/Research/Asia/0312ecran_ashporterssummers.pdf [https://perma.cc/R7MK-YVGY]

270. *China approves science infrastructure plan*, CHINA DAILY (Jan. 16, 2013), http://www.chinadaily.com.cn/china/2013-01/16/content16127710.htm [https://perma.cc/47TE-NG63].

environment intended to promote breakthroughs in future networks.[271] Interestingly, the State Council offers many of the same arguments here that Huawei would later use to justify New IP. It claims that the TCP/IP Internet is unable to meet the needs of future development, as emergence of technologies such as cloud computing and IoT have posed large challenges to Internet security, service quality, and mobility.[272] It is likely no coincidence that nearly a decade afterward, the experimental network testbed constructed as part of this very project was where Huawei completed large-scale testing of certain New IP-related features.[273]

The subsequent development period, marked by the issuance of thirteenth Five-Year Plan in 2016, saw the continuation of many key initiatives from the previous Plan.[274] Just as importantly, it was during this period that China announced Internet Plus, an initiative seeking to promote the integration of ICTs into traditional industries—manufacturing, healthcare, energy, agriculture, and finance—in order to fuel economic growth and innovation.[275] The manufacturing dimension of the Internet Plus initiative is particularly relevant, as it helps shed light on why use cases like smart manufacturing and IIoT are so prominently featured throughout the New IP proposal.[276] The Internet Plus initiative is an important component of the

---

271. Guojia Zhongda Keji Jichu Sheshi Jianshe Zhong Chanqi Guiha 2012-2030 Nian (国家重大科技基础设施建设中长期规划2012—2030年) [Medium and Long-Term Plan for National Major Scientific and Technological Infrastructure Construction 2012-2030], (issued by State Council Mar. 4, 2013), http://www.gov.cn/zwgk/2013-03/04/content_2344891.htm [https://perma.cc/39LX-LZGW] [hereinafter Medium and Long-Term Infrastructure Construction Plan]. The future network test environment that was eventually built is called the China Environment for Network Innovations (CENI) and is supported by a new high performance backbone network connecting 40 different Chinese universities. *See* Stephen Chen, *China starts large-scale testing of its internet of the future*, S. CHINA MORNING POST (Apr. 20, 2021), https://www.scmp.com/news/china/science/article/3130338/china-starts-large-scale-testing-its-internet-future [https://perma.cc/BU7G-JLXQ]. Predictably, Huawei was selected as one of the primary vendors for the project and supplied much of the equipment underlying this new infrastructure. *See Jiangsu Future Networks Innovation Institute Uses Huawei's WDM Technologies to Build National Network Test Facilities in China*, HUAWEI (Aug. 29, 2019), https://e.huawei.com/se/news/ebg/2019/Jiangsu-future-network-huawei-wdm-technology [https://perma.cc/HFD3-MQLK].

272. *See* Medium and Long-Term Infrastructure Construction Plan, *supra* note 271.

273. *See* Shoushou Ren et al., *Deterministic Network Forwarding Technology*, 1 COMMC'NS HUAWEI RSCH. 184, 192-93 (June 2022), https://www-file.huawei.com/-/media/corp2020/pdf/publications/huawei-research/2022/huawei-research-issue1-en.pdf [https://perma.cc/TL7B-WLV8] (highlighting results of experimental verification conducted on national large-scale testbed); *see also* Yan Shen 闫岫 & Li Zhong 李忠, *Huawei New IP Jishu Shiyan* (华为 New IP 技术试验) [*Huawei New IP Technology Trial*], CENI, https://ceni.org.cn/406.html [https://perma.cc/BTV9-DGFG] (last visited Feb. 26, 2023).

274. *See* Hong, *supra* note 267, at 1759.

275. "*Internet Plus" to fuel innovation, development China unveils Internet Plus action plan to fuel growth*, XINHUA (June 4, 2015), http://english.www.gov.cn/policies/latest_releases/2015/07/04/content_281475140165588.htm [https://perma.cc/NVT5-C4QW].

276. Internet Plus is even explicitly referenced in initial New IP contribution that Huawei submitted to the ITU-T. *See* TSAG-C83, *supra* note 6 ("The combination of datamation and manufacturing industries, or 'Internet+', will bring a great deal of benefit to human society.").

"Made in China 2025" plan, a long-term strategy to radically transform China's manufacturing base and move up the global value chain.[277] Made in China 2025 aims evolve Chinese manufacturing from a cheap, quantity-based model to an "intelligentized," one based on high quality.[278] China believes this can be achieved, in part, by leveraging technologies like IoT, advanced robotics, cloud computing, and big data analytics to improve manufacturing speed, quality, and efficiency.[279] The industrial Internet is the common thread connecting all of these technologies together.

Though certainly not lacking in buzzwords, China has taken concrete steps to advance this agenda. A recent National Informatization Plan published by the CAC, for instance, sets a goal of increasing "Enterprise Industrial Equipment Cloud Usage" from thirteen percent to thirty percent by the end of 2025.[280] The type of fully autonomous manufacturing scenario depicted in the New IP proposals, where connected machinery is monitored and controlled by software running in a remote data center, is not all that far-fetched.[281] There are obvious risks associated with connecting Industrial Control Systems (ICS) to the public Internet, let alone moving them to the cloud. It would place a lot of pressure on networks to meet performance demands with little margin for error. From a security standpoint, it also expands the attack surfaces of these systems, introducing new pathways that malicious actors could potentially infiltrate. High-profile incidents like the Stuxnet worm and Colonial Pipeline hack illustrate the type of real-world impact that cyberattacks directed at Operational Technology can have.[282]

China seems to recognize these different risks to some extent. In 2017, the State Council issued a guiding opinion on *Deepening the Internet Plus Advanced Manufacturing*, in which it called for the acceleration of research and development into new capabilities that help meet the need for secure, low-

277. *See* Scott Kennedy, *Made in China 2025*, CTR. STRATEGIC & INT'L STUD. (June 1, 2015), https://www.csis.org/analysis/made-china-2025 [https://perma.cc/KCJ3-W3MK] (summarizing Made in China 2025); Jost Wübbeke et al., *Made in China 2025: The making of a high-tech superpower and consequences for industrial countries*, 20 (MERICS Papers on China, No. 2, Dec. 2016), https://merics.org/sites/default/files/2020-04/Made%20in%20China%202025.pdf [https://perma.cc/LJ7D-CTWZ] (explaining the relationship between Internet Plus and Made in China 2025).

278. *See* Zhongguo Zhizao 2025 (中国制造2025) [Made in China 2025] (issued by State Council July 7, 2015), *translated in* CTR. SEC. & EMERGING TECH. 5 (Mar. 8, 2022), https://cset.georgetown.edu/wp-content/uploads/t0432_made_in_china_2025_EN.pdf [https://perma.cc/5RH6-DDMJ].

279. *See id.* at 11-14 (outlining tasks for promoting the "deep integration of informatization and industrialization," one of the key points of the plan).

280. Rogier Creemers et al., *Translation: 14th Five-Year Plan for National Informatization*, STAN. DIGICHINA (Jan. 24, 2022), https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/ [https://perma.cc/DN67-KALK].

281. *See, e.g.*, TSAG Tutorial, *supra* note 120, at 7; Li, *Market Opportunities*, *supra* note 121, at 8.

282. *See generally* David Kushner, *The Real Story of Stuxnet*, IEEE SPECTRUM, Mar. 2013, at 48; Andy Greenberg, *The Colonial Pipeline Hack Is a New Extreme for Ransomware*, WIRED (May 8, 2021), https://www.wired.com/story/colonial-pipeline-ransomware-attack/ [https://perma.cc/F4JG-QULQ].

latency, and highly reliable industrial networks.[283] Among the specific areas into which it directs intensified research efforts are Deterministic Networking, "heterogeneous identifier interoperability," and—most emphatically—measures for providing strong "security guarantees," all of which happen to be major elements of the New IP proposal.[284] Thus, while much of what China envisions here is extremely ambitious—often to the point of being overzealous—there is little doubt these aspirations have informed the type of future Internet capabilities reflected in New IP.

B. The Role of China's Oft-Forgotten "Private" Sector

Given the extent to which discussions of New IP have revolved around the Chinese government, it becomes easy to forget that it was in fact Huawei that conceived and led the initiative. This tendency to overlook the role and interests of the Chinese firms participating in SDOs also manifests itself in the wider debate over China's growing engagement in ICT standards development. Of course, we would be remiss not to acknowledge the legitimate questions surrounding the level of independence these firms enjoy from the party-state and whether it is fair to consider them as belonging to the private sector.[285] Huawei and its mysterious ownership structure are certainly no exception.[286] Yet, as long as Chinese firms like Huawei have a profit motive, there is strong reason to believe they are more than mere agents of the party-state and are responsive to the myriad of economic incentives they face in the standard-setting arena.[287]

There are indeed many economic interests at stake in the outcome of the standardization process. As Janet Abbate explains, these "technical decisions can have far-reaching economic and social consequences, altering the balance of power between competing businesses or nations."[288] Firms that are successful in shaping a standard are often able to translate this into a significant competitive advantage.[289] There is also a prestige factor, as having a standard endorsed by an SDO can signal a firms' market leadership and/or

---

283. *See* Guowuyuan Guanyu Shenhua Hulianwang+ Zianjin Zhizao Ye Fazhan Gongye Hulianwang De Zhidao Yijian (国务院关于深化"互联网+先进制造业"发展工业互联网的指导意见) [Guiding Opinions of the State Council on Deepening the "Internet Plus Advanced Manufacturing" and Developing the Industrial Internet] (promulgated by State Council Nov. 19, 2017, effective Nov. 19, 2017), § III, CLI.2.305507 (EN) (PKULaw).

284. *See id.*

285. *See* Erie & Streinz, *supra* note 71, at 53-61 (examining the relationship between Chinese MNCs, SOEs, and the party-state).

286. *See also* Raymond Zhong, *Who Owns Huawei? The Company Tried to Explain. It Got Complicated*, N.Y. TIMES (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/technology/who-owns-huawei.html [https://perma.cc/CG6H-CPRX].

287. *See* Erie & Streinz, *supra* note 71, at 55.

288. ABBATE, *supra* note 81, at 179.

289. *See* Stanley M. Besen & Joseph Farrell, *Choosing How to Compete: Strategies and Tactics in Standardization*, J. ECON. PERSP., Spr. 1994, at 117, 124-25 (explaining that firms will often prefer different standard candidates despite having an interest in compatibility because it would give them an advantage over rivals).

capacity to innovate. A popular saying among Chinese policymakers states that "third-tier companies make products, second-tier companies make technology, and first-tier companies make standards."[290] The CCP has strong aspirations for China to be a country of first-tier companies and has shown a willingness to provide domestic firms with the financial support and incentives necessary to achieve this. Hence, Chinese firms are not only subject to the same commercial incentives that have historically driven the engagement of their Western counterparts, but additional carrots dangled by the party-state provide all the more reasons to pursue influence over shaping technical standards.

Beyond the firm-specific economic interests at play, the different groups of industry actors involved in the Internet standard-setting process—network operators, hardware vendors, application providers, etc.—have their own collective interests.[291] The ongoing conflict between the various groups vying to maximize their interests and move up the network value-chain has come be known as "the tussle."[292] This tussle can be seen playing out in the case of New IP. Huawei's proposal was interested in shifting the Internet architecture towards a more intelligent network core, thereby securing a greater opportunity for equipment vendors to add and capture value at a time when their role has been steadily diminishing.

Though Huawei is perhaps best known for its wireless access network equipment, it is also one of the world's leading vendors of core routers, switches, and other specialized appliances (i.e., "middleboxes"). It is important to understand that New IP was proposed against a backdrop in which network hardware has grown increasingly commoditized. This trend is largely due to the emergence of technologies like virtualization, which enable different network tasks traditionally bound to specialized hardware to instead be performed at the software-level on cheaper general-purpose hardware or more centrally in the cloud.[293] Insofar as the TCP/IP model even afforded opportunities for hardware vendors like Huawei to add value to the network, these opportunities have been slowly eroding away along with their margins. This has led major vendors scrambling for new potential revenue streams.[294]

Through New IP, Huawei is counteracting this trend by adding greater complexity to the network, shifting many of the functions for meeting

---

290. Seaman, *supra* note 61, at 14; Neaher et al., *supra* note 78, at 6; Russel & Berger, *supra* note 61, at 12.

291. *See* David D. Clark et al., *Tussle in Cyberspace: Defining Tomorrow's Internet*, 13 IEEE/ACM TRANSACTIONS NETWORKING 462, 462 (2005).

292. *Id.*

293. *See generally What is Software-Defined Networking (SDN)?*, VMWARE, https://www.vmware.com/topics/glossary/content/software-defined-networking.html [https://perma.cc/8J5K-WA8W] (last visited Feb. 26, 2023); *VNF and CNF, what's the difference?*, REDHAT (last updated July 28, 2022), https://www.redhat.com/en/topics/cloud-native-apps/vnf-and-cnf-whats-the-difference [https://perma.cc/RX5T-Y5YQ].

294. *See, e.g.*, Himanshu Agarwal et al., *Hardware's business-model shift: Finding a new path forward*, MCKINSEY (Mar. 3, 2021), https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/hardwares-business-model-shift-finding-a-new-path-forward [https://perma.cc/RWP2-P8VH] (noting that Cisco has responded to the trend of hardware commoditization by expanding its portfolio into the software space).

application-specific needs from the endpoints to the core.[295] Huawei frequently draws on the analogy of private courier services, which have been upgraded with a number of enhancements for package delivery that were not available with traditional postal services.[296] This includes the ability to customize the speed or method of delivery as well as to track and receive confirmation of delivery as a means of verifying that special requirements were met.[297] Recognizing that customers have been willing to pay more for value-added services in the package delivery context, Huawei hails New IP as the long-awaited introduction of these enhancements to network services.[298]

While Huawei views New IP as the network equivalent of FedEx, others have instead made comparisons to older "virtual circuit" technologies like Asynchronous Transfer Mode (ATM), which emerged as a potential challenger to the TCP/IP stack in the 1990s.[299] ATM networks are connection-oriented, meaning they establish a dedicated virtual path before any data is transmitted. The use of such virtual circuits, which can exist on a permanent basis or be set up on demand, allows for the reservation of dedicated resources that can provide QoS guarantees (not unlike *IntServ*).[300] ATM networks take an active role in flow and congestion control in order to ensure these guarantees can be met. The upshot of this approach is that much more sophisticated and hence expensive core network hardware is required to operate at scale. Cost was a major reason that the host-oriented model of TCP/IP over Ethernet largely prevailed over ATM.[301] Huawei seems to be betting that this time around, enhanced features will be more economically viable due to the combination of increased demand from emerging use cases and the massive strides made in hardware/software since the 1990s.

One factor that may be working in its favor is the expanding market for its products in developing countries, something being facilitated by China's

---

295. See Geoff Huston, *New IP and emerging communications technologies*, APNIC (May 25, 2020), https://blog.apnic.net/2020/05/25/new-ip-and-emerging-communications-technologies/ [https://perma.cc/MJE2-KNG2] (placing New IP in the same category as other past initiatives that were motivated by vendors and operators' desire to add value and a refusal to "accept their role as a commodity utility").

296. Li, *Market Opportunities*, *supra* note 121, at 24-25; Li et al., *New IP Data Packet Framework*, *supra* note 119, at 4.

297. Li et al., *New IP Data Packet Framework*, *supra* note 119, at 4.

298. *See* Richard Li et al., *Qualitative Communication for Emerging Network Applications with New IP*, PROC. 17TH INT'L CONF. ON MOBILITY, SENSING & NETWORKING (MSN 2021) 628, 629-30 (2021), https://doi.org/10.1109/MSN53354.2021.00096 [https://perma.cc/4K75-BECQ] ("With New IP, the network services become customizable, trackable, assurable, and billable at the packet level.").

299. *Id.* at 630; *see also* Alain Durand, *New IP* 28 (ICANN Off. Chief Tech. Officer, OCTO-017, Oct. 27, 2020), https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf [https://perma.cc/VEU2-QZBG] ("Better-than-best-effort networking appears to suggest a return to circuit-switched technology, harking back to ATM days."); Huston, *supra* note 295.

300. See Claffy & Clark, *supra* note 125, at 222 (explaining that a main impetus behind *IntServ* was the ongoing development of ATM and concerns over TCP/IP's future were it unable to support similar functionality).

301. Durand, *supra* note 299, at 28.

DSR initiative.[302] DSR countries, a large share of which are located in the Global South, tend to lack well-developed digital infrastructure and jump at the opportunity to help modernize their economies. In Africa, for example, Huawei has been contracted by several governments to carry out the construction of national fiber optic backbone or wireless broadband networks, projects financed with concessional loans from Chinese state-owned development banks.[303] As a result, many African countries have become heavily reliant on Huawei equipment in both their fixed and wireless networks.

There are strong indications that Huawei intends to push similar "value-added" network features in DSR countries. In the fall of 2022, it co-released a whitepaper with the African Telecommunications Union on IPv6 Development in Africa.[304] The whitepaper promotes something called "IPv6 enhanced," a collection of IPv6 feature extensions and network operation and management tools that help enable capabilities like deterministic QoS, low latency transmission, and ultra-high bandwidth.[305] A consequence of adopting more complex, vendor-specific network technologies—those in which networked applications become more tightly coupled to the network itself—is that it becomes increasingly challenging to migrate to alternatives in the future. It can thus lead to a type of path dependence or vendor lock-in, giving Huawei a much more durable hold on these markets in the future. As digital ecosystems within DSR countries begin to take shape around Huawei's network solutions, it may become very difficult for competing vendors to ever win them back.

---

302. *See* Erie & Streinz, *supra* note 71, at 50-53; Greene & Triolo, *supra* note 70 (maintaining that as DSR countries look to expand their digital infrastructure, Chinese tech companies "will enjoy significant state support" to help meet this demand).

303. Alan Weissberger, *China (led by Huawei) in bid to take over Africa's telecom networks*, IEEE COMSOC: TECH. BLOG (Aug. 14, 2021), https://techblog.comsoc.org/2021/08/14/china-led-by-huawei-in-bid-to-take-over-africas-telecom-networks/ [https://perma.cc/79DK-5XUD]; *see also* Motolani Agbebi, *China's Digital Silk Road and Africa's Technological Future*, COUNCIL ON FOREIGN RELS. (Feb. 1, 2022), https://www.cfr.org/sites/default/files/pdf/Chinas%20Digital%20Silk%20Road%20and%20Africas%20Technological%20Future_FINAL.pdf3 [https://perma.cc/44NJ-YQUG] (displaying a list of African telecom infrastructure construction projects Huawei has been involved in over the last decade).

304. *ATU, African Union & Huawei Release Africa IPv6 Development White Paper*, HUAWEI (Nov. 14, 2022), https://blog.huawei.com/2022/11/14/atu-african-union-huawei-release-africa-ipv6-development-white-paper/ [https://perma.cc/MX88-RFLE].

305. AFRICAN TELECOMM. UNION & HUAWEI, AFRICA IPV6 DEVELOPMENT WHITE PAPER: IPV6: THE WAY FORWARD FOR AFRICA'S DIGITAL FUTURE 5-6 (2022), https://e.huawei.com/za/material/networking/6706d69e17564b10bb2ac87498e633b9 [https://perma.cc/29YS-H2BT]; *see also infra* Section IV Part B for a more complete discussion on "IPv6 enhanced."

VI. CHINA'S RISE AND THE FUTURE OF THE GLOBAL INTERNET

The trojan horse narrative leads to a number of predictions about the consequences of failing to address the threat posed by China, ranging from an eventual ITU Internet takeover to the bifurcation of cyberspace into two separate Internets that reflect the new multipolar world order. Having made a case against the common understanding of what motivates China's desire to shape Internet standards, we now turn to another fascinating question: what might China's emergence in this sphere *really* hold in store for the global Internet? In this Part, we explore the future implications of this trend as it pertains to three areas: the ITU's involvement in Internet governance activities, China's role in shaping the Internet's technical architecture, and the possibility of a global "splinternet."

A. Internet Governance Activities at the ITU

In the planning process leading up to the most recent World Telecommunication Standardization Assembly (WTSA-20), the event at which ITU-T study group activities for the next period are approved, several proposed study topics related to New IP failed to gain approval.[306] As we point out in Part III, ITU-T's adherence to consensus-based decision-making made this predictable. However, this outcome also reaffirms something that has been evident for some time: that concerns about the ITU's takeover of Internet governance functions have been overstated. Despite claims that authoritarian states like Russia and China have made advances in the ITU,[307] the easy defeat of New IP provides a stark reminder of just how much of an uphill battle these countries face.

It is important to recognize this, as claims that the ITU is attempting to take over the Internet are hardly new and will likely resurface again in the future. This takeover narrative rears its head every few years when some major event transforms the ITU into a battleground for competing visions of governance with the fate of the Internet allegedly hanging in the balance. Previous iterations include: the ITU's bid to inherit responsibility for managing the Internet's namespace prior to the establishment of Internet Corporation for Assigned Names and Numbers (ICANN) in the late 1990s,[308]

306. *See* SG13 December 2020 Meeting Report, *supra* note 186, at 4. Also note that WTSA-20 was postponed due to the COVID-19 pandemic and did not take place until March 2022. However, the planning process took place according to the originally scheduled timeline.

307. *See, e.g.*, FREEDOM HOUSE, *supra* note 174, at 3 ("Diplomats from China and Russia have made inroads at institutions like the International Telecommunication Union (ITU), seeking to transform the United Nations agency into a global internet regulator that advances authoritarian interests"); THE NEW BIG BROTHER, *supra* note 10, at 44 (citing China's "ushering in of the proposed New IP" as evidence that its strategy to leverage its influence at multilateral institutions like the ITU has been successful).

308. *See* Wolfgang Kleinwachter, *Beyond ICANN vs. ITU? How WSIS Tries to Enter the New Territory of Internet Governance*, 66 GAZETTE: INT'L J. COMMC'NS STUD. 233, 235-240 (2004) (recalling early attempts by the ITU to assume control of managing the DNS).

a renewed push to take control over these functions just a few years later at the World Summits on Information Society (WSIS),[309] the proposed revisions to the International Telecommunications Regulations (ITRs) at the World Conference on International Telecommunications (WCIT) convened in Dubai in 2012,[310] and the efforts to advance a number of proposals related to the Distributed Object Architecture, an alternative system of Internet identifiers purported to be ideal for IoT and that would be administered by a body under the auspices of the ITU.[311]

The example that is particularly instructive here is that of the 2012 WCIT, which involved ITU member states contemplating updates to the treaty-level ITRs. Some of proposed revisions submitted by countries like Saudi Arabia and Russia led commentators to sound the alarm over what they perceived to be a government-led power grab.[312] Vint Cerf, one of the Internet's founding fathers, testified before Congress that the outcome of WCIT risked "a fundamental shift in how the Internet is governed."[313] Likewise, then-FCC commissioner Robert McDowell penned a *Wall Street Journal* op-ed warning the WCIT threatened to give the U.N. "unprecedented powers over the Internet."[314] Fortunately, this never materialized, as less than half of all member states ultimately signed a watered-down version of the updated ITRs.

Yet, even in the leadup to WCIT, many respected voices from the Internet governance and policy realm recognized that the prospect of the ITU unilaterally expanding its authority over certain Internet governance functions had been inflated.[315] They correctly pointed out that the ITU lacked the power

309. MUELLER, NETWORKS AND STATES, *supra* note 36, at 57-59 (providing a history of WSIS, the ITU-led multi-phase summit through which a number of participating states took aim at ICANN and its relationship with the U.S.).

310. *See* Robert M. McDowell, *The U.N. Threat to Internet Freedom*, WALL ST. J. (Feb. 21, 2012), http://online.wsj.com/article/SB10001424052970204792404577229074023195322.html [Insert Permalink] (arguing that revisions to the ITRs could result in giving the U.N. "unprecedented powers over the Internet").

311. *See* Robert M. McDowell & Gordon M. Goldstein, *The Authoritarian Internet Power Grab*, WALL ST. J. (Oct. 25, 2016), https://www.wsj.com/articles/the-authoritarian-internet-power-grab-1477436573 [https://perma.cc/979S-K6D5] (arguing the DOA is a strategic attempt by countries like China to take "centralized control" over the IoT).

312. *See, e.g.*, Violet Blue, *WCIT-12 leak shows Russia, China, others seek to define "government-controlled Internet,"* ZDNET (Dec. 8, 2012), https://www.zdnet.com/article/wcit-12-leak-shows-russia-china-others-seek-to-define-government-controlled-internet/ [https://perma.cc/33R2-ZZ82].

313. *International Proposals to Regulate the Internet: Hearing Before the Subcomm. on Commc'ns and Tech. of the H. Comm. on Energy & Com.*, 112th Cong. 80 (2012) (statement of Vinton Cerf), https://www.govinfo.gov/content/pkg/CHRG-112hhrg79558/html/CHRG-112hhrg79558.htm [https://perma.cc/53J3-YPM4].

314. *See* McDowell, *supra* note 310.

315. *See, e.g.*, Jack Goldsmith, *WCIT-12: An Opinionated Primer and Hysteria-Debunker*, LAWFARE (Nov. 30, 2012), https://www.lawfareblog.com/wcit-12-opinionated-primer-and-hysteria-debunker [https://perma.cc/K7R9-K67U]; Milton Mueller, *ITU Phobia: Why WCIT was derailed*, INTERNET GOVERNANCE PROJECT (Dec. 18, 2012), https://www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/ [https://perma.cc/MXH2-HP3R].

to simply assume regulatory control over the global Internet through a majority vote. In reality, the ITU had no real power of its own. The power to regulate the Internet within a country's borders resides exclusive with national governments, and insofar as the ITU has any ability to dictate how this power is exercised, it is because governments have voluntarily agreed to be bound by treaty instruments like the ITRs. Those who objected to the new ITRs could simply choose not to sign and ratify them, which is precisely what ended up happening.[316] Far from a power grab, these voices instead characterized WCIT as an attempt by the ITU to remain relevant amid a changing technological landscape.

The ITU's reduced importance in the modern ICT standards ecosystem, is arguably one reason why authoritarian countries have repeatedly sought an expanded role for it within Internet governance. The organization is, in many ways, a vestige of an era in which public telecommunications networks existed as state-owned or regulated monopolies, making an intergovernmental body the most natural standardization venue. Yet, the technology environment has evolved, markets have liberalized; new venues have emerged; and much of the subject matter within ITU-T's expert remit (i.e., circuit-switched telephony) has been relegated to legacy status. Authoritarian countries have recognized that ITU-T is an organization in search of a purpose and have sought to take advantage of it.[317] However, what is crucial is that none of these attempts have succeeded, nor do these countries appear to have made any significant inroads in gaining international support for an expanded ITU mandate.

This is unlikely to change anytime soon, a fact further reinforced by two recent developments. The first is the 2022 "Declaration for the Future of the Internet," a statement issued by a U.S.-led partnership of sixty (mostly) democratic countries reaffirming their commitment to upholding a free and open global Internet and the multistakeholder model of governance.[318] The declaration itself does little more than endorse a set of aspirational principles that are entirely non-binding on signatories. At the very least, however, it does send a message that there exists a coalition that is willing to defend multistakeholderism, a reminder of the opposition that those interested in

316. *See* Anthony Rutkowski, *Saying No to the ITRs*, CIRCLEID (Dec. 5, 2012), https://circleid.com/posts/20121205_saying_no_to_the_itrs [https://perma.cc/G5DE-RU3U] (arguing there are no real adverse consequences of not acceding to the new ITRs).

317. Anthony Rutkowski, *Privatizing the ITU-T: Back to the Future*, CIRCLEID (Aug. 17, 2012), https://circleid.com/posts/20120816_privatizing_the_itu_t_back_to_the_future [https://perma.cc/8E6G-95Q9] ("The problem with an intergovernmental organization without a purpose is that it becomes a venue of mischief.").

318. *See generally* White House, *A Declaration for the Future of the Internet*, WHITE HOUSE (Apr. 28, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf [https://perma.cc/CYF8-49W4].

pushing Internet governance functions to the ITU that their efforts will likely face.[319]

The other major development was the election of a new ITU Secretary-General at the 2022 Plenipotentiary Conference. It was effectively a two-candidate race between Rashid Ismailov, a Russian telecom official and former Huawei executive, and the United States' Doreen Bogdan-Martin, a thirty-year veteran of the ITU who received strong backing from the Biden Administration.[320] The election earned coverage from several mainstream media outlets, where it was heralded as "the most important election in the history of the Internet"," and a clash between two competing visions that would determine the fate of the net's future.[321] Fortunately, this latest iteration of the ITU Internet takeover narrative, like those before it, never came to be. The American candidate prevailed in a landslide to become the first female Secretary General in the institution's long history.[322] Although it is not certain how much of an upper hand (if any) a Russian victory would have given countries seeking to use the ITU to expand state control over the Internet, the election of Bogdan-Martin makes any such takeover all the more difficult.

The purpose of highlighting the exaggerated nature of concerns over the ITU's creep into Internet governance is not to suggest that developments taking place within it can be safely ignored without consequence. Even post-New IP, there continues to be a steady inflow of proposed standardization work at ITU-T that, if fully developed and implemented, has the potential to be highly disruptive to the technical foundation of the Internet and the established systems for managing its critical resources. One such example is a Chinese-led work item in ITU-T Study Group 13 titled "Decentralized Trustworthy Network Infrastructure" (DNI).[323] It proposes a permissioned blockchain network that would support decentralized management of the

---

319. Some have suggested that the intended target of the Declaration were the signatory countries who had been drifting away from the democratic vision of cyberspace, not those like Russia or China who reject it outright. Alex Engler, *The Declaration for the Future of the Internet Is for Wavering Democracies, Not China and Russia*, LAWFARE (May 6, 2022, 12:27 PM), https://www.lawfareblog.com/declaration-future-internet-wavering-democracies-not-china-and-russia [https://perma.cc/N4K6-UEDE]. While this may be true, it does not change what is being signaled to countries like China and Russia.

320. *Meet the Candidates*, ITU NEWS MAG. (Sept. 2020), at 10-18, https://www.itu.int/pub/S-GEN-NEWS-2022-4 [https://perma.cc/Z5N6-AKSQ].

321. *See, e.g.*, Michael Morell, *This obscure election will decide the fate of the open internet*, WASH. POST (Sept. 28, 2022), https://www.washingtonpost.com/opinions/2022/09/28/un-international-telecommunication-union-election/ [https://perma.cc/FJN9-8WBW]; *An election that could make the global internet safer for autocrats*, THE ECONOMIST (Sept. 20, 2022), https://www.economist.com/international/2022/09/20/an-election-that-could-make-the-global-internet-safer-for-autocrats [https://perma.cc/CY4C-LRAW].

322. Press Release, Member States Elect Doreen Bogdan-Martin as ITU, INT'L TELECOMM. UNION (Sept. 29, 2022), https://www.itu.int/en/mediacentre/Pages/PR-2022-09-29-ITU-SG-elected-Doreen-Bogdan-Martin.aspx [https://perma.cc/TF32-KQC7].

323. Though DNI is concerned with the Internet's supporting infrastructure (i.e., the DNS, PKI, etc.), whereas New IP focuses on protocol innovation at the network layer, the two still appear to be loosely related. Huawei has been the driving force behind both initiatives and even identifies some of the same problems DNI intends to address in its New IP submissions to the ITU-T. *See* TSAG Tutorial, *supra* note 120, at 10.

Internet's global name and address spaces.[324] The blockchain network's nodes, which only organizations like regional and national Internet registries would be eligible to run, approve transactions (e.g., an address block assignment or domain name transfer) through some sort of consensus process and write it to a distributed, immutable ledger.[325] This blockchain-oriented solution would effectively displace the existing regime for managing these activities currently led by ICANN. A draft Recommendation defining requirements and a high-level framework for DNI reached the "last call" stage of ITU-T's Alternative Approval Process in late 2021. This draft would have been approved were it not for substantive issues raised by UK delegates to ITU-T.[326] The draft must now go up for additional review at a future Study Group meeting, where it will struggle to gain final approval.

The DNI example illustrates the risks of neglecting ITU-T entirely. Although its approval would not have brought the dream of replacing ICANN with the blockchain much closer to reality, it would have still allowed a controversial idea to gain further legitimacy and momentum, increasing the likelihood that it become a source of unnecessary conflict in the future. Proposals like this should be expected to continue until there is a serious re-evaluation of certain ITU-T study groups, their mandates, and the need for their continuation. While a push to scale-back activities at ITU-T is something on which the United States' delegation should strongly consider taking the lead, they and other like-minded Member States need to remain vigilant for the time being.

Instead of encouraging disengagement from the ITU, the reason we highlight the exaggerated nature of its threat to Internet governance is to caution against it turning into a distraction. Myopically focusing on each new high-profile iteration of the recurring "ITU Internet takeover" cycle—growing to expect threats towards Internet values like openness and freedom to come from the actions of authoritarian challengers in Geneva—makes it very easy to overlook what is arguably a more formidable set of threats: the slow retreat from these values by liberal democracies. Indeed, many that have historically championed Internet freedom and openness have recently taken actions out of line with these values. A non-exhaustive list may include: the United States' flirtation with bans on popular Chinese apps,[327] the EU's

---

324. Int'l Telecomm. Union Telecomm. Standardization Sector [ITU-T], *Draft new Recommendation ITU-T Y.2086 (formerly Y.DNI-fr): "Framework and Requirements of Decentralized Trustworthy Network Infrastructure" - for consent*, SG13-TD613/WP3, at 9 (July 16, 2021), https://www.itu.int/md/T17-SG13-210716-TD-WP3-0613 [https://perma.cc/99WC-X7EJ].

325. *Id*. app. I.

326. *Y.2086: Framework and Requirements of Decentralized Trustworthy Network Infrastructure*, ITU-T AAP, https://www.itu.int/t/aap/recdetails/10055 [https://perma.cc/LS79-G3LV] (last visited Feb. 26, 2023).

327. *See* Paul Rosenzweig, *The WeChat and TikTok Bans Show the U.S. No Longer Stands for Internet Freedom*, SLATE: FUTURE TENSE (Sept. 28, 2020), https://slate.com/technology/2020/09/tiktok-wechat-icann-dns-internet-freedom.html [https://perma.cc/BDP9-2RDX]; Bobby Allyn, *Trump Signs Executive Order That Will Effectively Ban Use of TikTok in the U.S.*, NPR (Aug. 6, 2020), https://www.npr.org/2020/08/06/900019185/trump-signs-executive-order-that-will-effectively-ban-use-of-tiktok-in-the-u-s [https://perma.cc/JZ53-HKJ7]

ongoing development of a public DNS resolver service with built-in filtering of unlawful content,[328] and the UK's proposed Online Safety Bill that many warn would severely undermine online free expression.[329] Whereas the ITU is limited in its power to regulate the Internet, national governments are not. Thus, if one is truly concerned threats to the free and open Internet, they would be wise to broaden their sights beyond the ITU, as these developments are just as likely to come from Brussels, European capitals, or D.C. as Geneva.

B. Internet Evolution in China

As illustrated in Part IV, China has identified a number of future Internet capabilities it sees as necessary for supporting its long-term strategic objectives and has taken major steps to facilitate enterprise-driven innovation in these areas. Given their overall importance to its vision, China is not simply going to abandon the pursuit of these capabilities simply because Huawei's New IP proposal—one of many possible ways to achieve them—was unsuccessful. Some type of Internet architecture evolution, whether it be a clean slate design or merely a set of enhancements, will inevitably come out of China in the coming years. Although there are strong hints as to what this evolution may look like, it is still somewhat undetermined.

The most likely candidate at present is something called "IPv6+" (or "IPv6 enhanced"), which has been promoted by both China's CAC and MIIT as well as fully embraced by Huawei following the demise of New IP.[330] IPv6+ and New IP share many of the same functional goals (e.g., network determinism) which has led some to conclude IPv6+ is a simply a re-packaged version of New IP after the latter failed to catch on at the ITU.[331] Yet, there are significant differences between the two, the most notable being that IPv6+

---

328. *See* Markus Reuter, *EU will eigenen DNS-Server mit Filterlisten und Netzsperren* [*EU wants own DNS-Server with filter lists and blocking*], NETZPOLITIK.ORG (Jan. 24, 2022), https://netzpolitik.org/2022/dns4eu-eu-will-eigenen-dns-server-mit-filterlisten-und-netzsperren/ [https://perma.cc/LK64-DXJW]; Geoff Huston, *Some Thoughts on DNS4EU - the European Commission's Intention to Support the Development of a New European DNS Resolver*, CIRCLEID (Feb. 13, 2022), https://circleid.com/posts/20220213-some-thoughts-on-dns4eu-new-european-dns-resolver [https://perma.cc/6EVS-UJY6]; *Europe: Content moderation at infrastructure level must respect human rights*, ARTICLE 19 (Mar. 9, 2022), https://www.article19.org/resources/europe-content-moderation-at-infrastructure-level-must-respect-human-rights/ [https://perma.cc/4WWU-JH8P] (highlighting some of the concerns presented by DNS4EU project proposal).

329. *See also* Joe Mullin, *The UK Online Safety Bill Attacks Free Speech and Encryption*, ELEC. FRONTIER FOUND. (Aug. 5, 2022), https://www.eff.org/deeplinks/2022/08/uks-online-safety-bill-attacks-free-speech-and-encryption [https://perma.cc/35CQ-JUP5]; *UK: House of Lords must reject the Online Safety Bill*, ARTICLE 19 (Jan. 30, 2023), https://www.article19.org/resources/uk-house-of-lords-must-reject-the-online-safety-bill/ [https://perma.cc/5KXZ-RF5X].

330. *See IPv6 Enhanced Paves the Way for IP on Everything*, HUAWEI (Apr. 26, 2022), https://www.huawei.com/en/news/2022/4/has-ipv6-ip-on-everything [https://perma.cc/7B5Y-R4YJ].

331. *See, e.g.*, Luca Bertuzzi, *China rebrands proposal on internet governance, targeting developing countries*, EURACTIV (June 6, 2022), https://www.euractiv.com/section/digital/news/china-rebrands-proposal-on-internet-governance-targeting-developing-countries/ [https://perma.cc/QUA5-TZ6E].

is not actually a protocol itself. The name is rather misleading, as IPv6+ is just a buzzword the Chinese are using to denote a variety of IPv6-compatible technologies already being developed at places like the IETF.[332]

There is a growing amount of evidence suggesting that IPv6+ is indeed a large part of China's future Internet plans. As mentioned above, it is being actively pushed by major state and Party organs. In 2021, the CAC and MIIT jointly issued a notice on accelerating IPv6 deployment efforts which established the goal for China to become a driving force behind global IPv6+ technology by the year 2025.[333] The same notice calls for strengthening domestic IPv6 research and standardization activities as well as increasing the participation of Chinese actors in the formulation of IPv6-related international standards.[334] Here, it identifies two particular standards bodies by name: the European Telecommunications Standards Institute (ETSI) and the IETF.[335] Not coincidentally, of the new Internet Drafts submitted to IETF working groups that are home to IPv6+ technologies, a large percentage feature authors affiliated with companies like Huawei, ZTE, and China Mobile.[336] In fact, Chinese participation in the IETF has been increasing in general.[337] In terms of total submissions, 2022 was the most active Chinese authors have ever been within the organization.[338] The progress made within the IETF was even emphasized in a recent whitepaper issued by China's State Council

332. One of the major IPv6+ technologies is Segment Routing over IPv6 (SRv6), a type of source routing that allows the network to better steer traffic by selecting a pre-determined path and embedding it into the packet header. IPv6+ also includes DetNet, the architecture developed by the IETF Deterministic Networking Working Group for ensuring minimal packet loss and bounded latency. For a complete list of component technologies *see IPv6+*, IPV6PLUS.NET https://www.ipv6plus.net [https://perma.cc/7FPC-3SVV] (last visited Feb. 26, 2023).

333. Zhongyang Wangluo Anquan He Xinxi Hua Weiyuanhui Bangongshi Guojia Fazhan He Gaige Weiyuanhui, Gongye He Xinxi Hua Bu Guanyu Jiakuai Tuijin Hulianwang Xieyi Di Liu Ban (IPv6) Guimo Bushu He Yingyong Gongzuo De Tongzhi (中央网络安全和信息化委员会办公室、国家发展和改革委员会、工业和信息化部关于加快推进互联网协议第六版(IPv6)规模部署和应用工作的通知) [Notice of the Office of the Central Cyber Security and Information Commission, the National Development and Reform Commission, and the Ministry of Industry and Information Technology of Accelerating the Large-Scale Deployment and Application of Internet Protocol Version 6 (IPv6)] (issued July 7, 2021) CLI.4.5054538 (EN) (PKULaw).

334. *Id.*

335. *Id.*

336. The examples are too numerous to list here. To see for oneself, the ipv6plus.net website, *supra* note 332, includes links to several related IETF Internet Drafts or RFCs for each IPv6+ feature listed. Virtually all of these were either authored or co-authored by individuals affiliated with Chinese entities.

337. *See* Nanni, *supra* note 79, at 2358 (finding a general increase in participation by Chinese actors—particularly Huawei—in select IETF working groups examined).

338. *Internet-Draft and RFC statistics*, IETF https://datatracker.ietf.org/stats/document/yearly/country/ [https://perma.cc/7DJ9-UQUG] (last visited Feb. 26, 2023).

Information Office.[339] Chinese actors continue to inch towards matching the contribution level of those from the United States, something difficult to imagine just a decade ago.

Given that criticisms of the New IP proposal included its top-down design approach, potential redundancy, lack of interoperability, and the venue it was presented at, one might think IPv6+ would be a welcome development. However, it has not managed to avoid its own share of controversy. In 2020, Huawei successfully pushed for a new working group on "IPv6 enhanced innovation" to be established within ETSI, one of the two standards body explicitly referenced in China's IPv6 strategy. The working group, which aimed to promote and support implementation of IPv6+ technologies developed at the IETF, quickly became one of the largest within ETSI in terms of active participants.[340] Yet, despite the group's ostensible popularity, concerns about IPv6+'s connection to Huawei and New IP persisted. When the working group was set to expire and requested an extension, it encountered strong opposition and was not allowed to continue.[341] It was further reported that the European Commission "played a decisive role" in coordinating this opposition.[342] One reason the Commission's involvement may be especially significant here is that it followed the release of a new EU Standardization Strategy just a few months earlier, a document allegedly motivated by growing concerns over Chinese influence at international and regional standards venues.[343]

Since all signs point towards continued growth in Chinese involvement in the IETF, politically motivated resistance to contributions from Huawei and other Chinese actors could have severe unintended consequences. It is understandable why the CCP's role in actively promoting this trend may make some given its less than stellar human rights record. We do not mean to suggest that stakeholders should disregard the political dimension of standard-setting or abdicate their responsibility for ensuring protocols are

339. *See* SCIO, Shared Future in Cyberspace, *supra* note 94, § III(3(1) ("China has also participated in the activities of the Internet Society (ISOC), Internet Engineering Task Force (IETF), and Internet Architecture Board (IAB). It has played a constructive role in facilitating community exchange, promoting technical R&D and application, and becoming closely involved in the formulation of relevant standards and rules.").

340. *See* Will Liu, *ETSI ISG IPE: Off to a good start*, ETSI (May 19, 2021), https://www.etsi.org/newsroom/blogs/technologies/entry/etsi-isg-ipe-off-to-a-good-start [https://perma.cc/3RB7-UZN2] (showing a graphical list of IPE working group participants); Latif Ladid, *ETSI IPv6 Enhanced innovation (ISG IPE) starts PoC activities at IPE#08*, ETSI (Sept. 30, 2022), https://www.etsi.org/newsroom/blogs/technologies/entry/etsi-ipv6-enhanced-innovation-isg-ipe-starts-poc-activities-at-ipe-08 [https://perma.cc/L38U-GT3K] (reporting it had surpassed 100 participants at last meeting).

341. Luca Bertuzzi, *Controversial European working group on internet governance faces shutdown*, Euractiv (Dec. 1, 2022), https://www.euractiv.com/section/digital/news/controversial-european-working-group-on-internet-governance-faces-shutdown/ [https://perma.cc/MR59-E868].

342. *Id.*

343. Jorge Valero & Alberto Nardelli, *EU Seeks to Counter China's Influence Over Global Standards*, BLOOMBERG (Feb. 1, 2022), https://www.bloomberg.com/news/articles/2022-02-01/eu-seeks-to-counter-china-s-influence-over-global-standards [https://perma.cc/GXT9-W9H6].

compatible with certain values like respect for human rights. Protocol designs with the objective or probable consequence of curbing civil liberties should obviously be resisted, even if only to avoid condoning or being complicit in the erosion of online freedoms. However, the New IP saga demonstrates that there is a tendency in the West to project fears of China's techno-authoritarianism and growing influence—fears which alone are not necessarily unfounded—onto Chinese technologies and standards when the evidence does not support it.

Adopting a combative response to the trend of increased Chinese engagement would have damaging effects on the legitimacy of venues like the IETF and would lend credence to the CCP's claims that incumbent multistakeholder Internet governance bodies exist only to serve Western interests. This is especially the case where opposition is promoted by policymakers. As former IETF Chair Alissa Cooper astutely observed in recent congressional testimony, such efforts could have the effect of "undermining the successful industry-led standardization system, fragmenting standards development into silos, and diminishing the influence of U.S. companies in global organizations."[344] So in short, Internet protocol evolution does appear to be coming to China, and the response of Western actors at venues like the IETF may greatly influence where and how that evolution takes shape.

C. The Prospect of a "Splinternet"

Those who pay attention to the ongoing discussions in the technology law and policy sphere have likely heard something by now about the worrying trend of Internet fragmentation. A recent report published by a Council on Foreign Relations-sponsored independent task force, for example, declared that the "era of the global Internet is over" and that the global Internet is becoming irreversibly fragmented.[345] In a similar vein, former Google CEO Eric Schmidt predicted in 2018 that an emergent China would lead to the creation of "two distinct Internets": the existing Western-centric Internet and a Chinese-led alternative that will come to dominate Asia.[346] Indeed, one of the concerns surrounding New IP was its potential to precipitate this exact

344. *Setting the Standards: Strengthening U.S. Leadership in Technical Standards, Hearing Before the Subcomm. Rsch. & Tech. of the H. Comm. Sci., Space, & Tech.*, 117TH CONG. (Mar. 17, 2022) (statement of Alissa Cooper), https://www.congress.gov/117/meeting/house/114508/witnesses/HHRG-117-SY15-Wstate-CooperA-20220317.pdf [https://perma.cc/6SRM-LRLA].

345. COUNCIL ON FOREIGN RELS., CONFRONTING REALITY IN CYBERSPACE: FOREIGN POLICY FOR A FRAGMENTED INTERNET 7 (May 2022), https://www.cfr.org/report/confronting-reality-in-cyberspace [https://perma.cc/ZA4R-SG8A].

346. Lora Kolodny, *Former Google CEO predicts the internet will split in two — and one part will be led by China*, CNBC (Sept. 20, 2018), https://www.cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html [https://perma.cc/69N3-85DB].

type of scenario.[347] Yet, the prospect of a true Chinese-led "splinternet," in which the country secedes from the global Internet to form an incompatible alternative, remains extraordinarily unlikely.

Given the inconsistent meanings attached to terms like "fragmentation" and "balkanization" as they frequently appear in the Internet context, it is crucial first to distinguish some important concepts. As Milton Mueller observes in his book *Will the Internet Fragment?*, if fragmentation is understood as the state of being separated into parts that are distinct from the whole, then the Internet has always been fragmented.[348] The Internet, as explained earlier in Part II, is a network of networks; it consists of thousands of independent autonomous systems—each with their own rules, policies, and configurations—interconnected through their ability to speak the same universal language at the network layer (IP) and the assistance of supporting global infrastructure like the DNS.[349]

A corporate network, for example, may be configured to block traffic to social media websites to ensure employees are being productive while on the clock. At a more macro level, data flows may rarely leave a country's national borders due to localization requirements and/or technical controls implemented at international gateways like China's. Similarly, Internet search results displayed to users in one country or geographic region may be hidden from users in another, such as those de-linked pursuant to EU's Right to Be Forgotten.[350]

In the scenarios above, the way the Internet is experienced by users—the content available to them and where they retrieve it from—varies significantly. However, the underlying architecture remains capable of universal interconnection; the only thing preventing the free flow of information is some entity, whether it be a government or private company, deciding to place a barrier in the way. This type of fragmentation is thus conceptually distinct from the type that involves the Internet breaking into separate parts that are *incapable* of interoperating due to technical

347. *See, e.g.*, Hoffman et al., *Standardising the Splinternet*, *supra* note 13, at 253-55 (arguing "decentralised internet infrastructure," a group of Chinese technologies the authors lump New IP in with, "could enable countries to decouple or disconnect from the current global internet"); Lauren Dudley, *Part Three: Huawei's Role in the China-Russia Technological Partnership*, COUNCIL ON FOREIGN RELS.: NET POLITICS (Dec. 16, 2020), https://www.cfr.org/blog/part-three-huaweis-role-china-russia-technological-partnership [https://perma.cc/2F32-FCGQ] (arguing New IP could further promote "the bifurcation of the global technological system"); Flavia Kenyon, *China's "splinternet" will create a state-controlled alternative cyberspace*, THE GUARDIAN (June 3, 2021), https://www.theguardian.com/global-development/2021/jun/03/chinas-splinternet-blockchain-state-control-of-cyberspace [https://perma.cc/4RCP-RS2T].

348. MILTON MUELLER, WILL THE INTERNET FRAGMENT?: SOVEREIGNTY , GLOBALIZATION AND CYBERSPACE 21-22 (2017) [hereinafter MUELLER, WILL THE INTERNET FRAGMENT?].

349. *Id.* at 24.

350. *See generally* Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772, (Sept. 24, 2019) (judgment) (limiting the territorial scope of the EU's right to be forgotten to within the EU's borders).

incompatibilities. The latter type has occasionally been referred as *technical fragmentation* to better capture the distinction.[351]

Although the two types of fragmentation are frequently conflated, the distinction matters. This softer variety of fragmentation, perhaps more appropriately conceptualized as the Internet growing increasingly *federated*, is undoubtedly a growing trend that is undesirable in many cases. However, the impact of the harder, technical form of fragmentation is much more severe, and the forces preventing it from happening are also much stronger.[352] When commentators raise concerns over long-term potential for a Chinese-precipitated "splinternet," this is typically the type of fragmentation to which they are alluding, as the other type of fragmentation already exists to an extreme degree with China's Internet. Yet, there is strong reason to doubt China will attempt a hard break from the global Internet any time soon.

Even if China were to push domestic adoption of a new Internet protocol suite that, by default, was incompatible with TCP/IP, the incentive to develop a mechanism for bridging the protocols (e.g., a translation gateway) would be near-overwhelming.[353] This is because completely isolating itself from the global Internet would cause China a great deal of self-inflicted economic damage. It is not just the global Internet it would be decoupling itself from but also the entire digital economy that operates on top of it.[354] Despite the restrictiveness of its Internet, China has become increasingly integrated into the global digital economy. Chinese firms in digital markets such as cloud services, e-commerce, and social media have gradually expanded their global reach.[355] Look no further than ByteDance, the Beijing-based parent company of TikTok, which, albeit controversial, has amassed a user base of over 100 million in the United States alone.[356]

A hard break from the global Internet would also be completely antithetical to long-term strategic initiatives like DSR. At the center of these are promoting digital interconnectedness and expanding the international

---

351. WILLIAM DRAKE ET AL., INTERNET FRAGMENTATION: AN OVERVIEW 4 (World Econ. F., Future of the Internet Initiative White Paper, 2016), https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf [https://perma.cc/A5UL-QDA2].

352. MUELLER, WILL THE INTERNET FRAGMENT?, *supra* note 348, at 30.

353. *Id.* at 62-63; *see also* Paul A. David & Julie Ann Bunn, *The Economics of Gateway Technologies and Network Evolution: Lessons from Electricity Supply Industry*, 3 INFO. ECON. & POL'Y 165, 197 (1988) (explaining that the economic significance of ex ante incompatibilities between network technologies can be mitigated through the use of gateway technologies).

354. U.N. Conf. on Trade & Dev., *Digital Economy Report 2021*, 114 U.N. Doc. UNCTAD/DER/2021 (Sept. 29, 2021), https://unctad.org/system/files/official-document/der2021_en.pdf [https://perma.cc/62UD-BSKX] [hereinafter UNCTAD Report] (noting that Internet fragmentation and digital economy fragmentation would be "joint processes").

355. *See* Longmei Zhang & Sally Chen, *China's Digital Economy: Opportunities and Risks* 4-6 (IMF Working Paper, No. 2019/016, 2019), https://www.imf.org/en/Publications/WP/Issues/2019/01/17/Chinas-Digital-Economy-Opportunities-and-Risks-46459 [https://perma.cc/FYK8-T5TH].

356. Alex Sherman, *TikTok reveals detailed user numbers for the first time*, CNBC (July 24, 2020), https://www.cnbc.com/2020/08/24/tiktok-reveals-us-global-user-growth-numbers-for-first-time.html [https://perma.cc/N9K5-MCMW].

presence of its digital national champions.[357] Even with aid and generous financing, the Chinese would have a difficult time persuading countries to adopt digital infrastructure incapable of interoperating with most of the world. It is conceivable that, at some point in the distant future, DSR countries will have become so deeply integrated into China's digital ecosystems and dependent on Chinese infrastructure that they would have no choice but to join China in breaking away from the global Internet.[358] This would make a splinternet more economically tolerable for China, as the loss of positive network externalities from migrating to a separate, smaller Internet would not be as drastic. Until then, however, a hard break from the global Internet would be prohibitively costly for China and should remain so for the foreseeable future.

China's Great Firewall and restrictions on information flows already come at a significant economic opportunity cost, one that it has been willing to accept in exchange for greater domestic security, stability, and control. The tradeoff here represents a tension that has become one of the most important themes in Chinese technology and industrial policy.[359] While unfettered access to information via the Internet risks weakening the Party's grip over China, so too would completely walling the Country off from the rest of the digital world. It is widely recognized that the legitimacy of CCP rule rests largely on its continued ability to deliver economic growth.[360] Even though China has historically given greater weight to stability and security-related concerns, it still recognizes the need to delicately balance these with the goals of economic modernization and the development of its technology sector. President Xi Jinping has characterized these two sets of oft-conflicting priorities as "two wings of a bird."[361] There is thus little reason to believe China would abruptly change course and become willing to completely sacrifice one such wing in favor of the other. This is precisely what it would be doing by splintering from the global Internet in favor of an isolated, authoritarian alternative.

---

357. *See* Erie & Streinz, *supra* note 71, at 48; UNCTAD Report, *supra* note 354, at 112.

358. Henry Farrell & Abe Newman, *Weaponized Interdependence: How Global Economic Networks Shape State Coercion*, 44 INT'L SEC. 42, 45 (2019) (referring to the leverage possessed by states that are the "hubs" of asymmetric economic and technological networks as "weaponized interdependence").

359. *See, e.g.*, Creemers, *China's Conception of Cyber Sovereignty*, *supra* note 93, at 107.

360. *See, e.g.*, G. John Ikenberry, *The Rise of China and the Future of the West*, 87 FOREIGN AFFS. 23, 32 (2008) ("State power today is ultimately based on sustained economic growth, and China is well aware that no major state can modernize without integrating into the globalized capitalist system."); Joseph S Nye Jr., *Power and Interdependence with China*, WASH. Q., Jan. 2020, at 7, 12 ("The legitimacy of the Chinese Communist Party depends heavily upon economic growth, and Chinese economic growth increasingly depends upon the internet.").

361. *Xi Jinping leads Internet security group*, XINHUA (Feb. 27, 2014), https://www.chinadaily.com.cn/china/2014-02/27/content17311358.htm [https://perma.cc/3WE6-WJC2].

VII. CONCLUSION

China is an authoritarian-leaning country with a substandard human rights record. It engages in widespread surveillance and censorship of its citizens in both the physical world and, as illustrated in Part III, the digital one. Its idealized version of the Internet technical architecture—if re-designing it from scratch without costs or other constraints were possible—likely looks different from what is currently in place. It may even reflect and reinforce values most would deem repressive.

However, this does not necessarily mean every technology or technical standard originating from China is aimed at advancing these values. The New IP proposal, though questionable in both its technical merits and practicality, was not necessarily a trojan horse intended to expand state control of the Internet or embed authoritarianism into its architecture. Parts of the proposal raise legitimate concerns, namely its intrinsic security features, but these do not appear to be an integral part of New IP and should not be mistaken for its true aim. Instead, China has spent the last decade heavily investing in and promoting innovation into the exact type of future network capabilities proposed by New IP in order to support its long-term industrial policy objectives. Likely recognizing that such capabilities strongly aligned with its business interests—particularly the capabilities demanded by future business-critical industrial use cases like deterministic QoS—Huawei simply seized the opportunity being dangled in front of it.

It is important to recognize that New IP may be only the beginning of China's push for evolution of the Internet's technical architecture. Contrary to some predictions, this trend is not a harbinger of an impending Chinese-led "splinternet." Quite the opposite, in fact, as China has been promoting increased involvement at traditional Internet standards bodies like the IETF. This should come as no surprise; it would be naïve to expect the country with the most Internet users and a rapidly growing ICT sector to sit idly by while others continue to shape such vital technologies.

The way stakeholders and policymakers respond to this trend will have significant implications for U.S. technological leadership in the business arena. Some have called for building coalitions to counter Chinese influence at places like the ITU as well as for an increased governmental role in coordinating U.S. contributions at international standards bodies to increase competitiveness relative to China.[362] These approaches are unlikely to succeed and may even harm the model of standards development that made the Internet a historic success. While important to keep a watchful eye on ITU-T, resources would be better spent in pushing to scale down the sector

362. *See supra* note 18; *see also* Brett Schaefer & Danielle Pletka, *Countering China's Growing Influence at the International Telecommunication Union*, HERITAGE FOUND. (Mar. 7, 2022), https://www.heritage.org/global-politics/report/countering-chinas-growing-influence-the-international-telecommunication [https://perma.cc/5EZ6-X89F]; *see also, e.g.*, U.S.-CHINA ECON. & SEC. REV. COMM'N, 2020 REPORT TO CONGRESS 537 (Dec. 2020), https://www.uscc.gov/sites/default/files/2020-12/2020_Annual_Report_to_Congress.pdf [https://perma.cc/6ND3-8P8K].

and the many study groups whose work is duplicative, receives little attention in the marketplace, and/or falls outside the ITU's expert remit.

Just as importantly, Chinese actors are going to be increasingly active at primarily industry-led venues such as the IETF, and not every proposal they bring to the table has an ulterior motive beyond the obvious commercial incentives. Instead of trying to orchestrate a unified front for combatting China's growing role, a more constructive response for policymakers would be to increase their focus on targeted investment and policies that promote U.S. participation at these venues and cultivate the type of innovation that naturally translates to standards competitiveness. This is the surest way to see that system by which Internet standards have historically been developed, and the United States' leadership thereof, are both preserved going forward.

Amazon's Acquisition of One Medical: The Lack of Health Data Regulation in the Age of Big Tech

Angela M. Gasca*

TABLE OF CONTENTS

* J.D., May 2024, The George Washington University Law School; B.A. in Studio Art and English Literature, Goucher College, 2014. The Author expresses sincere gratitude to Professor Meredith Rose for her generous guidance and thoughtful editorial support. Special appreciation is also extended to the FCLJ staff for their assistance in the publication of this piece. This Note is dedicated to the memory of Angelo C. Gasca and Aurora T. Gasca. All views expressed are the Author's own, as are any errors.

I. INTRODUCTION

On July 21, 2022, Amazon—the behemoth one-stop e-shop that can ship everything and anything to your doorstep—entered into an agreement to acquire One Medical, a membership-based healthcare provider.[1] Seven months later, on February 22, 2023, the acquisition was completed.[2] A friend, who had joined One Medical about a year prior to this announcement and had appreciated the primary care model One Medical provided, expressed concern over the tech giant's acquisition: "If Amazon has access to my health information, I'm not keeping my membership." Whether Amazon indeed has access to their patient health data is a valid concern, as patient health information is one of the most private forms of data.[3]

Amazon and One Medical claim that patient data in their possession is handled in compliance with the Health Insurance Portability and Accountability Act (HIPAA), but this statement is misleading.[4] An early account of Amazon's history notes how Amazon found a loophole to get around book distributor requirements that threatened the fledgling company's viability.[5] It appears history is repeating itself because others—U.S. Senator Amy Klobuchar and the Federal Trade Commission (FTC) included—also think this statement is misleading.[6] Amazon is a company with a "passion for invention" that, as evidenced by its business model, clearly comprehends the

1. *See* Press Release, *Amazon and One Medical Sign an Agreement for Amazon to Acquire One Medical*, AMAZON (July 21, 2022), https://press.aboutamazon.com/2022/7/amazon-and-one-medical-sign-an-agreement-for-amazon-to-acquire-one-medical [https://perma.cc/4GAR-LQJM].

2. *See* Press Release, *One Medical Joins Amazon to Make It Easier for People to Get and Stay Healthier*, ONE MEDICAL (Feb. 22, 2023), https://www.onemedical.com/mediacenter/one-medical-joins-amazon/ [https://perma.cc/3EP2-AS9E].

3. *See* Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data*, FED. TRADE COMM'N (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal [https://perma.cc/KL5W-EQQN].

4. *See* Geoffrey A. Fowler, *Amazon Just Bought My Doctor's Office. That Makes Me Very Nervous*, WASH. POST (July 22, 2022, 6:00 AM), https://www.washingtonpost.com/technology/2022/07/22/amazon-one-medical-privacy/ [https://perma.cc/7UVZ-D4XN].

5. *See* Avery Hartmans, *Jeff Bezos Originally Wanted to Name Amazon 'Cadabra,' and 14 Other Little-Known Facts About the Early Days of the e-Commerce Giant*, BUS. INSIDER (last updated July 2, 2021, 2:42 PM), https://www.businessinsider.com/jeff-bezos-amazon-history-facts-2017-4#an-obscure-book-about-lichens-saved-amazon-from-going-bankrupt-3 [https://perma.cc/AT25-65FB].

6. *See* Press Release, *Klobuchar Urges Federal Trade Commission to Investigate Amazon's Proposed Acquisition of One Medical*, OFF. OF U.S. SEN. AMY KLOBUCHAR (July 21, 2022), https://www.klobuchar.senate.gov/public/index.cfm/news-releases?ID=54F73C9C-F713-44A9-B33E-07E61F551DF2 [https://perma.cc/S57S-YFFL]; *see also* Dave Muoio, *Amazon's $3.9B One Medical Purchase is Being Reviewed by FTC, Filings Show*, FIERCE HEALTHCARE (Sept. 6, 2022, 11:05 AM), https://www.fiercehealthcare.com/health-tech/amazons-39b-one-medical-purchase-being-reviewed-ftc-filings-show [https://perma.cc/R49W-UZ35].

value of data to drive their business forward.[7] Thus, there is a risk that Amazon will capitalize on customer health data.[8]

If major technology firms want to enter the healthcare sector, then, at a minimum, patient-consumers should know how their data is being handled and should be given the opportunity to control some aspects of its use. Current HIPAA regulations do not provide adequate protection for patient health information in the hands of major tech companies. There are too many gaps that allow for the disclosure of patient health information. When drafted, HIPAA likely did not envision a world where powerful e-commerce companies would enter the healthcare space. The pressing issue, among other concerns, is not only about who has access to this information but what is done with that information once access is acquired.

With Amazon nudging its way into sectors outside of e-commerce, the effects of major tech firms' acquisitions and the protection and regulation of consumer data need greater attention, specifically in the context of sensitive health data. The principal concern with Amazon's acquisition of One Medical is that sensitive health information was acquired—without any notice or consent from the patients to whom the data belongs—and is subsequently being converted into revenue-generating data fueling Amazon's growth.[9]

Protection and regulation of patient health information cannot be viewed solely through the lens of HIPAA. Nor is HIPAA reform the solution. One approach to protecting sensitive health data acquired through mergers and acquisitions would be to regulate at entry. Provisions in existing laws—namely the Hart-Scott-Rodino Act and the California Consumer Privacy Act—may prove adequate to regulate and protect the use of patient health data obtained through tech company mergers.

This Note begins with a brief background on Amazon, One Medical, and the heightened sensitivity to information disclosure in the healthcare space. In Section III, this Note will discuss how data collected by One Medical (and other technology firms) falls outside the scope of HIPAA regulation and how the FTC's Section 5 authority can address these gaps. Section IV will look at the Hart-Scott-Rodino Act and the California Consumer Privacy Act as existing tools for regulating sensitive health data. Finally, Section V will discuss how the FTC's Section 5 authority, the Hart-Scott-Rodino Act, and elements from the California Consumer Privacy Act could be used at the pre-merger stage to regulate health data acquired by non-clinical entities through mergers and acquisitions.

---

7. *See Amazon and One Medical Sign an Agreement for Amazon to Acquire One Medical*, *supra* note 1.

8. *See* Fowler, *supra* note 4.

9. *See Klobuchar Urges Federal Trade Commission to Investigate Amazon's Proposed Acquisition of One Medical*, *supra* note 6.

II. BACKGROUND

A. The Giant Called Amazon

Amazon began in 1994, selling books out of Jeff Bezos' garage.[10] Nearly thirty years later, Amazon is the fifth most valuable company in the world with a market capitalization near $1.5 trillion USD.[11] Amazon is a member of the "big five" tech companies, along with Apple, Alphabet, Microsoft, and Meta.[12]

The list of Amazon's acquisitions is long. Highlights include the $930 million acquisition of online shoe retailer Zappos (2009), the $13.7 billion acquisition of Whole Foods (2017), and the subsequent pivot to big-screen entertainment with the $8.45 billion purchase of Metro-Goldwyn-Mayer (MGM) Studios (2021).[13] With each acquisition, Amazon gained access not only to customers but to more data which fuels the company's growth.[14]

Most individuals interact daily with a product or service provided by Big Tech companies.[15] We get from one place to another by using Uber or Lyft (dependent on Google Maps), watch movies on Netflix (hosted on the Amazon Web Services cloud), and use Instagram (owned by Meta) as a social and e-commerce platform.[16] Healthcare is the one area where Big Tech's presence has not felt quite as pervasive. While technology underlies the infrastructure of healthcare services, the ways in which we receive care and interact with providers remain largely traditional—Amazon's entrance into the healthcare space could change this. The acquisition of One Medical gives Amazon a new type of data to collect, probe, and capitalize on. As Senator Klobuchar stated in her letter to the FTC, the "proposed deal could result in the accumulation of highly sensitive personal health data in the hands of an already data-intensive company."[17] As data-driven companies (Amazon included) use data to push growth in their healthcare services offerings,

---

10. *See* Hartmans, *supra* note 5.

11. *See The 100 Largest Companies in the World by Market Capitalization in 2022*, STATISTA, https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/ [https://perma.cc/4JAT-MH2J] (last visited Nov. 14, 2022).

12. *See* Conor Sen, *The 'Big Five' Could Destroy the Tech Ecosystem*, BLOOMBERG (Nov. 15, 2017, 11:00 AM), https://www.bloomberg.com/opinion/articles/2017-11-15/the-big-five-could-destroy-the-tech-ecosystem [https://perma.cc/S9KP-EQB6].

13. *See* Stacy Mitchell & Olivia LaVecchia, *Amazon's Stranglehold: How the Company's Tightening Grip on the Economy Is Stifling Competition, Eroding Jobs, and Threatening Communities*, INST. FOR LOC. SELF-RELIANCE (Nov. 29, 2016), https://ilsr.org/amazon-stranglehold/ [https://perma.cc/23C2-67YT]; *Amazon's Major Acquisitions Over the Years*, REUTERS (May 26, 2021, 10:16 AM), https://www.reuters.com/technology/amazons-major-acquisitions-over-years-2021-05-26/ [https://perma.cc/GG3D-K4ZK].

14. *See* Elma Mrkonjić, *How Amazon Uses Big Data*, SEEDSCIENTIFIC (Aug. 29, 2022), https://seedscientific.com/how-amazon-uses-big-data/ [https://perma.cc/4622-ACCG].

15. *See* Kashmir Hill, *I Tried to Live Without the Tech Giants. It Was Impossible*, N.Y. TIMES (July 31, 2020), https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html [https://perma.cc/C35J-MZMT].

16. *Id.*

17. *See Klobuchar Urges Federal Trade Commission to Investigate Amazon's Proposed Acquisition of One Medical*, *supra* note 6.

sensitive data gleaned from patient-consumers needs sufficient regulatory protection because patients face risks if their data is compromised or misused.

B. One Medical—The "Starbucks of Primary Care"

Physician and entrepreneur Tom Lee founded One Medical in 2007.[18] Dr. Lee's mission was to use a technology-based infrastructure to create efficient delivery of primary care services.[19] Based in San Francisco, the single-office healthcare startup now has offices in over twenty major U.S. cities.[20] The One Medical model differs from other primary care providers in that it is membership-based; that is, patients pay a membership fee to have access to One Medical care and all the perks that accompany a yearly subscription.[21] Member benefits include 24/7 access to virtual care, in-office lab services, and efficient appointment scheduling via the One Medical app, as well as in-app prescription management.[22] An investor in One Medical described the company as the "Starbucks of primary care."[23]

Amazon's proposed acquisition of One Medical was announced on July 21, 2022,[24] and was completed on February 22, 2023.[25] In 2022, One Medical reported 836,000 total members.[26] In addition to having a substantial membership count and a unique "pay for care" model, the company also "built its own medical records technology from the ground up to help doctors

---

18. *See* Christina Farr, *How Tech-Infused Primary Care Centers Turned One Medical into a $2 Billion Business*, CNBC TECH (July 28, 2019, 9:56 AM), https://www.cnbc.com/2019/07/28/one-medical-opening-primary-clinics-in-portland-and-atlanta.html [https://perma.cc/C2FR-HKF8].

19. *See* Tom Taulli, *One Medical: Playbook to Disrupt the Massive Healthcare Industry*, FORBES (Feb. 1, 2020, 1:58 PM), https://www.forbes.com/sites/tomtaulli/2020/02/01/one-medical-playbook-to-disrupt-the-massive-healthcare-industry/?sh=1f52608867a2 [https://perma.cc/766A-AGZC].

20. *See Locations,* ONE MEDICAL, https://www.onemedical.com/ [https://perma.cc/6SHY-ZJAP] (last visited Jan. 16, 2023).

21. Currently, One Medical membership costs $199 per year, but the company does provide membership alternatives for those with financial hardships. *See Membership*, ONE MEDICAL, https://www.onemedical.com/membership/ [https://perma.cc/R56K-KUCT] (last visited Jan. 16, 2023).

22. *Id.*

23. Farr, *supra* note 18.

24. *See Amazon and One Medical Sign an Agreement for Amazon to Acquire One Medical*, *supra* note 1.

25. *See One Medical Joins Amazon to Make It Easier for People to Get and Stay Healthier*, *supra* note 2. The acquisition was finalized after the FTC said "it would not challenge the purchase." However, an FTC spokesperson stated the investigation of "Amazon's acquisition of One Medical continues" due to the "possible harms to consumers that may result from Amazon's control and use of sensitive consumer health information held by One Medical" as a core reason for continuing their investigation. *See* Brian Fung, *Amazon closes $3.9 Billion Deal to Acquire One Medical*, CNN BUS. (Feb. 22, 2023, 2:13 PM), https://edition.cnn.com/2023/02/22/tech/ftc-amazon-one-medical-deal/index.html [https://perma.cc/C5TE-538A].

26. *See One Medical Announces Results for Fourth Quarter and Full year 2022*, GLOBALNEWSWIRE (Feb. 21, 2023, 5:53 PM) https://www.globenewswire.com/en/news-release/2023/02/21/2612770/0/en/One-Medical-Announces-Results-for-Fourth-Quarter-and-Full-Year-2022.html [https://perma.cc/R7HT-LWDG].

manage patient relationships" instead of relying on third-party medical record software systems.[27]

The acquisition of One Medical aligns with Amazon's other acquisitions in terms of existing customer bases absorbed, services offered, product delivery, and most importantly, proprietary technology acquired.[28] Notably, this was not Amazon's first foray into the health services industry; in 2018 it acquired PillPack, a "full-service [online] pharmacy."[29] The general consensus for the PillPack acquisition was that it "is just a piece of Amazon's expansive plan to uproot the $3 trillion U.S. health-care industry."[30] Acquiring One Medical brings Amazon one step closer to realizing that plan.

C. Healthcare is a Trusted Space

The way healthcare is delivered in the U.S. is far from efficient. A host of factors influence a patient's level of care.[31] One Medical's founder (who had left the company by the time of the acquisition) commented that "healthcare . . . is a private, personal, trusted space."[32] Dr. Lee went on to say that some patients will accept the idea of a "non-clinical entity" overseeing this trusted space, while others will not. In other words, there is an inherent tension in trusting a non-clinical entity to properly handle sensitive medical information such as family clinical history, medical diagnostics, and digital appointment notes and care summaries.

A paper published by the American Economic Liberties Project notes that "Amazon's power is not primarily based on providing a better set of products or services, but on *exploiting gap*s in antitrust, tax, *privacy* or other forms of law to acquire a continual set of competitive advantages."[33] One journalist reporting on the proposed acquisition has found that "lots of companies find completely legal ways to grab intimate health data for

---

27. Farr, *supra* note 18.

28. *See* Daniela Coppola, *Amazon Prime – Statistics & Facts*, STATISTA (Nov. 17, 2022), https://www.statista.com/topics/4076/amazon-prime/#topicHeader__wrapper [https://perma.cc/7G4A-QRDJ].

29. Christina Farr, *The Inside Story of Why Amazon Bought PillPack in its Effort to Crack the $500 Billion Prescription Market*, CNBC TECH (May 10, 2019, 2:40 PM), https://www.cnbc.com/2019/05/10/why-amazon-bought-pillpack-for-753-million-and-what-happens-next.html [https://perma.cc/D76S-4ETP]; PILLPACK, https://www.pillpack.com/ [https://perma.cc/UUK3-97JE] (last visited Jan. 16, 2023).

30. Farr, *supra* note 18.

31. Factors that affect levels of access to healthcare include inadequate health insurance coverage, limited access to public transportation, and limited resources to receive specialized care. For further information on this point, *see Access to Health Services*, U.S. DEPT. OF HEALTH & HUM. SERVS., https://health.gov/healthypeople/priority-areas/social-determinants-health/literature-summaries/access-health-services [https://perma.cc/3FSD-Q9QM] (last visited Mar. 4, 2023).

32. *Interview by Jeremy Corr and Dr. Robert Pearl with Dr. Tom Lee, CEO*, GALILEO (Aug. 30, 2022), https://www.fixinghealthcarepodcast.com/wp-content/uploads/2022/08/Fixing-Healthcare-Transcript_Tom-Lee_Episode-63.pdf [https://perma.cc/8Y6H-XQ6R].

33. Matt Stoller et al., *Understanding Amazon: Making the 21st-Century Gatekeeper Safe for Democracy*, AM. ECON. LIBERTIES PROJECT (July 24, 2020) (emphasis added), https://www.economicliberties.us/our-work/understanding-amazon-making-the-21st-century-gatekeeper-safe-for-democracy/#_ftn4 [https://perma.cc/GEG8-NWE8].

marketing and other purposes with 'consent' few patients realized they were giving."[34] Even though an Amazon spokesperson stated the company "will never share One Medical customers' personal health information outside of One Medical . . . without clear permission from the customer,"[35] Amazon's reputation for coloring outside the lines is well-established.[36] The lack of direct notice to existing One Medical members regarding the proposed merger raises another red flag.[37] Failing to notify existing customers their primary care provider could be acquired by Amazon goes against the grain of basic procedural due process.[38]

The intentions behind the Amazon-One Medical merger could very well be aimed at "mak[ing] the health care experience more accessible, affordable, and . . . enjoyable."[39] But the fact remains that Amazon—a company with an unprecedented amount of customer data—will now be in possession of its customers' highly sensitive health data.[40]

III. HIPAA AND THE FTC ACT

The popular fallback for health privacy concerns is to refer to HIPAA. However, in 1996, HIPAA was not drafted with Amazon, and other similar

34. Fowler, *supra* note 4.

35. *Id.*; *see also* Stoller et al., *supra* note 33.

36. Amazon's Ring and Alexa technology have raised privacy and surveillance concerns. *See* Yael Grauer & Daniel Wroclawski, *Amazon Shared Ring Security Camera and Video Doorbell Footage with Police Without a Warrant*, CONSUMER REPS. (July 15, 2022), https://www.consumerreports.org/law-enforcement/amazon-shared-ring-footage-with-police-without-a-warrant-a6093504500/ [https://perma.cc/3TJ7-X8YA]; Geoffrey A. Fowler, *Amazon May Be Sharing Your Internet Connection with Neighbors. Here's How to Turn It Off*, WASH. POST (June 8, 2021, 11:07 AM), https://www.washingtonpost.com/technology/2021/06/07/amazon-sidewalk-network/ [https://perma.cc/4BWK-LQSF]; Geoffrey A. Fowler, *Alexa Has Been Eavesdropping on You This Whole Time*, WASH. POST (May 6, 2019, 9:00 AM), https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/ [https://perma.cc/BTZ4-7VC7].

37. *See* Ari Levy, *Amazon Already Knows a Lot About Me, But One Medical Takes It to a Whole New Level*, CNBC (July 23, 2022, 12:22 PM), https://www.cnbc.com/2022/07/23/amazon-one-medical-deal-gives-it-access-to-my-most-personal-info.html [https://perma.cc/4HAZ-NE4D]. The CEO of One Medical provided an update to existing members about the proposed transaction via a blog post eleven days after the proposed transaction was announced. *See* Amir D. Rubin, *Update from One Medical on Agreement to be Acquired by Amazon*, ONE MEDICAL (Aug. 2, 2022), https://www.onemedical.com/blog/newsworthy/update-one-medical-agreement-be-acquired-amazon/ [https://perma.cc/C36P-WKUZ].

38. *See* Mathews v. Eldridge, 424 U.S. 319, 348-49 (1976) (finding that "[t]he essence of due process is [the] requirement that a 'a person . . . be given notice . . . and [an] opportunity . . . to be heard.'") (citing Joint Anti-Fascist Comm. v. McGrath, 341 U.S. 123, 171-72 (Frankfurter, J., concurring)); *see infra* Section IV.

39. *See Amazon and One Medical Sign an Agreement for Amazon to Acquire One Medical*, *supra* note 1.

40. News of the proposed merger made current One Medical members question whether Amazon would "act in good faith with [their] health data." *See* Levy, *supra* note 37.

Big Tech companies, in mind.[41] Rather, HIPAA was initially designed to reform the health insurance market.[42] It was revised in 2002 to include the HIPAA Privacy Rule, which addressed gaps in the regulation of health information known as protected health information (PHI).[43] The Privacy Rule set out national standards for health care entities to abide by when handling sensitive health information.[44] In 2005, the HIPAA Security Rule was added to include the national standards for the protection of electronic patient health information held by, or transferred to, HIPAA covered entities, which include "health plans, health care clearinghouses, and . . . any health care provider."[45] Then in 2013, the U.S. Department of Health and Human Services (HHS) implemented the HIPAA Omnibus Rule which incorporated provisions from the Health Information Technology for Economic and Clinical Health Act (HITECH), which was signed into law four years prior.[46] The goal of implementing HITECH was to "promote the adoption and meaningful use of health information technology."[47] In other words, HITECH was introduced to push the use of electronic health records (EHR), and thus, spur technological innovation in the health services industry via financial incentives at a time when the American economy needed a financial boost.[48]

When HITECH was introduced in 2009, it strengthened existing HIPAA privacy and security provisions and focused on healthcare providers

41. *See* Press Release, *Statement of Commissioner Alvaro M. Bedoya Joined by Commissioner Rebecca Kelly Slaughter Regarding Amazon.com, Inc.'s Acquisition of 1Life Healthcare, Inc.*, FED. TRADE COMM'N (Feb. 27, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2210191amazononemedicalambstmt.pdf [https://perma.cc/AH7U-KDEK].

42. *See* S. REP. NO. 104-156, at 1-3 (1995), https://www.govinfo.gov/content/pkg/CRPT-104srpt156/pdf/CRPT-104srpt156.pdf [https://perma.cc/48M8-MM9T].

43. Protected Health Information is defined as "individually identifiable health information" related to the physical or mental condition of an individual, the care provided to the individual, and information related to the payment of care. *See generally Summary of the HIPAA Privacy Rule*, U.S. DEPT. OF HEALTH & HUM. SERVS. (last updated Oct. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html [https://perma.cc/E6JJ-2X9B].

44. *Id.*

45. *See Brief History of HIPAA and the Privacy Rule, in* BEYOND THE HIPPA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 63-64 (Sharyl J. Nass et al. eds., 2009), https://nap.nationalacademies.org/catalog/12458/beyond-the-hipaa-privacy-rule-enhancing-privacy-improving-health-through [https://perma.cc/D3MT-WMZD]; *see also Summary of the HIPAA Security Rule*, U.S. DEPT. OF HEALTH & HUM. SERVS. (last updated Oct. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html [https://perma.cc/JB6L-5RXE].

46. *See Omnibus HIPAA Rulemaking*, U.S. DEPT. OF HEALTH & HUM. SERVS. (last updated Sept. 13, 2019), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/omnibus-hipaa-rulemaking/index.html [https://perma.cc/83TE-3NW7]; *HITECH Act Enforcement Interim Final Rule*, U.S. DEPT. OF HEALTH & HUM. SERVS. (last updated June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html [https://perma.cc/LFV8-AJ7U].

47. *HITECH Act Enforcement Interim Final Rule*, *supra*, note 46.

48. *See* Howard Burde, *The HITECH Act—An Overview*, 13 AM. MED. ASSOC. J. OF ETHICS 172-75 (2011), https://journalofethics.ama-assn.org/article/hitech-act-overview/2011-03 [https://perma.cc/W38D-3XCJ].

looking to adopt new technology to bolster patient services.[49] Amazon acquiring One Medical flips this model around; Amazon has now tacked on a pre-built healthcare service to the menu of products and services offered to its customers.[50] Combining the strengths of Amazon with the One Medical model to streamline the patient experience and improve the delivery of healthcare services for those who can access care in this manner is not, in and of itself, a bad concept.[51] The data driving the innovation,[52] and the apparent lack of regulation over this data, are the cause for concern.

A. Loopholes Within the Law

Despite the revisions to HIPAA, the law as it exists today does not adequately protect or regulate patient health information in the context of a non-clinical entity subsuming a provider of health care services. The HIPAA Privacy Rule concerns itself with protection of PHI used by covered entities.[53] One Medical is a covered entity under HIPAA but attempts to circumvent the law through language in its privacy notices.[54] The One Medical HIPAA Privacy Policy states the company may disclose a patient's protected health information *without authorization* to support "Healthcare Operations."[55] This broad characterization is defined as: "[t]o administer and support [One Medical's] *business activities* . . . [f]or example (and without limitation), [One

49. *See* 45 C.F.R. pt. 160, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf [https://perma.cc/43W6-JT62]; *see also HITECH Act Enforcement Interim Final Rule*, *supra* note 46.

50. *See A Letter from Amazon's CEO, Amazon Welcomes One Medical*, AMAZON, https://www.amazon.com/welcomeomletter/b?node=86386266011[https://perma.cc/Y893-V3SQ] (last visited Apr. 8, 2023).

51. *See Amazon and One Medical Sign an Agreement for Amazon to Acquire One Medical*, *supra* note 1.

52. Amazon's parallel acquisition of iRobot (also under FTC investigation) is another proposed purchase that further illustrates the company's eagerness to collect consumer data to feed the ever-growing Amazon machine. *See* Josh Sisco, *FTC Digs in on Amazon's iRobot Deal*, POLITICO (Sept. 2, 2022, 7:55 PM), https://www.politico.com/news/2022/09/02/amazons-ftc-problem-keeps-growing-with-irobot-one-medical-probes-00054749 [https://perma.cc/A6AR-Q2AK].

53. *See Your Rights Under HIPAA*, U.S. DEPT. OF HEALTH & HUM. SERVS. (last updated Jan.19, 2022), https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html#:~:text=We%20call%20the%20entities%20that%20must%20follow%20the%20HIPAA%20regulations%20%22covered%20entities.%22 [https://perma.cc/2RY2-5JDT]. A covered entity under 45 CFR § 160.103 includes "a health plan, a health care clearinghouse, a health care provider who transmits any health information in electronic form in connection with a transaction covered" under Title 45. Covered entities can engage with business associates, which includes health information organizations, subcontractors, and other individuals who "provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information." *Covered Entities and Business Associates*, U.S. DEPT. OF HEALTH & HUM. SERVS. (last updated June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html [https://perma.cc/NX5Q-ZF27].

54. *See Notice of HIPAA Privacy Practices*, ONE MEDICAL (last updated Oct. 17, 2022), https://www.onemedical.com/hipaa/ [https://perma.cc/4R6Q-PEKC]; *see also 1Life Healthcare Inc. Privacy Policy*, ONE MEDICAL (last updated Nov. 3, 2022), https://www.onemedical.com/privacy/ [https://perma.cc/87UG-HK23].

55. *Id.*

Medical] may use [a patient's] PHI to conduct quality analysis, data aggregation, review and improve our services and the care [patients] receive and to provide training."[56] The broad language used here signals patient health information is already being used by One Medical in a manner that is beyond the reach of HIPAA protection.

With the announcement of the completed merger, One Medical and Amazon released a statement where they noted HIPAA "governs what One Medical, *Amazon, and others* can do with Protected Health Information . . . information like medication history, medical conditions, and treatment information."[57] This language implies that Amazon sees itself not as a covered entity, but as a "business associate" which now has access to protected health information generated by a covered entity.[58] While the "business associate" designation grants access, and One Medical's current HIPAA Privacy Policy uses broad language that technically still covers patient health information and data under HIPAA, it's important to note that coverage does not equal responsible regulation.

B. Big Tech Data Collection—Beyond the Scope of HIPAA

Health information generated within a clinical entity is confined by HIPAA privacy provisions and treated differently than health information created outside of a traditional medical environment. Personal health data generated by Amazon customers, and by Big Tech users in general, falls outside the scope of HIPAA protection.[59] For example, when individuals use Amazon to purchase allergy medicine, pregnancy tests, or other health-related products, those interactions are not covered by HIPAA, and Amazon can use these data points to expand its business in the health services space.[60] In addition, Amazon's access to this information provides insight into a customer's demographic profile, which can influence how Amazon markets health products to customers.[61] The type of data collected is health related but is customer generated and not created or provided within a clinical entity under HIPAA purview.[62]

---

56. *Id.*

57. *See One Medical Joins Amazon to Make It Easier for People to Get and Stay Healthier*, *supra* note 2.

58. *See* 45 C.F.R. § 160.103 (2019); *see also Covered Entities and Business Associates*, *supra* note 53.

59. *See* Health Breach Notification Rule, 16 C.F.R. § 318 (2009), https://www.ftc.gov/legal-library/browse/federal-register-notices/health-breach-notification-rule-final-rule [https://perma.cc/9HBR-458Q] ("[Some] web-based entities that collect consumers' health information . . . are not subject to the existing privacy and security requirements of the Health Insurance Portability and Accountability Act.").

60. *See* Ryan Mueller, *Big Data, Big Gap: Working Towards a HIPAA Framework that Covers Big Data*, 97 IND. L. J., 1505, 1516-17 (2022).

61. Professor Barbara Kahn acknowledges the influence of customer insights acquired from data interactions and how those interactions influence "selling all types of different services and content" to customers. *See Is Amazon Getting Too Big?*, KNOWLEDGE AT WHARTON (May 20, 2019), https://knowledge.wharton.upenn.edu/article/amazon-too-big/ [https://perma.cc/K3W7-66ZZ].

62. *See* Cohen, *supra* note 3.

C. Where HIPAA Falls Short, the FTC Act Steps in

Recognizing the gap in regulation over this type of user-generated health data, the HHS Office of Civil Rights, in conjunction with the FTC, issued a report in 2016 on the "gaps in oversight between HIPAA-covered entities that collect health data from individuals and those that are not regulated by HIPAA."[63] As affirmed in the HHS report, the FTC Act is currently "the primary federal statute applicable to the privacy and security practices of businesses that collect health information where those entities are not covered by HIPAA."[64] Thus, where HIPAA falls short, Section 5 of the FTC Act and the Health Breach Notification Rule provide gap fillers.[65] Section 5 of the FTC Act specifically prohibits "unfair methods of competition" and "unfair or deceptive acts or practices in or affecting commerce."[66] Thus, when tech companies issue privacy policies promising non-disclosure of sensitive health information but violate those policies, the FTC can step in and enforce their authority over these "deceptive acts or practices" under Section 5.

For example, the Federal Trade Commission recently issued a complaint against Flo Health, a reproductive health app, for the misuse of their users' sensitive health information and for privacy misrepresentations.[67] The company had claimed since 2016 that sensitive user information would not be disclosed to third parties, and only certain tech companies (specifically, Facebook(now Meta), Google, and Fabric) would receive anonymized data.[68] Then in 2019, the Wall Street Journal published an article revealing how Flo Health shared its users' *identifiable* information with Facebook "for its own research and development purposes."[69] In January 2021, Flo Health came to a settlement with the FTC and agreed to notify users of the privacy breach; receive consent from all users prior to sharing their health information moving forward; and conduct a review of all internal privacy practices.[70]

As evidenced above, Section 5 authority provides some regulation over misuse of sensitive health information for entities not covered by the HIPAA umbrella. One drawback to Section 5 authority, however, is timing.

---

63. Dr. Karen B. De Salvo & Jocelyn Samuels, *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated By HIPAA*, HEALTH IT BUZZ (June 19, 2016), https://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/examining-oversight-privacy-security-health-data-collected-entities-not-regulated-hipaa/ [https://perma.cc/8SFB-LK6L].

64. *Id.*

65. *Id.*; *see also* Health Breach Notification Rule, *supra* note 59.

66. 15 U.S.C. § 45 (2006).

67. *See* Complaint, In the Matter of Flo Health, Inc., FTC Docket No. C-4747 (June 17, 2021), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf [https://perma.cc/984Z-NFR8].

68. *Id.* at 3.

69. *Id.* at 5.

70. *See* Press Release, *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others*, FED. TRADE COMM'N (June 22, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google [https://perma.cc/6RZT-UNNG].

Generally, Section 5 enforcement is reactive, coming after a violation. Section 5 authority provides a capable defense when an unfair or deceptive practice is uncovered. But what about the need for prophylactic measures? That is, can the FTC use its "extensive data protection enforcement authority" to implement a privacy regulation over sensitive health data acquired at the pre-merger stage?[71] Given the FTC is currently the "established . . . U.S. data protection authority," this Note contends the FTC should exercise its "enforcement powers" to fill this regulatory gap at the pre-merger stage, specifically for non-clinical entities acquiring sensitive health data from healthcare entities.[72]

IV. U.S. PRIVACY LAW AND ANTITRUST LAW

The General Data Protection Regulation (GDPR) is the EU's comprehensive data security and privacy law, but unlike the EU, the U.S. does not have a federal data privacy law in place.[73] Instead, there are privacy acts regulating various discrete types of information, a few being data housed within government agencies, personal financial information held by financial institutions, data collected from users under the age of thirteen, and as discussed *supra* Section III, health information used by healthcare and health insurance entities.[74] The amalgam of various privacy laws "leave[s] consumers vulnerable to privacy harms."[75]

Only three states have passed consumer privacy laws: California, Colorado, and Virginia, with California's law being the most robust.[76] The California Consumer Privacy Act (CCPA) provides consumers with broad rights regarding the protection of their personal data, and imposes data security obligations on businesses.[77] The Virginia Consumer Data Protection Act (VCDPA) provides, "consumers the right to access their personal data and request that it be deleted by businesses."[78] However, unlike the CCPA,

---

71. Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2246 (2015).

72. *Id.* at 2266; *see also Statement of Commissioner Alvaro M. Bedoya Joined by Commissioner Rebecca Kelly Slaughter Regarding Amazon.com, Inc.'s Acquisition of 1Life Healthcare, Inc*, *supra* note 41.

73. Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES: WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/T2NZ-5RP3].

74. *See* The Privacy Act of 1974, 5 U.S.C. § 552a; Gramm-Leach-Bliley Act, 15 U.S.C. 6801; Children's Online Privacy Protection Rule, 15 U.S.C. §§ 6501-6505; Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (1996).

75. *See* Hartzog & Solove, *supra* note 71, at 2266.

76. *See* Klosowski, *supra* note 73.

77. *See* California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100-1798.199 (West 2023); *see also* Klosowski, *supra* note 73.

78. *What Is the Virginia Consumer Data Protection Act (VCDPA)?*, BLOOMBERG L. (Dec. 28, 2022), https://pro.bloomberglaw.com/brief/what-is-the-vcdpa/#:~:text=CCPAVCDPA%20Ambiguities-,What%20is%20the%20Virginia%20Consumer%20Data%20Protection%20Act%20(VCDPA)%3F,targeted%20advertising%20and%20sales%20purposes [https://perma.cc/86U6-VAUG].

the VCDPA leans heavily towards placating the needs of large tech companies, and this is not by accident.[79] Despite differences in the two state privacy acts, they are examples of privacy regulation taking shape.

U.S. laws governing the use of data belonging to most U.S. consumers provide inadequate protection and regulation. The current federal agency that is best positioned to be "the leading regulator of privacy" remains the FTC.[80] Established in 1914, the FTC's purpose is to protect consumers from unfair methods of competition, unfair or deceptive acts or practices, and to prevent the concentration of power, thereby preserving competition in the markets.[81] As discussed above, Section 5 of the FTC Act gives the FTC jurisdiction to pursue data security enforcement actions, and although "modest" in cases pursued, the FTC has established its authority as "being the U.S. data protection authority."[82]

A. Consider the Data

In addition to the FTC Act, the other principal antitrust laws are the Sherman Act, the Clayton Act, the Robinson-Patman Act, and the Hart-Scott-Rodino Act. The earliest U.S. antitrust law, the Sherman Act of 1890, prohibits contracts in restraint of trade and conduct by a single entity that unreasonably restrains competition by creating or maintaining monopoly power.[83] The Clayton Act, introduced in 1914, prohibits mergers and acquisitions where the effect of the merger may substantially lessen competition or tends to create a monopoly.[84] In 1936, the Robinson-Patman Act was enacted to prohibit price discrimination on the part of large buyers.[85]

Then, in 1976, the Hart-Scott-Rodino Antitrust Improvements Act (HSR Act) was passed to implement a "federal premerger notification program, which provides the FTC and the Department of Justice with

79. The "first cut" of the state privacy bill was presented to Virginia Senator David Marsden by a lobbyist for Amazon, and other major tech and financial institutions were eager "to have a hand in shaping the legislation" as well. It is not surprising Amazon, whose second headquarters are located in northern Virginia, wanted to assert its interests. However, drafting the text of state legislation once again demonstrates Amazon's tendency to push boundaries. *See* Emily Birnbaum, *From Washington to Florida, Here Are Big Tech's Biggest Threats from State*s, PROTOCOL (Feb. 19, 2021), https://www.protocol.com/policy/virginia-maryland-washington-big-tech [https://perma.cc/P5JU-QQ4C].

80. Hartzog & Solove, *supra* note 71, at 2267.

81. *See* Federal Trade Commission Act, 15. U.S.C. § 45 (2012); *see also* Marc Winerman, *The Origins of the FTC: Concentration, Cooperation, Control, and Competition*, 71 ANTITRUST L. J. 1, 2-5 (2003).

82. *See* Hartzog & Solove, *supra* note 71, at 2266; *see also* FTC Data Security Actions Tracker, Practical Law Practice Note Overview W-027-3592, https://us.practicallaw.thomsonreuters.com/w-027-3592 [https://perma.cc/3SZR-F5UA].

83. *See* Sherman Antitrust Act of 1890, 15 U.S.C. §§ 1-7; *see also* U.S. Antitrust Laws: Overview, Practical Law Practice Note Overview 9-204-0472, https://us.practicallaw.thomsonreuters.com/9-204-0472 [https://perma.cc/4PZQ-QDGH].

84. *See* Clayton Antitrust Act, 15 U.S.C. §§ 12-27; *see also* U.S. Antitrust Laws: Overview, *supra* note 83.

85. *See* Robinson-Patman-Act of 1936, 15 U.S.C. § 13(a)-(f); *see also* U.S. Antitrust Laws: Overview, *supra* note 83.

information about large mergers and acquisitions before they occur."[86] The HSR Act has a three-part jurisdictional test,[87] and companies considering mergers that meet this test must notify the FTC and Antitrust Division of the Department of Justice (DOJ) of the proposed transaction prior to finalization or face civil penalties.[88] Often, "[t]rying to undo a merger which is ultimately declared illegal is frequently compared to attempting to unscramble an egg."[89] Thus, pre-merger notification gives the relevant agencies time to identify potential antitrust violations that could result from the merger.[90] Agencies have a set waiting period during which they must conclude their review, or issue further requests for information which extends the clock.[91]

An amended version of the Hart-Scott-Rodino Act could serve to address the collection of personal data by major tech companies. The FTC's Section 5 authority over unfair and deceptive practices makes it well-positioned to assess privacy practices for data-heavy business models and the potential harms generated by mergers between data-heavy companies. Section 5 is "intentionally broad" in its language, [92] and it seems likely the FTC already considers data use in its merger reviews.[93]

---

86. *Premerger Notification Program*, FED. TRADE COMM'N: ENF'T https://www.ftc.gov/enforcement/premerger-notification-program [https://perma.cc/7RU4-X5ND] (last visited Jan. 21, 2023).

87. If no exemptions apply to a proposed transaction, then HSR reportability requirements include a commerce test, size-of-person test, and size-of-transaction test. The first requirement, the commerce test, is met if the transacting parties engage in conduct affecting commerce—this is most often easily satisfied. The size-of-transaction test is met when "a transaction's value exceeds $111.4 million," and the size-of-person test is triggered when the "size-of-transaction is greater than $111.4 million and no more than $445.5 million." Transactions over $445.5 million are automatically subject to review under the HSR Act. *See Determining Hart-Scott-Rodino Applicability*, Practical Law Practice Note 9-516-9560, https://us.practicallaw.thomsonreuters.com/9-516-9560 [https://perma.cc/C7L4-B97J] (last visited Apr. 8, 2023).

88. *See What Is the Premerger Notification Program? An Overview*, FED. TRADE COMM'N: PREMERGER NOTIFICATION OFF. (last revised Mar. 2009), https://www.ftc.gov/sites/default/files/attachments/premerger-introductory-guides/guide1.pdf [https://perma.cc/AJU7-6C67]; *see also* U.S. v. Canon Inc., No. 1:19-cv-01680-TSC, 2019 WL 5793200, at *1 (D.D.C. Oct. 8, 2019) (finding defendants acted in violation of the HSR Act and were ordered to pay a $5 million civil penalty and implement an internal HSR Act compliance program).

89. Earl W. Kintner, Joseph P. Griffin & David B. Goldston, *Hart-Scott-Rodino Antitrust Improvements Act of 1976: An Analysis*, 46 GEO. WASH. L. REV. 1, 12 (1977).

90. *See What Is the Premerger Notification Program? An Overview*, *supra* note 88, at 1.

91. *See* Lee Van Voorhis et al., *Hart-Scott-Rodino Act: Overview*, Practical Law Practice Note, https://www.westlaw.com/9-383-6234?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 [https://perma.cc/2HJU-BCBC] (last visited Jan. 27, 2023).

92. Hartzog & Solove, *supra* note 71, at 2246.

93. The FTC evaluating the use of data in mergers and acquisitions in their review for potential antitrust violations is evidenced in Senator Klobuchar's letter to the FTC urging them to "consider the role of data" as they investigated the Amazon-One Medical proposed merger. *See Klobuchar Urges Federal Trade Commission to Investigate Amazon's Proposed Acquisition of One Medical*, *supra* note 6. Further, after the transaction was completed, an FTC spokesperson stated the investigation of "Amazon's acquisition of One Medical continues" due to the "possible harms to consumers that may result from Amazon's control and use of sensitive consumer health information held by One Medical." *See* Fung, *supra* note 25.

B. The CCPA Gives Consumers More Control

An existing law that is instructive for how sensitive health data should be regulated and protected is the California Consumer Privacy Act.[94] The CCPA partially went into effect on January 1, 2020, with full enforcement beginning six months later.[95] On November 3 of that same year, voters approved to expand the law's scope.[96] The CCPA "gives consumers more control over the personal information that businesses collect about them."[97] Specifically, the CCPA gives consumers:

> The *right to know* about the personal information a business collects about them and how it is used and shared; the *right to delete* personal information collected from them (with some exceptions); the *right to opt-out* of the sale or sharing of their personal information; and the *right to non-discrimination* for exercising their CCPA rights.[98]

In addition to these four codified consumer privacy rights, the passage of Proposition 24 gave California consumers the "right to correct" incorrect personal information held by a business and the "right to limit the use and disclosure of sensitive personal information."[99] These provisions have positioned California as the "nation's de facto . . . tech and data regulator."[100] One could argue that residents of California have far greater protection over their private data than those living in the other 49 states.

One Medical's privacy policy is an example of how sensitive data is regulated under the CCPA. The policy contains a section specifically for California residents and provides patients with a summary of the "[p]ersonal information collected, the sources of collection, the business/commercial purpose for collecting or 'sharing' personal information, and the categories of third parties to whom [One Medical] discloses Personal Information."[101] In addition, the company makes both a "right to know" and "right to deletion" request form available to California patients as obligated under California

---

94. *See* Cal. Civ. Code § 1798.100 (West 2020).

95. *See* Maria Korolov, *California Consumer Privacy Act (CCPA): What You Need to Know to be Compliant*, CSO ONLINE (July 7, 2020), https://www.csoonline.com/article/565923/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html [https://perma.cc/9VLT-3VHD].

96. *CPPA Releases New Modified Proposed CPRA Regulations*, HUNTON PRIV. BLOG (Nov. 7, 2022), https://www.huntonprivacyblog.com/2022/11/07/cppa-releases-new-modified-proposed-cpra-regulations/ [https://perma.cc/DZU2-BXLY].

97. *California Consumer Privacy Act*, OFF. OF THE CAL. ATT'Y GEN. (last updated on Jan. 20. 2023), https://oag.ca.gov/privacy/ccpa [https://perma.cc/T7QE-3QBG].

98. *Id.* (emphasis added).

99. *Id.*

100. Natasha Singer, *Charting the "California Effect" on Tech Regulation*, N.Y. TIMES (Oct. 12, 2022), https://www.nytimes.com/2022/10/12/us/california-tech-regulation.html [https://perma.cc/M52U-BVQC].

101. *1Life Healthcare Inc. Privacy Policy: Section XI*, ONE MEDICAL (last updated Sept. 13, 2023), https://www.onemedical.com/privacy/ [https://perma.cc/BUP9-3NKR].

Civil Code Section 1798.120.[102] Here, we see the CCPA at work: (1) patients are given an opportunity to know how their sensitive information is being handled and (2) are given the right to have that information deleted.[103] Boiled down, these are basic data privacy rights that should extend to all and not just to those who reside in the Golden State.[104]

In short, the CCPA provides an appropriate blueprint to follow when thinking through the parameters for how consumers should be able to regulate the way in which their data, specifically sensitive data, is used. An FTC enforcement mechanism built with aspects of the CCPA in mind is one approach for engineering a regulatory structure around data acquired through Big Tech transactions that HIPAA does not cover. Specifically, an amendment to the HSR Act's reportability requirements could include a "sensitive data" test, which could implement the CCPA's four codified rights into the pre-merger process. Doing so would ensure consumers know that their data is being acquired and would give them more control over how it is used, if at all.

V. ANALYSIS AND RECOMMENDATION

A. The Amazon Effect

When major technology firms, such as Amazon, come into possession of sensitive health data via acquisition generated from the acquiree's consumer base, it is irresponsible for lawmakers and regulatory agencies to look the other way.[105] When transactions of this magnitude and sensitivity are proposed, consumers should, at the very least, be informed about how their data could be used and given the right to opt out of their data being used altogether. One approach for implementing good governance over the use of consumer data by major tech firms is to enact regulation at market entry.

Drawing upon the CCPA, the following section will broadly outline the elements this type of regulation would include and who would hold enforcement authority. Regulating sensitive data obtained through mergers and acquisitions under a revised HSR Act would put more boundaries around how technology companies use patient health data, with key aspects resembling basic procedural due process elements: notice and an opportunity to respond.

---

102. *1Life Healthcare Inc. Privacy Policy: Section XI(b), Exercising Your Rights*, ONE MEDICAL (last updated Sept. 13, 2023), https://www.onemedical.com/privacy/ [https://perma.cc/BUP9-3NKR]; *see* Privacy Portal, ONE MEDICAL, https://privacyportal-cdn.onetrust.com/dsarwebform/6f62a1b4-fb5e-4a72-bfc3-fd066b342a4a/3569fa78-512c-455d-8c53-2883ea88d733.html [https://perma.cc/TS3L-V76A] (last visited Aug. 18, 2023).

103. *See 1Life Healthcare Inc. Privacy Policy: Section XI*, *supra* note 101.

104. *See* Laura Hautala, *California's New Privacy Rights Could Come to Your State, Too*, CNET (Jan. 3, 2020, 10:04 AM), https://www.cnet.com/news/privacy/californias-new-ccpa-privacy-rights-could-come-to-your-state-too/ [https://perma.cc/CCR7-ZJ9M].

105. *See The World's Most Valuable Resource Is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [https://perma.cc/8E6N-A3KG].

Amazon has built its brand on convenience and efficiency, and the Amazon effect could, in fact, substantially improve the reorganization of healthcare delivery. This argument, however, could be made for every market Amazon enters, and it has already entered quite a few.[106] Knowing Amazon will continue to innovate, the relevant question is how to best govern a data-powered company as it enters the trusted space that is healthcare.[107] How can the objectives of Amazon, as well as those of other major tech firms likely to follow suit, align with the privacy concerns held by many consumers?

Amazon's attempt to streamline the healthcare experience may be welcome news to some, regardless of the company's data policies. Meanwhile, for others, the merger with One Medical pushes a privacy boundary perhaps a bit too far. The proposed recommendation aims to address the needs of a broad audience.

B. Elements of a Data Privacy Standard in the Age of Big Tech

One advantage Amazon has over other major tech firms is the fact that it "[hasn't] violated consumer trust yet,"[108] or at least in ways comparable to how other firms have violated that trust.[109] Barbara Kahn, Professor of Marketing at The Wharton School, stated in an interview that even though current Amazon customers know the company has troves of their personal information, customers "haven't seen [Amazon] do anything inappropriate with that information."[110] There is still the opportunity for error. Rather than passively anticipating potential harm, it is time to proactively implement substantive regulations to mitigate risks.

1. Privacy Regulation by Way of Pre-Merger Review

As mentioned *supra* Section II.C, one of the most concerning aspects of the Amazon-One Medical merger was the lack of notice to existing One Medical patients.[111] A One Medical member wrote in response to the proposed merger: "After a broadly positive experience with One Medical, I cancelled [my] membership today. I do not trust Amazon to *act in good faith* with my health data."[112] Instead of trying to hide information from customers,

106. *See supra* Section II.A.

107. *See Is Amazon Getting Too Big?*, *supra* note 61.

108. *Id.*

109. *See, e.g.*, the Cambridge Analytica scandal. *See* Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html [https://perma.cc/WX5A-YVLP]; *see also* Douglas MacMillan & Robert McMillan, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, THE WALL ST. J. (Oct. 8, 2018), https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194 [https://perma.cc/7KJ4-CT6B].

110. *See Is Amazon Getting Too Big?*, *supra* note 61.

111. *See* Levy, *supra* note 37.

112. *Id.* (emphasis added).

best practice requires bringing customers into the fold.[113] Companies should gain customer trust by practicing transparency and making their data use practices known. They should provide customers with the option to decide on how their data can or cannot be used, and to do this, Amazon and other companies could use a little boost from the FTC.

If data practices are not readily disclosed to customers or are deceptive, the FTC can step in to create a new norm *before* Section 5 authority is triggered. In *The FTC and The New Common Law of Privacy*, Professors Daniel J. Solove and Woodrow Hartzog acknowledge "[o]nce [data privacy] standards become well established, there is an expectation that companies follow them" and "[m]oreover, people begin to expect that these standards are followed, and a large part of privacy involves managing people's expectations."[114] To get here, the FTC, by way of the HSR Act, can implement a data privacy standard through the pre-merger review process.

2. Data Integration Within the Hart-Scott-Rodino Act

The Hart-Scott-Rodino Act, combined with aspects of Section 5 authority, can be the vehicle by which data regulation in the age of Big Tech gets traction. Apart from identifying mergers amounting to combinations in restraint of trade, the HSR Act pre-merger review process also aims to identify mergers that would cause harm to consumers.

Under the HSR Act, companies who satisfy specific criteria must report their plans to merge to "enforcement agencies before consummating the transaction."[115] HSR Act rules for reportability include a commerce test, size-of-transaction test, and size-of-person test.[116] Integrating a "sensitive data" test as part of the reportability requirements in the HSR Act would be one way to shape data regulation early on, before more and more major tech firms enter markets where sensitive information is collected. Borrowing the CCPA's codified right to know, right to delete, right to opt-out, and right to non-discrimination could be data privacy requirements companies must have in place or must make available to their customers upon completion of a merger.

Amending the HSR Act threshold requirements to include a "sensitive data" test would ensure that companies are aware their acquisition of sensitive data and their corresponding consumer protections (or lack thereof) for this type of data would undergo FTC review. Conversely, consumers could have

---

113. *See* Rebecca Pifer, *Why Regulators Didn't Challenge Amazon-One Medical Deal, Despite Data Concerns*, HEALTHCARE DIVE (Mar. 1, 2023), https://www.healthcaredive.com/news/why-regulators-didnt-challenge-amazon-one-medical-deal-data/643316/ [https://perma.cc/852L-SF9E].

114. Daniel J. Solove & Woodrow Hartzog, *The FTC and The New Common Law of Privacy*, 114 COLUM. L. REV. 583, 662 (2014).

115. *See What Is the Premerger Notification Program? An Overview*, *supra* note 88, at 2.

116. *See Determining Hart-Scott-Rodino Applicability*, *supra* note 87; *see also Steps for Determining Whether an HSR Filing is Required*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/premerger-notification-program/hsr-resources/steps-determining-whether-hsr-filing [https://perma.cc/8JAN-KXKK] (last visited Mar. 5, 2023).

some comfort in knowing the potential sharing of their sensitive data between firms looking to merge would not go unchecked.

3. Review of Existing Privacy Policies & Statements

In the 1965 case of *Atlantic Refining Co. v. Federal Trade Commission*, the Supreme Court praised Congress's "foresight" in keeping Section 5 authority broad so it could be nimble in responding to evolving "business ingenuity and legal gymnastics."[117] In the instant case, the FTC should rely on its broad Section 5 authority to examine Amazon and One Medical's existing privacy policies and press statements for misleading privacy representations and the potential to misuse patient health information.

On February 22, 2023, with the merger completed, Amazon and One Medical released a statement hailing the partnership as a way to deliver "a more human health care experience."[118] Remarkably, the language in one of their responses to a frequently asked question (FAQ) about the protection of private health information states HIPAA "governs what One Medical, *Amazon, and others* can do with Protected Health Information."[119] However, in a previous blog post, the CEO of One Medical stated, "[o]nce the transaction closes, One Medical customers' HIPAA Protected Health Information will be handled *separately* from other Amazon business, as required by law."[120] Upon review, the threshold question is why Amazon is now included as an entity governed by HIPAA, whereas previously, One Medical implied Amazon would not have access to protected health information upon completion of the deal.[121] The second question is who does "and others" include?

At first glance, the statements released by Amazon and One Medical are just that—statements—and they contradict one another. The response to the FAQ does not provide a link to an updated privacy policy that further elaborates on their response or even a placeholder stating an updated policy is forthcoming.[122] The merger between the two companies was met with skepticism,[123] yet in the seven months between proposal and completion, it appears no action was taken to meaningfully address privacy concerns. Absent FTC review, the sharing and use of protected health information

117. Atl. Refin. Co. v. Fed. Trade Comm'n, 381 U.S. 357, 367 (1965).

118. *See One Medical Joins Amazon to Make It Easier for People to Get and Stay Healthier*, *supra* note 2.

119. *Id.* (emphasis added).

120. *See* Rubin, *supra* note 37 (emphasis added).

121. *Compare One Medical Joins Amazon to Make It Easier for People to Get and Stay Healthier*, *supra* note 2 (now including Amazon under HIPAA coverage along with One Medical) *with* Rubin, *supra* note 37 (emphasis added) (previously stating customer's protected PHI would be "handled separately from other Amazon business").

122. *See One Medical Joins Amazon to Make It Easier for People to Get and Stay Healthier*, *supra* note 2.

123. *See* Fowler, *supra* note 4; *Klobuchar Urges Federal Trade Commission to Investigate Amazon's Proposed Acquisition of One Medical*, *supra* note 6; Levy, *supra* note 37.

between the two companies is left unchecked.[124] Pursuant to Section 5 authority, the FTC should review existing privacy policies against statements made by Amazon and One Medical as they seem to be at odds with one another. The discrepancy could be an innocuous oversight; instead, it seems deceptive. The contradicting statements read as though, at the outset, the companies promised to keep sensitive health data siloed and have now relented on that promise.

4. Notice and Customer Response

The lack of transparency around the Amazon-One Medical merger suggests the companies were trying to downplay the merger and, thereby, potentially not acting in good faith. Companies have valid reasons to conduct transactions behind closed doors, but this transaction dealt with individuals' personal and private health information.[125] The lack of direct notice to existing One Medical patients about who might take over ownership of their doctor's office is a significant violation of their patients' trust.[126] Had One Medical directly notified existing patients about the proposed transaction, patients might have been less alarmed and skeptical about the merger. To regain and keep their patients' trust, Amazon and One Medical needed to communicate their intentions and spell out how exactly sensitive health information would be used and protected within the Amazon-One Medical ecosystem.[127]

To fill this notice gap, under an amended HSR review process, the FTC could implement a default pre-merger rule requiring companies involved in sharing sensitive health data to notify existing patients, giving them the opportunity to decide how they want their data used, if at all. As discussed *supra* Section IV.B, One Medical provides members in California with the option of knowing how their data is used.[128] The notice and response practice is already in place. Extending these fundamental rights—notice and opportunity to consent—to existing members outside of California and those who become members under the Amazon-One Medical deal would address data misuse concerns.[129]

As a baseline, a default rule—inspired by the CCPA—would mandate merging companies to build into their privacy practices three foundational rights: a consumer's right to know, the right to opt-out, and the right to data

124. *See Statement of Commissioner Alvaro M. Bedoya Joined by Commissioner Rebecca Kelly Slaughter Regarding Amazon.com, Inc.'s Acquisition of 1Life Healthcare, Inc.*, *supra* note 41.

125. *See* Fowler, *supra* note 4.

126. *See* Levy, *supra* note 37 ("The company said nothing to provide One Medical customers with any comfort, and there was no conference call discussing the acquisition, as is customary with many large transactions.").

127. *See* Pifer, *supra* note 113, at 19.

128. *See 1Life Healthcare Inc. Privacy Policy: Section XI*, *supra* note 101.

129. *See* Pifer, *supra* note 113 (noting Amazon can "mitigate" data misuse concerns by "communicating privacy policies or consent for data use in clear language").

deletion.[130] These rights are borne out of procedural due process.[131] A notice requirement, especially in the context of clinical entities merging with non-clinical entities, is of heightened importance. Consumers should be given appropriate notice about how their data is being used and afforded the opportunity to opt out of personal data collection or have the option of deleting their data altogether.

5. Additional Enforcement Actions

A final recommendation for an amended pre-merger review process would involve incorporating the FTC's existing Health Breach Notification Rule.[132] Under the current rule, "vendors of personal health records and related entities [must] notify consumers following a breach involving unsecured information."[133] In the Flo Health example discussed *supra* Section II.C, one of the agreed upon remedies required the company to notify customers of the data breach and the subsequent disclosure of user's sensitive health data.[134] Incorporating this rule into an amended HSR Act review process would link the breach notice requirement to data-intensive transactions between major tech firms.

In summary, the tools for safeguarding and regulating sensitive health data exist but need to be actively employed. The FTC holds substantial enforcement authority and is well-positioned "to take . . . bolder steps toward developing . . . a meaningful, and broad approach to regulating privacy in the United States."[135] The CCPA is one example of an articulate state privacy law. Including the CCPA's privacy rights in an amended HSR Act is one approach to regulate sensitive health data acquired by major tech firms entering the health services sector prior to a merger.

VI. CONCLUSION

As consumers, we enter e-commerce spaces and navigate mobile apps with the expectation that our data is collected; we place our trust in the privacy policies we click on and agree to.[136] But agreeing to have our most sensitive form of data—personal health data—shared between a clinical entity and a massive tech company is unsettling for some. The Amazon-One Medical merger is likely the start of many similar transactions, ones where Big Tech moves into spaces it has not previously occupied. As major tech firms move

130. *See* Cal. Civ. Code § 1798.100 (West 2020).

131. *See* Bd. of Regents of State Colls. v. Roth, 408 U.S. 564, 571-72 (1972) (finding "property interests protected by procedural due process extend well beyond actual ownership of real estate, chattels, or money").

132. *See* Health Breach Notification Rule, 16 C.F.R. § 318.1 (2009).

133. *Id.*

134. *See FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others*, *supra* note 70 ("As part of the settlement, Flo Health must notify affected users about the disclosure of their health information and instruct any third party that received users' health information to destroy that data.").

135. *See* Solove & Hartzog, *supra* note 114, at 676.

136. *Id.* at 667.

to consolidate services, consumer data must be handled responsibly. Companies must work to build systems consumers can trust, where they know their data is collected and managed ethically, and where transparent privacy practices are in place. Likewise, lawmakers must hold companies responsible for their use of data and work to create substantive regulations to prevent firms from falling short.

Decriminalizing Trivial Computer Use: The Need to Narrow the Computer Fraud and Abuse Act (CFAA) After *Van Buren*

Benjamin A. Soullier*

TABLE OF CONTENTS

* J.D., May, 2024, The George Washington University Law School; B.A. May, 2019, European History and Mass Communications, Washington and Lee University. I would like to thank Michael Beder and Thompson Hangen for their encouragement, feedback, and support throughout this process. I would also like to thank Bernard Baffoe-Mensah and Jordyn Johnson for their help during the editing stages. Most notably, I would like to thank Ryan Dickey for introducing me to the CFAA and for the many conversations involving the conception and reworking of the GPS hypotheticals. Finally, I would like to thank Isabelle Chancey for her support throughout my law school journey.

I. INTRODUCTION

Since its conception, the Computer Fraud and Abuse Act (1986) (the CFAA) has tried to play catch-up to tackle issues far more advanced than the current statutory language can support.[1] For years, courts applied the statute almost as broadly as allowable to rule on technologically complicated legal problems.[2] Yet, technological advancement creates the need to narrow certain provisions within the CFAA to prevent the federal government from charging someone for an offense that otherwise would not be considered a crime.[3]

The following hypotheticals are used solely to demonstrate the overbroad nature of the CFAA and how it could potentially be misapplied, thus proving the need to amend the statute.[4] For example, if an individual were to break into a car, start the ignition, and use the car's Global Positioning System (GPS)[5] to plug in a known address and drive to a "chop shop" to sell the car, under most state criminal codes, this is grand larceny.[6] Yet, on top of the state law criminal liability for theft, this scenario could quickly carry serious federal computer crime charges.[7] As implausible as it may seem, the federal hacking statute is engaged solely because of the use of the GPS to navigate to the chop shop.[8] In short, this individual could receive a five-year sentence, in addition to any sentence they receive for the grand larceny charge, for typing in an address he already knew.[9] It may seem equally implausible that a GPS is even a computer[10] and encompassed by the CFAA,

1. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986); Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561-67 (2010); Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 475-77 (1990).

2. *See* Greg Polaro, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 9 DUKE L. & TECH. REV. 1, 1-12 (2010).

3. *Id.*

4. 18 U.S.C. § 1030(c)(2)(B)(ii).

5. *GPS Applications*, UNITED STATES SPACE FORCE: GPS.GOV (2014), https://www.gps.gov/applications/ [https://perma.cc/RRT7-ZSKP].

6. VA. CODE ANN. § 18.2-152.8 (WEST 2011).

7. 18 U.S.C. § 1030(c)(2)(B)(ii) (Anyone who violates § 1030(a)(2)(C) in "furtherance of any criminal or tortious act" that violates State or Federal law can be punished via fine or up to five years in prison.).

8. 18 U.S.C. § 1030(a)(2)(C); United States v. Van Buren, 141 S. Ct. 1648, 1660-64 (2021) (The GPS scenario is based on the fact that the individual surpassed the computer's "gate," as the Supreme Court requires for a breach in authorized access, through breaking through the car's door locks and starting the ignition, thus meeting the elements for an (a)(2)(C) violation. In short, the door locks and ignition requirement to start the GPS system serve as the owner expressly intending to prevent access to the car and all its applications to strangers.).

9. 18 U.S.C. § 1030(a)(2)(C), § 1030(c)(2)(B)(ii) (The unauthorized use of the GPS to sell stolen goods qualifies as violating § 1030(a)(2)(C) to further another crime, thus triggering the felony enhancement for the CFAA hacking provision.).

10. 18 U.S.C. § 1030(e)(1) (Any device with data processing or data storage capabilities is considered a "computer."); *See* United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 1995) (considering a radio system as a computer).

as an instrumentality of interstate commerce.[11] Additionally, the car's door locks and ignition serve as a "gate" that prevents unauthorized access to the GPS.[12] While all of the above may seem somewhere between unlikely and impossible, this Note will prove otherwise.[13] Furthermore, this Note argues that this scenario is outside of the original scope and purpose of the CFAA, especially for § 1030(a)(2)(C), and as such, the language of the statute should be amended to prevent the prosecution of such actions.[14]

Now, focus on another hypothetical with mostly the same facts as above, but this time, the thief sees a suggested route titled "Home" on the navigation application on the car's dashboard.[15] The thief uses that address to navigate to the owner's home and break in.[16] At this point, the best-case scenario is stolen or damaged property, but if the owner or someone else happens to be in the house, the scenario could become violent very quickly if the burglar turns aggressive.[17] The only aspect that changed between the two scenarios is that in the second hypothetical, the thief used unauthorized access to the GPS to obtain the car owner's home address and burglarize the home.[18] Legally, the difference between the two acts is that in the second, the unauthorized access led to the acquisition of information that was essential to the thief burglarizing the car owner's home, satisfying the felony enhancement standard.[19] Without the electronically stored address and the GPS directions, the thief could not have burglarized the home, or in terms of the statute, advanced another crime or tort, whereas the information obtained in the first hypothetical was simply directions to a known location.[20]

The felony enhancements under § 1030(a)(2)(C)(ii) must be narrowed to exclude punishment for frivolous or insignificant use of technology during

11. 18 U.S.C. § 1030(e)(2)(B) (A "protected computer" means a device "used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."); Generally, courts hold any device that connects to the Internet, or similar interstate or international network, is considered a protected computer; *see* United States v. Auernheimer, 748 F.3d 525, 534 (3rd Cir. 2014); United States v. Yücel, 97 F. Supp. 3d 413, 419 (S.D.N.Y. 2015); United States v. Fowler, No. 8:10-cr-65-T-24, 2010 U.S. Dist. LEXIS 118260, at *4-*8 (M.D. Fla. Oct. 25, 2010); United States v. Morgan 748 F.3d 1024, 1032 (10th Cir. 2014) (finding GPS devices are instrumentalities of interstate commerce for the purposes of Federal kidnapping statutes).

12. *Van Buren*, 141 S. Ct. at 1660-64.

13. 18 U.S.C. § 1030(c)(2)(B)(ii).

14. Griffith, *supra* note 1, at 475-77.

15. *Connected Navigation*, FORD MOTOR CO.: TECH. (2023), https://www.ford.com/technology/connected-navigation/?gnav=footer-connetedNav [https://perma.cc/88MD-KRJF].

16. *Id.*

17. Deane Biermeier & Samantha Allen, *Surprising Home Burglary Facts and Stats*, FORBES (Jan. 23, 2023 8:00 AM), https://www.forbes.com/home-improvement/home-security/home-invasion-statistics/ [https://perma.cc/YPT3-YTGU].

18. *Connected Navigation*, *supra* note 15.

19. *Van Buren*, 141 S. Ct. at 1660-63.

20. 18 U.S.C. § 1030(c)(2)(B)(ii).

the commission of a crime or tort.[21] On the other hand, the amended language must continue to serve the original purposes of the CFAA.[22] This Note specifically focuses on the technological components of car GPS devices to illustrate the need to amend the language of the felony enhancement, but this issue is not exclusive to automobiles or GPS devices.[23] Specifically, analysis of car technology through the two GPS hypotheticals depicts the "gate" breach of a protected computer and the crime of grand larceny as committed through a singular act, thus creating a nexus between two statutory interests: protections against cybercrime and physical crime.[24]

Section 1030(a)(2)(c) of the CFAA prohibits unauthorized use of any "protected computer" or exceeding authorized access.[25] The felony enhancement this Note discusses involves § 1030(c)(2)(B)(ii), which states that anyone who violates (a)(2)(c) "in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State" can be punished by fine or up to five years in prison.[26] Additionally, in *United States v. Yücel*, the Court defined "protected computers" as any device that connects to the Internet.[27] The Court also held that this definition maintained the constitutionality of the CFAA under the Interstate Commerce Clause.[28]

The potential for misapplication of this Section of the CFAA, as illustrated by the GPS hypotheticals, was amplified by the more recent U.S. Supreme Court decision in *Van Buren v. United States*.[29] While this case did not examine the felony enhancements, it clarified what counts as "unauthorized access," thus creating the possibility for the nexus act.[30] In *Van Buren*, the Court used a "gates up, gates down" test to determine if a user is authorized to access a "protected computer."[31] According to the Court, the "gates" must be sufficiently up to prevent access to the computer.[32] In other words, there must be an actual obstacle to access beyond implied permission such as employment agreement policies.[33]

The lasting and perhaps unintended consequence of *Van Buren* is that the Court implies that gates can include physical barriers, so long as they significantly signify to others that access is prohibited or actually restrict or

---

21. *See generally* Kerr, *supra* note 1, at 1561-67 (examining the history of amending the CFAA, as technology advances, to restrict prohibitions to the original scope and purposes of the act).

22. CONG. RSCH. SERV., RL97-1025, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS, at 1 (2014), HTTPS://CRSREPORTS.CONGRESS.GOV/PRODUCT/PDF/RL/97-1025 [https://perma.cc/4UQX-R6YQ] (describing the CFAA's purpose to "shield[] [protected computers] from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud").

23. Kerr, *supra* note 1, at 1561-67.

24. *Van Buren*, 141 S. Ct. at 1658-63.

25. 18 U.S.C. § 1030.

26. *Id.*

27. *Yücel*, 97 F. Supp. 3d at 419.

28. *Id.*

29. *Van Buren*, 141 S. Ct. at 1652; ORIN S. KERR, COMPUTER CRIME LAW, 50-61 (5th ed. 2022).

30. *Van Buren*, 141 S. Ct. at 1652.

31. *Id.* at 1658-59.

32. *Id.*

33. *Id.* at 1659-63.

prevent access to the protected computer.[34] While the Court did not explicitly define what constitutes a sufficient "gate" to prevent access to a protected computer, the Court broadly stated that at minimum, there must be a clear effort to prevent the access in question.[35] This leaves the possibility for physical barriers or non-code-based barriers[36] to potentially serve as "gates."[37]

Given the recency of *Van Buren*, the GPS hypotheticals are meant to serve as a lens to view the larger issue of the overbroad felony enhancements by analyzing simple technology and the nexus between a "gate" and a traditional auto theft.[38] The scope of this issue is not limited to car theft or GPS misuse. Conversely, the hypotheticals are used to demonstrate the larger issue which is the overbroad nature[39] of § 1030(c)(2)(B)(ii)'s felony enhancement leading to potential misapplication following the decision in *Van Buren* and the creation of the "gates up or down" standard.[40] In other words, the simple fact that these car theft hypotheticals could reasonably occur proves the need for a narrower statute and standard. Additionally, the Court in *Van Buren* refused to accept the government's argument that prosecutorial discretion would prevent arbitrary criminal charging based on private employer-drafted work policies.[41] The Court specifically said this argument would lead to prosecutions that "may not be warranted" and not expressly "prohibited," contradicting the CFAA's text and purpose.[42] Therefore, after evaluating the statute through the lens of the GPS hypotheticals, the law must be narrowed by either the Court or Congress in order to correct the problem and avoid the type of arbitrary prosecution the Court was concerned about in *Van Buren*.[43]

To address these issues, felony enhancements under § 1030(c)(2)(B)(ii) should be amended to apply only when an individual knowingly[44] uses the information obtained through unauthorized access to a protected computer to

---

34. *Id.*

35. *Id.*

36. This Note does not address the issue of whether "breaching authorized access" should be narrowed to only apply to code-based restrictions because even if this were the case, the felony enhancements remain too broad and must be limited. Therefore, this Note focuses only on the nature of the felony enhancements and creating a more specific legal standard. *See generally* George F. Leahy, *Keeping Gates Down: Further Narrowing the Computer Fraud and Abuse Act in the Wake of Van Buren*, 14 WM. & MARY BUS. L. REV. 215, 218-22 (2022) (discussing the importance of code-based barriers protecting personal information).

37. *Van Buren*, 141 S. Ct. at 1660-63 (The Court determined that the "gates" did not necessarily need to be limited to traditional passwords, encryption, or other cyber methods of securing computers, but that physical locks or other efforts to prevent access that were expressly communicated as security measures could also be considered "gates.").

38. *Id.*

39. Kerr, *supra* note 1, at 1561-67.

40. *Van Buren*, 141 S. Ct. at 1660-63.

41. *Id.* at 1662.

42. *Id.*

43. *Id.*

44. Knowingly, as defined in the context of the CFAA damage statute 18 U.S.C. § 1030(a)(5), is an action taken where the result is practically certain; *see* United States v. Morris, 928 F.2d 504, 510 (2d Cir. 1991) (The court held whether or not a defendant intends to cause damage is irrelevant so long as the defendant knew or reasonably should have known their actions could cause damage.).

substantially[45] further "any criminal or tortious act."[46] The statute as amended would protect against the potential criminalization of computer acts that would not, if isolated, be violations of the CFAA, while also preserving the privacy protection interests the CFAA was originally intended to fortify.[47] In other words, the amended provision sufficiently gives citizens clear notice of potential violations, while punishing those who purposefully use a computer, without authorization, as a critical component to advance a criminal or tortious act or use a protected computer without authorization to significantly violate the owner's privacy rights to contribute to a criminal or tortious goal.[48] Ultimately, no one would receive jail time for frivolous or incidental use of technology.[49]

This Note first describes Congress's motivation and purpose in drafting the CFAA.[50] Then, this Note will define § 1030(a)(2), the standard for breaching or exceeding authorized access, and the changes established by *Van Buren*.[51] Additionally, this Note will outline the felony enhancements under § 1030(c)(2)(B)(ii). This Note will subsequently define a "computer" and "protected computer" and establish car theft as a major issue throughout the U.S.[52] Finally, this Note will examine in more detail the hypothetical situations mentioned previously to illustrate the overbroad nature of the felony enhancements and the effectiveness of the proposed amended provision to correct this issue.[53]

II. BACKGROUND

A. The CFAA and Subsequent Jurisprudence

This Section first looks to the origins of the Computer Fraud and Abuse Act and the information privacy concerns it intended to address to establish why the § 1030(a)(2)(C) felony enhancements create opportunities for overbroad application and frivolous prosecution.[54] Next, it is important to examine what constitutes a § 1030(a)(2)(C) violation after the decision in *Van Buren,* because in order to apply the felony enhancements,[55] an individual must first breach the "gate" to a "protected computer."[56] Afterward, this Note

45. The "substantial" prong of this standard is based on federal criminal attempt law, which requires the individual to take a "substantial step" towards completing the crime; *see* United States v. Taylor, 142 S. Ct. 2015, 2020 (2022) ("a substantial step . . . beyond mere preparation"); *see also* United States v. Resendiz-Ponce, 549 U.S. 102, 107 (2007); MODEL PENAL CODE § 5.01 CRIMINAL ATTEMPT (AM. L. INST. 2023).

46. 18 U.S.C. § 1030(c)(2)(B)(ii).

47. Griffith, *supra* note 1, at 475-77.

48. *Id.*

49. *Id.*

50. 8 U.S.C. § 1030; *see also* Griffith, *supra* note 1, at 475-77.

51. *Van Buren*, 141 S. Ct. at 1660-63.

52. *Auernheimer*, 748 F.3d at 534; *Yücel*, 97 F. Supp. 3d at 419; *Fowler*, 2010 U.S. Dist. LEXIS, at *4-*8.

53. Kerr, *supra* note 1, at 1561-67.

54. Griffith, *supra* note 1, at 475-77.

55. 18 U.S.C. § 1030(c)(2)(B)(ii).

56. 18 U.S.C. § 1030(a)(2)(C); *Van Buren*, 141 S. Ct. at 1660-63.

will establish which devices constitute "computers"[57] and "protected computers."[58]

B. Origins of the CFAA

The CFAA is rooted in the protection of privacy, as well as the fear of how far technology could advance beyond the scope of statutory regulations drafted for traditional crimes of the physical world.[59] However, the CFAA was not the first attempt at addressing these issues.[60] The proposed Computer Trespass Act of 1984 was an attempt by Congress to regulate computer crimes in the early stages of computer development.[61] The bill, which never made it into law, would have targeted the unauthorized use, or use exceeding authorization, of computers to "obtain certain information classified under the Atomic Energy Act of 1954 or certain financial records covered by the Right to Financial Privacy Act of 1978."[62] Government and military computers would also have been protected, but the bill was not designed to protect the personal computers of individual citizens unless financial documents were involved.[63] Congress's initial focus on national security and the financial sector carried into the early drafting of the CFAA.[64] However, the final version that was passed in 1986 remains largely intact today and includes more general provisions intended to replicate traditional criminal code and tort law, specifically copyright infringement.[65]

Initially introduced in 1984 and passed in full in 1986, the Computer Fraud and Abuse Act was drafted to broadly regulate potential violations of

57. 18 U.S.C. § 1030(e)(1).

58. 18 U.S.C. § 1030(e)(2).

59. Griffith, *supra* note 1, at 467-70.

60. Computer Trespasses Act, H.R. 5616, 98th Cong. (1984), https://www.congress.gov/bill/98th-congress/house-bill/5616 [https://perma.cc/82C8-2ATL] (The act passed the House of Representatives and then passed the Senate with amendments, but the changes were not reconciled.).

61. *Id.*

62. *Id.*

63. *Id.*

64. *See generally* STEPHANIE RICKER SCHULTE, "THE WARGAMES SCENARIO" REGULATING TEENAGERS AND TEENAGED TECHNOLOGY 1-5 (1980–1984) (2008) (The plot of the 1983 hit movie "WarGames" follows a teenager, played by Matthew Broderick, who "hacked" into a military computer controlling the U.S. nuclear operations and accidentally almost started World War III. This influenced Congress to punish computer trespasses and, "hearings ultimately resulted in the nation's first comprehensive legislations about the Internet and the first ever federal legislation on computer crime: the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984."); *see* 18 U.S.C. § 1030(e)(2)(A) (The act mentions computers "exclusively for the use of a financial institution or the United States Government" when defining protected computers, suggesting the importance lawmakers placed on insuring these devices were secure.).

65. *See* H. MARSHALL JARRETT AND MICHAEL W. BAILIE, PROSECUTING COMPUTER CRIMES 20 (Office of Legal Education Executive Office for United States Attorneys: Computer Crime and Intellectual Property Section Criminal Division 2017) (this U.S. Attorney's Office publication specifically mentions how the language of the felony enhancements for 18 U.S.C. 1030(a)(2)(C), detailed in 18 U.S.C. 1030(c)(2)(B)(ii), were borrowed from the copyright law and wiretap statutes); s*ee* Copyright Act, 17 U.S.C. §§ 101-1511 (1980); s*ee* Wiretap Act, 18 U.S.C. § 2511 (1968).

privacy and abuses of functionality regarding computers.[66] Congress hoped to enact a new set of laws to address issues of computer insecurity and protect the private information of American citizens.[67] In general, there are two types of "computer crimes" that the American legal system is equipped to regulate: (1) "computer misuse crimes," which are considered the "intentional interference with the proper functionality of computers" and (2) "traditional criminal offenses facilitated by computers."[68] Examples of computer misuse crimes include hacking, denial of service attacks, phishing, and virus implementation.[69] "Traditional" computer-facilitated offenses typically include fraud, online threats, child pornography, and gambling.[70] The CFAA was drafted to regulate both computer misuse crimes and computer-facilitated offenses, but §§ 1030(a)(1)–(5) are predominately concerned with acts of computer misuse.[71]

C. Breaching Authorized Access Under § 1030(a)(2)(C) and Van Buren

This Note specifically examines § 1030(a)(2)(C), which is ordinarily a misdemeanor but carries a felony enhancement under § 1030(c)(2)(B).[72] Section (a)(2)(C) reads, "whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished as provided in subsection (c) of this section."[73] Cases involving violations of § 1030(a)(2) typically include breaching a computer's security measures but can also include the use of a computer or network for purposes other than its intended use.[74] So in the context of the GPS hypothetical, the computer's security measures or the "gate" preventing unauthorized access would be the combination of the car's locked doors and ignition powering on the GPS.[75]

In 2021, however, the Supreme Court clarified what exactly is required to determine when an individual is authorized to access a computer and, if

66. 18 U.S.C. § 1030; Griffith, *supra* note 1, at 476 (The original format of the CFAA and specifically § 1030(a)(2), directly referenced the Right to Financial Privacy Act of 1978. Specifically, "[t]he premise of . . . [§ 1030](a)(2) was to protect, for privacy reasons, the computerized credit records and computerized information relating to customers' relationships with financial institutions. Congress wanted to extend the same privacy protection to the financial records of all customers of financial institutions, including individuals, partnerships, or corporations. To accomplish this aim, Congress redefined the terms "financial institution" and "financial record" in broader terms than those provided by the Right to Financial Privacy Act of 1978.").

67. Griffith, *supra* note 1, at 476.

68. KERR, *supra* note 29, at 1-5.

69. *Id.*

70. *Id.*

71. 18 U.S.C. § 1030.

72. 18 U.S.C. § 1030(a).

73. *Id.*

74. *Morris*, 928 F.2d at 504-08 (Defendant, a graduate student, was authorized to access Cornell University's computer equipment and network but used a computer program or "worm" that multiplied itself onto other systems, including U.S. military systems and caused significant damage, leading the court to hold Morris breached authorized access.).

75. *Van Buren*, 141 S. Ct. at 1653, 1660.

they are, when authorized access is exceeded.[76] In *United States v. Van Buren*, police officer Nathan Van Buren (defendant) made a deal with Andrew Albo for a loan of $5,000 in exchange for Van Buren investigating a woman acquainted with Albo.[77] Albo then recorded his conversations and subsequent agreement with Van Buren and gave the tapes to the Federal Bureau of Investigation (FBI).[78] Using a police computer in his car, Van Buren conducted a full search of the woman in question.[79] Van Buren was then charged with violations of 18 U.S.C. § 1030(a)(2).[80]

Both parties agreed Van Buren was authorized to access the computer generally and conduct investigative searches for police purposes, but the two sides disputed whether he exceeded this access by conducting personally motivated searches in exchange for money.[81] The government argued individuals must be expressly approved to conduct each individual search and searches for personal gain were prohibited by department policy.[82] Whereas Van Buren argued that he was generally authorized to use the system and could conduct the search he chose without criminal liability.[83] In other words, the government argued that even though Van Buren technically could access the information and was allowed to conduct searches on his police computer, the search for Albo violated the interests of his employer.[84] On the other hand, Van Buren argued that the statute meant he must be prevented from searching altogether.[85] The Court agreed with Van Buren and held he did not breach or "exceed authorized access" to a protected computer because there was no barrier preventing him from accessing the information.[86] He was authorized, as a police officer, to search the system for information on individuals, and department policies about when such searches are permitted were not sufficient to serve as a "gate."[87]

After *Van Buren*, courts have looked for barriers preventing individuals from accessing the computer or the functionality of the computer.[88] In *Zap Cellular v. Weintraub*, the Eastern District of New York applied the *Van Buren* standard and held that a company terminating an employee was sufficient to close the gate on that individual's access to the computer system.[89] The Court explained that the company took an overt action to expressly prohibit the defendant's actions when it terminated the defendant's employment.[90] Thus, moving forward, the legal standard would likely accept

76. *Id.* at 1662.
77. *Id.* at 1653.
78. *Id.* at 1663.
79. *Id.* at 1653.
80. *Id.*
81. *Van Buren*, 141 S. Ct. at 1653-54.
82. *Id.*
83. *Id.* at 1654-55. (Civil liability or employment termination are separate issues.).
84. *Id.*
85. *Id.*
86. *Id.* at 1660.
87. *Id.*
88. Zap Cellular, Inc. v. Weintraub, No. 15-CV-6723, 2022 U.S. Dist. LEXIS 168735, at *1-*3 (E.D.N.Y. Sept. 19, 2022).
89. *Id.*
90. *Id.*

any clear indicator or effort to prevent access, stronger than employment policies, as a "gate" under *Van Buren*.[91]

Van Buren creates the need to narrow the scope of the statute because physical barriers can serve as security measures to prevent access to a computer, such as locking a car door to prevent access to the ignition.[92] Thus, the car door locks and ignition can become physical barriers to the dashboard computer.[93] More specifically, the lock on the car door prevents access to the ignition, and the ignition prevents access to the car's dashboard computer.[94] So technically, there are two gates, both connected to the crime of grand larceny because a burglar must bypass the door locks and ignition system.[95] Once both "gates" are breached, the ignition being the more vital to accessing the computer, and the burglar using the car's computer in relation to another crime or tort, the felony enhancements can be implemented.[96] In short, the Supreme Court's test allowing for physical barriers to determine who is authorized to access a computer presents the opportunity for the GPS hypothetical to be charged as a felony violation of § 1030(a)(2)(C).[97]

D. Felony Enhancements for § 1030(a)(2)(C) Crimes

Next, it is important to determine when the § 1030(a)(2)(C) felony enhancements are applicable.[98] The CFAA's hacking felony enhancements apply if "the [hacking of a protected computer] was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."[99] If convicted, individuals could be subject to a fine and up to five years in prison.[100] The underlying tort or criminal act being advanced cannot be the same as the action that violates § 1030(a)(2)(C); however, that act is not limited to traditional crimes or torts of the physical world.[101] In *United States v. Steele*, the defendant was fired by his employer but continued to use his account via a "backdoor" login to "access and download documents and emails" concerning active government contract bids involving the parent company.[102] The court held that termination of Steele's employment meant he was no longer "authorized" to access the system and thus violated § 1030(a)(2)(C), although he technically could still access the company's server.[103] The court also held that the application of the felony enhancements to the Virginia state crime of grand larceny did not merge with the defendant's hacking into his former employer's computer to steal company data because the data qualified as property under Va. Code

91. *Van Buren*, 141 S. Ct. at 1658-59; *Zap Cellular*, 2022 U.S. Dist. LEXIS, at *26-*28.
92. *Van Buren*, 141 S. Ct. at 1658-59.
93. *Id.* at 1658-59; FORD, *supra* note 15.
94. *Van Buren*, 141 S. Ct. at 1658-59.
95. VA. CODE ANN. § 18.2-95 (LEXIS 2022).
96. 18 U.S.C. § 1030(c)(2)(B)(ii).
97. *Van Buren*, 141 S. Ct. at 1658-59; 18 U.S.C. § 1030(c)(2)(B)(ii).
98. 18 U.S.C. § 1030(c)(2)(B)(ii).
99. *Id.*
100. *Id.*
101. United States v. Steele, 595 F. App'x 208, 216 (4th Cir. 2014).
102. *Id.* at 210.
103. *Id.* at 212.

Ann. § 18.2-152.[104] In other words, the defendant could be punished for breaching the gate to commit a crime and for stealing the data as property.[105] The data regarding the contract bids were obtained via Steele's unauthorized access, but the court found that Steele used that unauthorized access to commit grand larceny, and thus the government was not in danger of unconstitutionally subjecting Steele to double jeopardy.[106]

The felony enhancements in the CFAA were borrowed from the language in copyright law and wiretap statutes and, therefore, were never specifically drafted to address computer hacking issues.[107] According to a manual published by the U.S. Attorney's Office's Computer Crime and Intellectual Property Section Criminal Division, when investigating these crimes, a prosecutor should use their discretion to determine, "whether the defendant manifested an intent to commit a state tort" when they violated § 1030(a)(2)(C).[108] For hacking crimes in furtherance of a criminal act, prosecutors must simply prove a defendant committed a criminal act, and that act was progressed by an action that violated § 1030(a)(2)(C).[109]

While the use of prosecutorial discretion is the preferred method of the U.S. Attorney's Office for enforcing the CFAA, the Supreme Court refuses to accept these types of arguments and maintains statutory specificity through legislative action as the proper course of action.[110] Specifically, in *Van Buren*, the government argued that charging § 1030(a)(2) for computer use that violated workplace guidelines would not be arbitrary because prosecutorial discretion would only lead to charges that warranted punishment.[111] However, the Court refused to accept this argument, stating this strategy would be arbitrary because "[t]he policy instructs that federal prosecution 'may not be warranted'—not that it would be prohibited—'if the defendant exceed[s] authorized access solely by violating an access restriction contained in a contractual agreement or term of service with an Internet service provider or website.'"[112] In other words, the Court clarified the statute to require actual prevention of access (code-based or otherwise), instead of spoken or written employer policies serving as a gate.[113]

E. Defining a "Computer"

For the GPS hypothetical to become an issue of CFAA over-broadness, the car's navigation system must first be proven to be a computer and then

104. *Id.* at 216.
105. *Id.*
106. *Id.*
107. Jarrett, *supra* note 65, at 19-20, ("[T]he legislative history of § 1030 reveals that Congress intended the phrase to have the same meaning as identical language under the Wiretap Act, and cases construing that language hold the phrase encompasses state common law torts."); *see also* S. Rep. No. 104-357, at 8 (1996).
108. Jarrett, *supra* note 65, at 19-20.
109. *Id.* at 94.
110. *Van Buren*, 141 S. Ct. at 1660-62.
111. *Id.*
112. *Id.* at 1662.
113. *Id.*

subsequently a protected computer.[114] For CFAA prosecution, computers are devices subject to illegal manipulation or abuse, or tools for committing traditional crimes.[115] The CFAA's definition of computers is not limited to conventional understandings of desktops, laptops, or even smartphones.[116] According to 18 U.S.C. § 1030(e)(1), a "computer" is defined as:

> An electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable handheld calculator, or other similar device.[117]

In *United States v. Mitra*, the Seventh Circuit examined whether a radio system was considered a "computer" under the statute.[118] In this case, the city of Madison, Wisconsin, like most other cities, frequently used radio communications for their police, fire, and emergency response departments.[119] Mitra was able to analyze and eventually block radio communications for the city of Madison's emergency response personnel on a weekend when the city had a large number of visitors.[120] The appellate court held that radio signals, similar to the devices listed in the statute, are computers and in this case, protected computers.[121] Judge Frank Easterbrook wrote in his opinion for the court, "[E]very cell phone and cell tower is a 'computer' under the statute's definition; so is every iPod, every wireless base station in the corner coffee shop, and many another gadget[s]."[122] This definition of computers appears to be consistent with the statute's broad language describing computers as any device with "processing' capabilities.[123]

In a similar case in 2011, the Eighth Circuit held a cell phone, not a smartphone, used solely for voice calls and text messages was a "computer" under the statutory language.[124] In *United States v. Kramer*, the defendant pled guilty to "transporting a minor in interstate commerce with the intent to

114. 18 U.S.C. § 1030(a)(2)(C) (The statute requires information be acquired from a "protected computer.").

115. KERR , supra note 29, at 1-5; 18 U.S.C. § 1030(e)(2).

116. 18 U.S.C. § 1030(e)(2).

117. 18 U.S.C. § 1030(e)(1).

118. United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 2005); 18 U.S.C. § 1030(e)(1); KERR, *supra* note 29, at 82-83.

119. *Mitra*, 405 F.3d at 493.

120. *Id.* at 495.

121. *Id.*

122. *Id.*

123. 18 U.S.C. § 1030(e)(1).

124. 18 U.S.C. § 1030(e)(1); United States v. Kramer, 631 F.3d 900, 903 (8th Cir. 2011); KERR, *supra* note 29, at 82-83.

engage in criminal sexual activity with her."[125] While committing this crime, Kramer used a cell phone to call and text the victim for the six months leading up to the offense.[126] Although Kramer was not charged with violating the CFAA, the court examined § 1030(e)(1)'s definition of a computer to see if Kramer's cell phone met the requirements for sentence enhancement through the use of technology during a kidnapping offense.[127] The defendant argued that the phone's ability to make voice calls and send text messages did not make it a computer under the statute.[128] However, the court disagreed and found Kramer's cell phone was a computer under the statute, reasoning that "the definition captures any device that makes use of a[n] electronic data processor," which Kramer's cellphone possessed.[129] The court also held that "computers" do not necessarily need an Internet connection but instead simply require storage and processing capabilities.[130] It is also worth noting that in evaluating the sentence enhancement, the appellate court held that "the enhancement does not apply to every offender who happens to use a computer-controlled microwave or coffeemaker . . . [but] limits application of the enhancement to those offenders who use a computer 'to communicate directly with a minor.'"[131] Ultimately, the court seems to reason that (1) the cellular phone meets the broad definition of "data processing" device from the statute and (2) the cellphone was critical to the commission of the crime, justifying the sentence enhancement.[132] Overall, courts generally accept a broad definition of computers under the CFAA.[133]

F. Defining a "Protected Computer"

For someone to violate § 1030(a)(2), they must gain unauthorized access to or exceed authorized access to a "protected computer."[134] In other words, it does not matter if the gates are up or down if the device is not considered a "protected computer."[135] While the definition of a "computer" is primarily reliant on the device's data processing and storage capabilities and does not necessarily require an Internet connection, a "protected computer" carries a much narrower definition.[136] A "protected computer" includes any "computer," as defined above, "used in or affecting interstate or foreign

125. *Kramer*, 631 F.3d at 901 (Kramer was sentenced to 168 months in prison by the district for his offense, and in reaching this decision, the district court, "applied a two-level enhancement for its use to facilitate the offense, *see* U.S. SENT'G GUIDELINES MANUAL § 2G1.3(b)(3) (2009).").

126. *Kramer*, 631 F.3d at 902-03.

127. *Id.*

128. 18 U.S.C. § 1030(e)(1); Kramer, 631 F.3d at 903.

129. *Kramer*, 631 F.3d at 902-03.

130. *Id.* at 904.

131. *Id.* at 903; U.S. SENT'G GUIDELINES MANUAL § 2G1.3(b)(3) cmt. N.4 (U.S. SENT'G COMM'N 2009).

132. 18 U.S.C. § 1030(e)(1); *Kramer*, 631 F.3d at 904.

133. *Kramer*, 631 F.3d at 902-903; *Mitra*, 405 F.3d at 493; KERR, *supra* note 29, at 82-83.

134. 18 U.S.C. § 1030(a)(2).

135. *Id.*

136. 18 U.S.C. § 1030(e)(1)-(2)(B).

commerce or communication" or any computer used by financial institutions or the U.S. government.[137]

In practice, courts usually hold any computer with access to the Internet as a protected computer because these computers are connected to a larger network involved with or impacting interstate commerce.[138] In *United States v. Fowler*, the defendant accessed Suncoast Community Health Centers' computer system and caused damage, under § 1030(a)(5)(A).[139] Fowler transmitted a program after she was fired that prevented Suncoast employees from accessing their accounts.[140] Fowler argued that the Suncoast computers were not "protected computers" because they were not government or financial institution computers, and they were not involved in interstate commerce.[141] However, the court disagreed and held that since the computers were connected to the Internet, they were involved in interstate commerce.[142] The court heavily emphasized the longstanding doctrine that "the Internet is an instrumentality of interstate commerce," [143] or in other words, is a vessel through which "commerce" between the states is facilitated.[144] Thus, Congress is constitutionally authorized to regulate devices connected to a national and international network.[145] After establishing Internet-connected computers are considered an instrumentality of interstate commerce, the court in *Fowler* concluded that Suncoast's computers met the definition of "protected computer," as they could be, "used in or affecting interstate or foreign commerce or communications," as defined by the statute.[146]

A few years later in 2015, the Southern District of New York followed the principles established in *Fowler*.[147] In *United States v. Yücel*, the defendant was charged with being a leader of a group that "distributed malicious software," or malware, which allowed the group to control people's computers from a remote location.[148] The software also allowed the defendant and his co-conspirators to copy "keystrokes," turn on the owner's webcam, and search the computers' files and data.[149] The defendant argued that if any computer with Internet access is considered a "protected computer," then the statute is overly broad and gives Congress the power to limit too many acts.[150] However, the court disagreed in this regard because a "protected computer"

---

137. 18 U.S.C. § 1030(e)(2)(B); Jarrett, *supra* note 65, at 94.

138. 18 U.S.C. § 1030(e)(2)(B); *Auernheimer*, 748 F.3d at 534; *Yücel*, 97 F. Supp. 3d at 419; *Fowler*, 2010 U.S. Dist. LEXIS at *4-*8.

139. 18 U.S.C. § 1030(a)(5(A) ("knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer"); *Fowler*, 2010 U.S. Dist. LEXIS at *4-*8.

140. *Fowler*, 2010 U.S. Dist. LEXIS at 4-8.

141. 18 U.S.C. § 1030(e)(2)(B); *Fowler*, 2010 U.S. Dist. LEXIS at *4-*8.

142. *Fowler*, 2010 U.S. Dist. LEXIS at *4-*8 (citing United States v. Walters, 182 Fed. App'x 944, 945 (11th Cir. 2006) ("the Internet is an instrumentality of interstate commerce")).

143. *Id.*

144. Heart of Atlanta Motel, Inc. v. United States, 379 U.S. 241, 271 (1964).

145. *Fowler*, 2010 U.S. Dist. LEXIS at *4-*8 (citing *Walters*, 182 Fed. App'x At 945; United States v. Hornaday, 392 F.3d 1306, 1311 (11th Cir. 2004)).

146. 18 U.S.C. § 1030(e)(2)(B); *Fowler*, 2010 U.S. Dist. LEXIS at *4-*8.

147. *Yücel*, 97 F. Supp. 3d at 419.

148. *Id.*

149. *Id.*

150. *Id.* at 420.

was only one element in the crime, and the government must prove, in the case of *Yücel*, that the defendant breached authorized access and caused damage.[151] The court, after citing several cases from various jurisdictions, ultimately held that "the widespread agreement in the case law on the meaning of 'protected computer,' gives adequate notice to potential wrongdoers of what computers are covered by the statute."[152] In other words, the defendant was no special target under the circumstances of the case, and the standard, as applied, is constitutional.[153]

The concept of the Internet as an instrumentality is best illustrated in *Hornaday*.[154] In this case, the defendant sent an Internet message to an undercover government agent soliciting sex from two minors.[155] The defendant challenged Congress's power to regulate Internet solicitation of minors, but the Eleventh Circuit ultimately held that the Internet was an instrumentality through which the defendant sought "child victims."[156] The court also held that regardless of the Internet's mostly "intrastate" impact, Congress still has the power to regulate such conduct given the potentially massive impact on interstate and foreign commerce.[157]

III. CREATING THE "SUBSTANTIAL FURTHERANCE TEST"

This section will set forth the legal standard and framework for the "Substantial Furtherance Test" that this Note proposes.[158] The need for such a standard is clear based on the overbroad nature of the CFAA, specifically, the felony enhancement for § 1030(a)(2).[159] This test, if adopted by courts or the legislature, would serve as the last element of the CFAA hacking violation felony enhancement analysis.[160] This would serve to eliminate the issue illustrated by the two GPS hypotheticals and the vagueness associated with the act itself.[161]

In order to craft this test, this Note looks to combine the existing standard for the federal attempt law[162] and the mens rea definitions for knowledge requirement as applied in the computer damage statutes of the

151. *Id.*
152. *Id.*
153. *Yücel*, 97 F. Supp. 3d at 420.
154. *Hornaday*, 392 F.3d at 1311.
155. *Id.*
156. *Id.* at 1310-11.
157. *Hornaday*, 392 F.3d at 1311-12; (citing Heart of Atlanta Motel, Inc., 397 U.S. at 285 (1964) (holding that lodging for intrastate or local use still served an interstate instrumentality purpose and thus could be regulated under the Commerce Clause)).
158. 18 U.S.C. § 1030(a)(5); *Morris*, 928 F.2d at 509-11; *Taylor*, 142 S. Ct. at 2020; *see also Resendiz-Ponce*, 549 U.S. at 107; MODEL PENAL CODE § 5.01 CRIMINAL ATTEMPT (AM. L. INST. 2023).
159. *See generally* Kerr, *supra* note 1, at 1561-67.
160. 18 U.S.C. § 1030(a)(2)(C), § 1030(c)(2)(B)(ii).
161. Kerr, *supra* note 1, at 1561-67.
162. *Taylor*, 142 S. Ct. at 2020; *see also Resendiz-Ponce*, 549 U.S. at 107; MODEL PENAL CODE § 5.01 CRIMINAL ATTEMPT (AM. L. INST. 2023).

CFAA.[163] Attempt is defined as taking a "substantial step" towards achieving the goal of completing the crime "beyond mere preparation."[164] This is, in other words, an act that is "strongly corroborative of the actor's criminal purpose."[165]

The second component, knowledge, is derived from the CFAA damage statute § 1030(a)(5), which requires the defendant to "knowingly" cause damage.[166] This standard, as derived from *U.S. v. Morris*, must be an action taken where the result is practically certain.[167] In *Morris*, the defendant was charged § 1030(a)(5)(A) for damaging university and military computers by uploading a virus but argued he never intended to damage the computers, just gain access.[168] The court dismissed the defendant's argument and established the "intended function" test in which the court determined the software's intended function as a virus was to damage computers.[169] The defendant's intent was irrelevant so long as he knew or reasonably should have known the virus could cause damage if uploaded.[170]

The reasoning behind these additions to the standard is to eliminate the possibility of criminal liability for frivolous or insignificant computer use in connection to a crime or tort.[171] To achieve this goal, a line must be drawn between computer use that initiates or aids the attempt or completion of a separate crime or tort, and unauthorized computer use that does not initiate or aid such underlying acts.[172] Therefore, the test must include a significance factor, similar to that of a "substantial step" or "corroborative act," to determine when an individual knowingly makes an effort or makes a significant choice to use the information obtained through unauthorized access to further a crime or tort, and when that person just happens to use technology that is simply related to a crime or tort without significantly impacting the separate violation.[173] The current CFAA language simply states "in furtherance" of a crime or tort, without any requirement as to the significance of the technological contribution.[174] However, with the addition of a "substantial" effort requirement, the new test would significantly decrease the possibility of criminalizing computer use that minimally impacts the completion of the separate crime or tort, while continuing to punish acts that actually impact the attempt or completion of the underlying violation.[175] Additionally, a knowledge requirement would eliminate punishment for incidental computer use in relation to a crime or tort.[176] This new test, in full,

163. 18 U.S.C. § 1030(a)(5)(A) (requires an individual to "knowingly" cause damage to a protected computer and is a base felony offense).
164. *Taylor*, 142 S. Ct. at 2020.
165. MODEL PENAL CODE § 5.01 CRIMINAL ATTEMPT (AM. L. INST. 2023).
166. 18 U.S.C. § 1030(a)(5).
167. *Morris*, 928 F.2d at 509-11.
168. *Id.*
169. *Id.*
170. *Id.*
171. 18 U.S.C. § 1030(c)(2)(B)(ii).
172. *Id.*
173. *Id.*
174. *Id.*
175. *Id.*
176. *Id.*

would require an individual to knowingly[177] use the information acquired through unauthorized access to a protected computer, in violation of § 1030(a)(2)(C), as "a substantial step . . . beyond mere preparation"[178] to advance the efforts of another crime or tort.[179] This test would allow courts to draw the necessary distinction between the issues illustrated by two GPS scenarios and eliminate the overbroad nature of the statute.[180] The next section focuses on applying this test to the GPS fact patterns.

IV. APPLYING THE CFAA AND *VAN BUREN* TO INCIDENTS INVOLVING MODERN TECHNOLOGY REQUIRES MORE SPECIFICITY

The CFAA and its felony enhancements, as currently understood, can potentially be applied too broadly.[181] After *Van Buren*, physical barriers, when active, can be considered as "gates up" because it expressly signifies the owner does not want strangers to access the device.[182] Subsequently, physical barriers serving as "gates" present the opportunity for § 1030(a)(2)(C) to merge with traditional trespass crimes.[183] Therefore, the "substantial furtherance test" is necessary to determine when that merger point or nexus between committing a physical trespass and a hacking violation[184] should be charged as two separate crimes[185] or when the computer use is insignificant to warrant CFAA violation and punishment.[186] This section will use hypothetical fact patterns to show the value of the Substantial Furtherance Test and its continued importance as technology continues to advance.[187]

177. 18 U.S.C. § 1030(a)(5); *Morris*, 928 F.2d at 509-11.
178. *Taylor*, 142 S. Ct. at 2020.
179. 18 U.S.C. § 1030(c)(2)(B)(ii).
180. Kerr, *supra* note 1, at 1561-67.
181. *Id.*
182. *Van Buren*, 141 S. Ct. at 1658-60.
183. KERR, *supra* note 29, at 1-5; Van Buren, 141 S. Ct. at 1658-60.
184. 18 U.S.C. § 1030(a)(2)(C) (gaining unauthorized access to a protected computer).
185. This incident should be charged as a physical trespass crime and as a Section 1030(a)(2)(C) and 1030(c)(2)(B)(ii) felony enhancement hacking crime.
186. Griffith, *supra* note 1, at 475-78 (The CFAA was intended to protect private information stored on computers, mostly financial statements and similar documents.); s*ee also* Ric Simmons, *The Failure of the Computer Fraud and Abuse Act: Time to Take an Administrative Approach to Regulating Computer Crime*, 84 GEO. WASH. L REV. 1703, 1706 (2016) (advocating for administrative review of CFAA issues to avoid broad application and unfair punishment for crimes not "deserving" of punishment); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1656, 1660-63 (2003) (Before Van Buren negated the issue, Kerr argued employer agreements serving as barriers for authorized access violated traditional criminal punishment concepts.).
187. Griffith, *supra* note 1, at 475-78.

A. The Outdated Nature of the CFAA

The 1980s understanding of computer technology and the urgent desire to protect computers from cyber criminals are apparent through the text and background of the Computer Fraud and Abuse Act of 1986.[188] The statute was initially implemented to "criminalize only important federal interest computer crimes" and thus military computers and those of financial institutions were the primary concern.[189] Resultantly, changes throughout the years have focused on narrowing the statute to limit the term "authorized access."[190] However, legal scholar and professor Orin Kerr's fears of "vagueness" in this area are largely corrected by the decision in *Van Buren*.[191] Kerr was worried about the broad application of authorization because he was concerned about who could limit access to computers and who could be punished for it.[192] While the idea of terms of service violations being criminalized is troubling, the Supreme Court held in *Van Buren* that police department policies could not be used to criminalize the defendant's actions, thus correcting Kerr's fear.[193] While access authorization concerns have stabilized, future potential issues with the CFAA could arise as technology begins to merge crimes of the physical and cyber worlds.[194]

B. The "Other Criminal or Tortious Act:" Auto Theft

This Note will examine the need for the "substantial furtherance test" through the lens of car theft as the act of breaching the *Van Buren* "gate."[195] From 2019 to 2020, there was over a ten percent increase in the total number of motor vehicle thefts in the U.S.,[196] and from 2020 to 2021, there was an

188. Kerr, *supra* note 1, at 1561-67; Griffith, *supra* note 1, at 475-78.

189. Kerr, *supra* note 1, at 1561-67.

190. *Id.*

191. Kerr, *supra* note 1, at 1561-63 (Kerr's main concerns were over two cases in which "the government argued that violations of Terms of Service (TOS) render access to a computer unauthorized" and "an employee who accesses an employer's computer with illicit motives to hurt the employer accesses that computer without authorization," respectively).

192. *Id.*

193. *See* Van Buren, 141 S. Ct. at 1660-63.

194. Griffith, *supra* note 1, at 472-73 (Griffith notes that the Department of Justice and William G. Petty, "a representative of the National District Attorney's Association," both, "recommended the adoption of fraud language patterned after existing federal mail and wire fraud statutes because such legislation would be flexible enough to withstand advances in technology").

195. *Van Buren*, 141 S. Ct. at 1658-59.

196. Maggie Davis, *Vehicle Theft Statistics: Most Stolen Cars & Bikes by State*, VALUEPENGUIN (May 3, 2022 insert timestamp), https://www.valuepenguin.com/motor-vehicle-theft-statistics#:~:text=Since%201991%2C%20the%20overall%20level,1991%20to%20727%2C921%20in%202020 [https://perma.cc/9H9T-JWAJ].

additional six percent increase.[197] The total number of motor vehicle thefts in the U.S. at the end of 2021 was over 930,000.[198]

As motor vehicle thefts continue to rise, technology continues to improve within cars on the road today, but not only are security measures still being circumvented, but accessories inside vehicles are more valuable and useful to those stealing cars.[199] The concept of a "smart car" or a technologically advanced car is becoming more and more affordable at lower price points for consumers.[200] These services include Bluetooth capabilities, satellite radio access, and subscription-based navigation options.[201] As society becomes more reliant on the technology in automobiles, the necessity for their security and thus the security of the owner's personal data becomes increasingly important.[202]

C. Hypotheticals and Fact Pattern

The following hypotheticals illustrate the overbroad nature and potential for misapplication of the felony enhancements for § 1030(a)(2)(C), after the Supreme Court's decision in *Van Buren*.[203] The first hypothetical will illustrate how insignificant use of technology could still be considered a § 1030(a)(2)(C) violation, eligible for felony enhancement, and why the charging decision would be contradictory to the purposes of the CFAA and criminal punishment in general.[204] The second hypothetical will illustrate, using the same base crime of car theft, how the same type of access can be used to significantly further other criminal actions and why it is appropriate to apply the felony enhancements, to preserve the purposes of the CFAA and protect citizen privacy interests, as well as public safety and security of information.[205] These two extremes show how the proposed Substantial

197. NCIB, *NCIB Report Finds Vehicle Thefts Continue to Skyrocket in Many Areas of U.S.*, NAT'L INS. CRIME BUREAU (Sept. 1, 2022), https://www.nicb.org/news/news-releases/nicb-report-finds-vehicle-thefts-continue-skyrocket-many-areas-us [https://perma.cc/YTN7-UFEY].

198. *Id.*

199. Ironpaper, *Smart Car Statistics – The Increasingly Digital Experience of the Connected Vehicle*, IRONPAPER (July 18, 2018), https://www.ironpaper.com/webintel/articles/smart-car-statistics-the-increasingly-digital-experience-of-the-connected-vehicle [https://perma.cc/BV4B-6QRY]; s*ee also* Montaser N. Ramadan, et. al., *Intelligent Anti-Theft and Tracking System for Automobiles*, 2 INTERNATIONAL JOURNAL OF MACHINE LEARNING AND COMPUTING 88 (2012); FORD MOTOR COMPANY, *The Family of Ford Cars*, (last visited Apr. 9, 2023), https://www.ford.com/new-cars/?gnav=footer-all-vehicles [https://perma.cc/7QQD-ZNUK].

200. Ironpaper, *supra* note 199.

201. *Id.* (In 2014, it was estimated by CNBC that eighty-six percent of new cars included Bluetooth capabilities.).

202. YONG GOO KANG, ET. AL., AUTOMOBILE THEFT DETECTION BY CLUSTERING OWNER DRIVER DATA, 1, 2 (2019).

203. *Van Buren*, 141 S. Ct. at 1658-59.

204. *See also* Griffith, *supra* note 1, at 475-78; Simmons, *supra* note 186, at 1716; Kerr, *supra* note 186, at 1656, 1660-63.

205. *See also* Griffith, *supra* note 1, at 475-78; Simmons, *supra* note 186, at 1716; Kerr, *supra* note 186, at 1656, 1660-63.

Furtherance Test weeds out frivolous prosecution while protecting public safety and privacy.[206]

1. Hypothetical 1: The "Chop Shop"

One morning, in Arlington, Virginia, John Doe spots a late model Ford sedan on the street while walking to work and notes he has never seen the car parked there before.[207] Doe goes to work and leaves, spotting the same car on the street. The next day, he walks past the same car in the same spot and notices the same coffee cup left in the cup holder. This pattern continues for four days until finally, Doe decides the car is abandoned and ripe for taking. During his lunch break, Doe calls a friend who owns an automobile repair shop and is known to accept stolen goods from the street. Doe tells his friend about the car, and the two agree on a price if Doe can get the car to the body shop before it opens the next morning.

Waiting until the dark of night, Doe approaches the car and looks around to see if anyone is watching him. He manages to break into the parked car, surpassing the lock on the car door. Doe then hot-wires the car to start it and drives away. This act is grand larceny, punishable in Virginia by up to twenty years in prison.[208]

Immediately after Doe starts the car, the vehicle's computer system starts, and the dashboard is accessible.[209] On the dashboard, Doe notices a GPS application and decides to use the navigation system to direct him to the body shop,[210] or "chop shop," where the car will be stripped and sold for parts. He knew the address but decided it would be more convenient to use the GPS. He types in the address, and the car's navigation system takes him to the shop.[211] Once at his friend's chop shop, Doe receives his reward and leaves promptly. He is arrested a week later via security camera footage from a nearby convenience store. The chop shop is searched pursuant to a warrant and parts of the car are still found in the shop.

Doe decides it is in his best interest to plead guilty, given the overwhelming evidence against him. When entering his confession, Doe spares no details and tells police about the car's dashboard, using the navigation application and driving quickly to the chop shop. Doe is charged with one count of grand larceny with the intent to sell the stolen good(s).[212] This count is punishable by up to twenty years in prison.[213]

In examining the facts more closely, a young prosecutor called Jane Smith, looking at the case holistically, remembers the recent holding in *Van*

206. Kerr, *supra* note 186, at 1656, 1660-63.

207. *The Family of Ford Cars*, *supra* note 199.

208. VA. CODE ANN. § 18.2-95 (LEXIS 2022) (The car is presumably worth more than $2,500, thus satisfying the requirements of the statute.).

209. *Connected Navigation*, FORD MOTOR COMPANY: TECHNOLOGY (Apr. 2023), https://www.ford.com/technology/connected-navigation/?gnav=footer-connetedNav [https://perma.cc/88MD-KRJF].

210. *Id.*

211. *Id.*

212. VA. CODE ANN. §§ 18.2- 95 and 108.01 (LEXIS 2022).

213. *Id.*

Buren.[214] She remembers Arlington County's 2021 decrease in motor vehicle-related crimes and the Commonwealth Attorney's desire to continue to be diligent regarding car thefts to avoid Arlington falling in with the rising numbers of the rest of the nation.[215] She decides to reach out to the United States Attorney's Office for the Eastern District of Virginia, to learn more about the issue. The U.S. Attorney's Office decides to take the case on and investigate what charges they can bring.

Examining this situation involves looking at provisions 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii).[216] The first step in the analysis is whether the car or its navigation system is a computer, under the statute.[217] As discussed above, a computer is any machine or device with data processing or data storage capabilities.[218]

In examining the car's dashboard computer functionality,[219] the use of the navigation system is the main concern for the purposes of this Note. Accordingly, onboard subscription-based navigation applications, accessible through the dashboard, are most likely "computers" under § 1030(e)(1) because they process and store location data via a visual display to show the driver maps and step-by-step directions to their desired location.[220] Given the broad holdings of the courts' opinions in *Mitra* and *Kramer*, and that this is the general interpretation of most courts, an onboard GPS meets the definition of a computer.[221]

---

214. *Van Buren*, 141 S. Ct. at 1658-63.

215. Davis, *supra* note 196; Jo DeVoe, *Commonwealth's Attorney Touts Falling Rates of Carjackings, Car Thefts and Homicides in 2021*, ARLNOW (Jan. 6, 2022, 3:55 PM), https://www.arlnow.com/2022/01/06/commonwealths-attorney-touts-falling-rates-of-carjackings-car-thefts-and-homicides-in-2021/ [https://perma.cc/AT3K-842F].

216. 18 U.S.C. § 1030(a)(2)(C) (A violation of this section requires anyone who breaches authorized access or exceeds authorized access to obtain information from a protected computer.); *see also* 18 U.S.C. 1030(c)(2)(B)(ii) (This provision includes a felony enhancement for violations of (a)(2)(C), the most relevant of which is when the breach of access was in furtherance of another crime or tort.).

217. 18 U.S.C. § 1030(e)(1).

218. 18 U.S.C. § 1030(e)(1); *Mitra*, 405 F.3d at 495; *Kramer*, 631 F.3d at 903-05; KERR, *supra* note 29, at 82-83.

219. It is debatable whether a car is a computer or protected computer in and of itself because it operates as a mechanical apparatus, injecting fuel to function, but as cars become more dependent on Electronic Control Units to operate, they could be considered computers. However, "car hacking" or examining cars as protected computers is outside of the scope of this Note. Rick Cotta, *What Is an ECU?*, CARS.COM (Feb. 27, 2022), https://www.cars.com/articles/what-is-an-ecu-447580/ [https://perma.cc/A7FF-8JNX] (cars operate on Electronic Control Units or Engine Control Units (ECU) which means all of the car's processing functions from the braking, to fuel pumping, to the dashboard computer, are operational once the car's engine is ignited); *see generally* Bryson R. Payne, *Car Hacking: Accessing and Exploiting the CAN Bus Protocol*, 1 J. OF CYBERSECURITY EDUC., RSCH. AND PRAC., 2-5 (2019); *See generally* MARK BACCHUS, ET. AL., THE INSIGHTS INTO CAR HACKING (2014), https://api.semanticscholar.org/CorpusID:18719071 [https://perma.cc/EL7A-HZPJ].

220. *GPS Applications*, *supra* note 5 (GPS systems are operated by the U.S. government and use satellite data, transmitted to the user to provide location information.).

221. 18 U.S.C. § 1030(e)(1); *Mitra*, 405 F.3d at 495; *Kramer*, 631 F.3d at 903; KERR, *supra* note 29, at 82-83.

The next step in the process is that the government must show that the GPS is a protected computer.[222] The most critical factor for a car's GPS to be a "protected computer" is that the system relies on the global transmission of data.[223] According to GPS.gov, a U.S. government website run by the U.S. Space Force, GPS systems are connected to an international network "like the Internet" and "[are] an essential element of the global information infrastructure."[224] Subsequently, a GPS connecting to an international data network likely yields a similar result, in terms of connection to interstate commerce, that a laptop connecting to the Internet does, as per the reasoning in *Fowler, Yücel*, and *Hornaday*.[225] Thus, if GPS devices function like other computers, and their network impacts interstate commerce, they are likely to meet the low bar for a "protected computer."[226] Therefore, the last step is connecting a GPS device to interstate commerce or communication.[227] While the Supreme Court has not directly examined this issue, courts at the appellate and district level have found GPS devices to be included as instrumentalities of interstate commerce, specifically within the context of kidnapping statutes.[228] Additionally, GPS connects automobiles to a network that extends through state and national borders, thus heavily suggesting regulation under interstate commerce.[229]

After establishing the car's GPS as a protected computer, the government would next be required to prove that Doe breached authorized access or, in the eyes of the Court in *Van Buren*, breached clear gates that were up to prevent Doe from accessing the device.[230] After surpassing the car's locked doors and hot wiring the engine, Doe can then access whatever information is available on the dashboard.[231] The owner, through locking the car, clearly indicated they did not want another person to drive it or presumably use any of the car's applications or accessories.[232] This indication would likely satisfy the *Van Buren* standard because the owner established a physical barrier and their desire to not have others use their vehicle.[233]

Doe then continued to breach the security of the GPS or "protected computer" by starting the ignition.[234] The car's dashboard computer, with

222. 18 U.S.C. § 1030(a)(2)(C) and (e)(2)(A-B).

223. *GPS Applications*, *supra* note 5.

224. *Id.*

225. *Fowler*, 2010 U.S. Dist. LEXIS at *4-*8 (citing *Walters*, 182 Fed. App'x at 945; *Hornaday*, 392 F.3d at 1311; *Yücel*, 97 F. Supp. 3d at 419).

226. 18 U.S.C. § 1030(e)(2)(B).

227. *Id.*

228. 18 U.S.C.S. § 1201(a)(1); United States v. Morgan, 748 F.3d 1024, 1032 (10th Cir. 2014); United States v. Muller, No. 2:15-cr-0205, 2018 U.S. Dist. LEXIS 120186, (E.D. Cal. July 18, 2018).

229. *Fowler*, 2010 U.S. Dist. LEXIS at *4-*8; (citing *Walters*, 182 Fed. App'x at 945; *Hornaday*, 392 F.3d at 1311); *see also Yücel*, 97 F. Supp. 3d at 419.

230. *Van Buren*, 141 S. Ct. at 1658-60.

231. 18 U.S.C. § 1030(a)(2)(C) (the statute requires the violator to "[obtain] information from any protected computer" and in this case, the information Doe obtained was the directions to the "chop shop" after plugging in the address).

232. *Van Buren*, 141 S. Ct. at 1660-63.

233. *Id.*

234. *Id.*

access to several applications, starts when the engine is ignited.[235] With the ignition of the car directly causing the activation of the computer, the criminal trespass now merges with the barrier standard of *Van Buren*.[236] By breaking the locks on the car doors and starting the car's ignition, Doe breached authorized access to a protected computer.[237] Ultimately, Doe breached two gates: the door locks and protections against the ignition sequence.[238]

Lastly, to activate the felony enhancements under § 1030(c)(2)(B)(ii), the government must prove Doe furthered an underlying crime or tort.[239] As in *Steele*, where the defendant used his former employer's computers to steal valuable government contract information, thus committing grand larceny,[240] in this case, Doe used the GPS computer to pull up turn-by-turn directions to the "chop shop" and sell the stolen car, thus using a protected computer in "furtherance" of committing grand larceny with intent to sell.[241] Therefore, Doe's actions meet all the requirements of a § 1030(a)(2)(C) violation, with a felony enhancement under § 1030(c)(2)(B)(ii).[242]

The problem this hypothetical creates for society is that Doe can now be punished for frivolous use of technology and for an act that simply should not be considered illegal.[243] Substantively, Doe did not do anything more than he otherwise would have if he did not have a navigation system. Doe knew the address but simply decided it would be faster to plug in the address and get directions. If he simply drove to the shop or used his own smartphone for directions, he would not face an additional five years in prison for using a car GPS.[244] Additionally, in *Van Buren*, the Supreme Court refused to accept prosecutorial discretion as the only safeguard against frivolous or overbroad charging of the statute and chose to clarify the statute and legal standard through its holding.[245]

The potential for this charge to occur is unjust. The CFAA was intended to protect financial records and has since been developed to protect the broad privacy interest of citizens.[246] Additionally, almost twenty years before the issue was decided in *Van Buren*, Orin Kerr warned of the overbroad nature of § 1030(a)(2) leading to written agreements serving as barriers to authorized access and for individuals to be criminally liable for essentially breaching

235. FORD, *supra* note 209.

236. Van Buren, 141 S. Ct. at 1660-63.

237. *Id.*

238. *Id.*

239. *Steele*, 595 F. App'x at 216.

240. VA. CODE ANN. §§ 18.2- 95 AND 108.01 (LEXIS 2022); Steele, 595 F. App'x, at 216.

241. 18 U.S.C. § 1030(c)(2)(B)(ii).

242. *See* H. MARSHALL JARRETT ET. AL, PROSECUTING COMPUTER CRIMES 20 (Office of Legal Education Executive Office for United States Attorneys: Computer Crime and Intellectual Property Section Criminal Division 2017).

243. Doe is being punished for violation of 18 U.S.C. § 1030(a)(2)(C), but common knowledge suggests it is not illegal to use a GPS as an isolated incident.

244. 18 U.S.C. § 1030(c)(2)(B)(ii).

245. *Van Buren*, 141 S. Ct. at 1662 (The Court declared the need for statutory clarity through legislative action or jurisprudence by stating, "[t]he Government's approach would inject arbitrariness into the assessment of criminal liability.").

246. Griffith, *supra* note 1, at 475-78 (The CFAA has since developed into protecting more privacy interests than just financial documents.).

company policies.[247] Kerr argued that such a policy contradicted Congress's purpose to "limit the scope of criminal liability to conduct that satisfies both utilitarian and retributive goals."[248] Such goals "include deterrence, rehabilitation, and incapacitation."[249] Similarly, if unchecked, another overbroad provision within the CFAA could lead to punishment that contradicts the purposes of the act altogether, as outlined by Kerr.[250] The frivolous use of technology during a crime, such as typing a known address into a dashboard GPS, is not one society should be looking to deter with a potential five-year prison sentence.[251] In fact, GPS use is becoming more and more prevalent, so it seems absurd to criminalize such insignificant use during the theft.[252] Furthermore, the use of a GPS computer does not warrant rehabilitation because it is a legal act, if isolated, and a necessity in many occupations.[253] Doe's need for rehabilitation in this instance stems solely from the auto theft.[254] For that same reason, incarceration is unnecessary because the use of GPS harms no one.[255]

The possibility of charging Doe with a felony hacking violation for this GPS use illustrates the larger problem that these CFAA felony enhancements are much too broad.[256] The possibility of being charged for insignificant use of technology during a crime or tort must be eliminated by revising the statute to only apply to the knowing use of information acquired from a "protected computer" that substantially excels another criminal or tortious act.[257] Under the "Substantial Furtherance Test," the federal government would be unable to charge Doe with a § 1030(a)(2)(C) felony violation because Doe did not use the GPS navigation information to take a significant effort or "substantial step" to completing his sale of stolen goods.[258] He knew the "chop shop" and knew where it was. The GPS did not aid him in selling the car in any significant way; therefore, his use of the computer was not a knowing[259] act in "[substantial] [260] furtherance of any criminal or tortious act."[261]

2. Hypothetical 2: "Closer to Home"

While the substantial furtherance test absolves Doe of felony liability for his actions in the first hypothetical, it does not absolve him from using the same device to attempt or commit a crime he otherwise would not have been

247. Kerr, *supra* note 186, at 1656, 1660-63.
248. *Id.* at 1656.
249. *Id.* at 1656, 1660-63.
250. *Id.*
251. *Id.*
252. Kerr, *supra* note 186 at 1656, 1660-63; *GPS Applications*, *supra* note 5.
253. Kerr, *supra* note 186 at 1656, 1660-63.
254. *Id.*
255. *Id.*
256. 18 U.S.C. § 1030(c)(2)(B)(ii).
257. 18 U.S.C. § 1030(a)(2)(C); *Morris*, 928 F.2d at 509-11; *Taylor*, 142 S. Ct. at 2020.
258. 18 U.S.C. § 1030(c)(2)(B)(ii).
259. 18 U.S.C. § 1030(a)(5)(A); *Morris*, 928 F. 2d at 509-11.
260. *Taylor*, 142 S. Ct. at 2020; *see also Resendiz-Ponce*, 549 U.S. at 107; MODEL PENAL CODE § 5.01 CRIMINAL ATTEMPT (AM. L. INST. 2023).
261. 18 U.S.C. § 1030(c)(2)(B)(ii).

able to do without the information obtained from the GPS. In this second hypothetical, assume the same individual (John Doe) breaks into the same car under the same circumstances. However, this time, the car is a recently-made Ford model with a "Connected Navigation" subscription, and Doe notices a preset saved location in the owner's navigation app.[262] Doe then clicks on the location, believing it to be the owner's home, and drives to the house to see if there might be some added value to his escapade.[263] Doe assumes that since the car was relatively nice, the house is worth exploring as well. He uses the navigation to get back to the owner's house and sees no signs of alarms, dogs, or advanced home security.[264] From this point, Doe could cause considerable damage. He could break in and steal items or, far worse, if any individual is inside the house. For the sake of clarity, assume Doe breaks into the house, steals anything he can grab quickly, and then gets back in the car, selling his stolen goods to the chop shop owner, along with the car.

A week later, Doe is caught under the same circumstances as in the first hypothetical. He is charged this time with two counts of grand larceny with the intent to sell the stolen good(s) for the stolen car and the items he stole from the owner's house.[265] Both of these counts are punishable by up to twenty years in prison.[266] This time, the Commonwealth's Attorney is disturbed by the access to private information and that information led John Doe to the home of a family, who happened to be out of town.[267] Doe may or may not have been violent in that situation, but the potential is concerning, nonetheless. ACA Smith takes the same procedural path to the U.S. Attorney's Office, which once again decides to take the case on and investigate what charges they can bring.

Under the same analysis as the first hypothetical, the car's navigation system is a protected computer. Doe breached authorized access, and he obtained information to advance another crime or tort.[268] However, Doe's actions regarding the house appear to be much more extreme whether he intended to break into the car to obtain the physical address or not.[269] Under the proposed Substantial Furtherance Test, the government is required to prove that Doe used the information he obtained from the car's navigation computer[270] to knowingly[271] and substantially[272] "[further] any criminal or

---

262. FORD, *supra* note 209.

263. *Id.*

264. *Id.*

265. VA. CODE ANN. §§ 18.2- 95 and 108.01 (LEXIS 2022).

266. *Id.*

267. *Commonwealth Attorney Parisa Dehghani-Tafti*, ARLINGTON COUNTY VIRGINIA (2023), https://www.arlingtonva.us/Government/Departments/Courts/Commonwealth-Attorney/Meet-Parisa [https://perma.cc/9K8T-SVNT].

268. *Van Buren*, 141 S. Ct. at 1658-60; 18 U.S.C. § 1030(c)(2)(B)(ii).

269. 18 U.S.C. § 1030(a)(2); *Morris*, 928 F.2d at 506 (This case mostly deals with issues involving 1030(a)(5) issues with intent to cause damage, but it does clarify that the offender must "intentionally" breach access to the computer.).

270. 18 U.S.C. § 1030(a)(2)(C).

271. 18 U.S.C. § 1030(a)(5)(A); *Morris*, 928 F.2d at 509-11.

272. *Taylor*, 142 S. Ct. at 2020; *see also Resendiz-Ponce*, 549 U.S. at 107; MODEL PENAL CODE § 5.01 CRIMINAL ATTEMPT (AM. L. INST. 2023).

tortious act."[273] In this case, the information Doe received from the GPS was the car owner's home address. He would not have known that address without gaining access to the GPS by breaking through the car's locked doors and hot-wiring the ignition. He then used the information he obtained to go to the owner's home and burglarize or commit other heinous crimes. Doe knew, or reasonably should have known,[274] that an address labeled "Home" would be the owner's home address. He then used the information he received from the GPS to complete a "substantial step" in contributing to his intended crime of burglary by using the directions to go to the owner's house.[275] Therefore, under the Substantial Furtherance Test, and prior understandings of § 1030(a)(2)(C)'s felony enhancements, Doe could be charged and convicted of a hacking felony under the CFAA.[276]

Doe's violative use of technology to commit crimes of the physical world is exactly the type of act Congress was concerned with regulating when drafting began for the CFAA in the early 1980s because it violates someone else's privacy interests and puts personal data at risk.[277] It, therefore, satisfies the needs for "deterrence, rehabilitation, and incapacitation.[278] The critical difference between the two hypotheticals is that in the second one, Doe used someone else's computer to obtain information about them and then used that information to commit another crime.[279] In other words, Doe would not have gotten the owner's address without breaking into the car and gaining access to the GPS.[280] He then used that access to complete a crime he could have never even attempted without seeing the home address of the car owner saved in the GPS computer.[281] Conversely, in the first hypothetical, Doe knew about the chop shop already, and he knew the address. Even if the facts changed and he did not know the chop shop address, he already had a deal in place to sell the car and could presumably contact the buyer at any point. Despite the GPS making the process more convenient, Doe's attempted or completed effort to sell stolen goods is not initiated by the information displayed through the car's GPS, and the GPS use is frivolous in helping the process of furthering the separate crime.[282] In summary, the main difference is Doe obtained new and vital information from his breach of authorized access in the second hypothetical by finding someone's address.[283] He then used that new and vital

273. 18 U.S.C. § 1030(c)(2)(B)(ii).

274. 18 U.S.C § 1030(a)(5)(A); *Morris*, 928 F.2d at 509-11 (implied from the intended functionality of saved GPS locations labeled home).

275. *Taylor*, 142 S. Ct. at 2020; *see also Resendiz-Ponce*, 549 U.S. at 107; MODEL PENAL CODE § 5.01 CRIMINAL ATTEMPT (AM. L. INST. 2023).

276. 18 U.S.C. § 1030(a)(2)(C), § 1030(c)(2)(B)(ii).

277. Jarrett, *supra* note 242, at 19-20; s*ee generally* STEPHANIE RICKER SCHULTE, "THE WARGAMES SCENARIO" REGULATING TEENAGERS AND TEENAGED TECHNOLOGY 1-5 (1980–1984) (2008).

278. Kerr, *supra* note 186, at 1656, 1660-63.

279. *See* 18 U.S.C. § 1030(a)(2)(C), § 1030(c)(2)(B)(ii); *Van Buren*, 141 S. Ct. at 1660-1663 (2021).

280. FORD, *supra* note 209.

281. *Id.*

282. *See* 18 U.S.C. § 1030(a)(2)(C), § 1030(c)(2)(B)(ii); VA. CODE ANN. § 18.2-91 (LEXIS 2022); *Van Buren*, 141 S. Ct. at 1658-59.

283. *See* 18 U.S.C. § 1030(a)(2)(C); Jarrett, *supra* note 242, at 19-20; s*ee generally* SCHULTE, *supra* note 277, at 1-5.

information to complete another crime.[284] Society does not want individuals thinking they can break into cars, start them, and obtain personal information or location information to then break into someone's home, steal property, or cause physical injury.[285] Simply put, in the first hypothetical, Doe is not abusing the GPS, but in the second hypothetical, he is because he knowingly violated public trust.[286] The Substantial Furtherance Test still satisfies the goals of criminal punishment in the context of the CFAA because it limits punishment to acts that abuse technology or critical information obtained via unauthorized use while excluding the use of technology that is trivial in relation to a separate crime or tort.[287] Lastly, the test ensures the CFAA can more accurately regulate the potentially serious and dangerous offenses described in the second hypothetical, while not punishing simplistic uses of technology that do not aid in additional crimes as described in the first hypothetical.[288]

D. Looking Beyond the Limited Lens of GPS Devices

Simplistic GPS computers are much rarer today as people rely more and more on their smartphones for navigation.[289] Furthermore, most new cars, including newer Ford models, as well as Tesla cars, include a tablet-like device on the dashboard that is connected to the Internet and allows the driver to use various applications, similar to a smartphone.[290] These devices are connected to the Internet, and process and store data, thus making them protected computers.[291] Take the same facts as above, but imagine all of the personal identifying information contained on a smartphone or in a car's tablet.[292] The violations of privacy and potential "[furthered] criminal or tortious acts"[293] become much more vast. This dilemma that advancing technology creates increases the need for the Substantial Furtherance Test because the CFAA must be narrowed to accurately regulate computer crimes

284. *See Van Buren*, 141 S. Ct. at 1658-59.

285. *Id.*

286. Kerr, *supra* note 186, at 1660-63.

287. 18 U.S.C. § 1030(c)(2)(B)(ii); Griffith, *supra* note 186, at 476; Simmons, *supra* note 185, at 1716; Kerr, *supra* note 186, at 1656, 1660-63.

288. Kerr, *supra* note 186, at 1662.

289. *See* Amy He, *People Continue to Rely on Maps and Navigational Apps,* INSIDER INTEL. (July 18, 2019), https://www.insiderintelligence.com/content/people-continue-to-rely-on-maps-and-navigational-apps-emarketer-forecasts-show [https://perma.cc/Z4HY-SVD2].

290. FORD, *supra* note 209; *Dashcam, Sentry, and Security*, TESLA https://www.tesla.com/ownersmanual/models/en_us/GUID-49096E34-97D2-4182-9414-2F7F4E88EE79.html [https://perma.cc/36NC-78RE] (last visited Month Day, 2023).

291. FORD, *supra* note 209; *Dashcam, Sentry, and Security*, TESLA, *supra* note 290, (2023) https://www.tesla.com/ownersmanual/models/en_us/GUID-49096E34-97D2-4182-9414-2F7F4E88EE79.html [https://perma.cc/36NC-78RE]; *see Fordpass,* FORD MOTOR CO., https://www.ford.com/support/category/fordpass/fordpass-connect-wifi-hotspot/#:~:text=Download%20the%20FordPass%20App%20d,find%20the%20Vehicle%20Hotspot%20icon. [https://perma.cc/2Y22-KXLH] (last visited Nov. 6, 2023).

292. *See Connect iPhone to CarPlay*, APPLE, https://support.apple.com/guide/iphone/connect-to-carplay-iph6860e6b53/ios [https://perma.cc/XR4Z-ZDD3] (last visited Nov. 22, 2022).

293. 18 U.S.C. § 1030(c)(2)(B)(ii).

as they continue to merge with traditional crimes of the physical world.[294] The Test limits the felony enhancement to the use of information obtained from a protected computer[295] to knowingly[296] and substantially[297] "[further] any criminal or tortious act,"[298] thus not criminalizing computer use that is trivial to the separate crime or tort while continuing to punish violations of privacy and use of technology that directly aid the attempt or completion of the separate crime or tort,[299] in accordance with Congress's original intentions for the CFAA.[300]

V. CONCLUSION

The CFAA of 1986 was an admirable attempt at predicting and regulating the unimaginable modern world of technology based on the knowledge and understanding of the time period.[301] Through the benefit of hindsight however, it is clear Congress did not account for more complicated hacking issues such as GPS systems in cars to be potentially interpreted as computers, for the Supreme Court to simplify the language of § 1030(a)(2)(C) to the point of establishing a barrier for access to protected computers, and for the connection between a car door lock and the ignition system powering on a computer to merge a traditional crime of the physical world with federally regulated cybercrimes.[302] The decision in *Van Buren* brings with it the potential for abuse of prosecutorial discretion without focusing on protecting specific cyberspace targets, such as automobiles, especially as cars become more technologically advanced and integrated into society.[303]

This Note shows the necessity for modernizing the felony enhancement requirements for § 1030(a)(2)(C) violations to ensure individuals are not arbitrarily charged and punished for acts not otherwise deemed criminal while establishing a precedent for future protections of technologically advanced cars and the personal data they store.[304] The statutory language must be targeted at computer use that substantially furthers or is a critical component of an underlying crime or tort or when the personal information obtained from the protected computer is used directly to advance that criminal or tortious

294. Kerr, *supra* note 186, at 1656, 1660-63.

295. 18 U.S.C. § 1030(a)(2)(C).

296. 18 U.S.C. § 1030(a)(5)(A); *Morris*, 928 F.2d at 509-11.

297. *Taylor*, 142 S. Ct,. at 2020; *see also Resendiz-Ponce*, 549 U.S. at 107; MODEL PENAL CODE § 5.01 CRIMINAL ATTEMPT (AM. L. INST. 2023).

298. 18 U.S.C. § 1030(c)(2)(B)(ii).

299. *Id.*

300. *See* Kerr, *supra* note 186, at 1656, 1660-63.

301. *See generally* Kerr, *supra* note 1 *see also* Griffith, *supra* note 1.

302. 18 U.S.C. § 1030(a)(2)(C); *Van Buren*, 141 S. Ct. at 1658-1662; KERR, *supra* note 29.

303. *Van Buren*, 141 S. Ct. at 1658-59; Ironpaper, *supra* note 198, (July 18, 2018), https://www.ironpaper.com/webintel/articles/smart-car-statistics-the-increasingly-digital-experience-of-the-connected-vehicle [https://perma.cc/BV4B-6QRY]; s*ee generally* Kerr, *supra* note 1, at 1561-67.

304. *Van Buren*, 141 S. Ct. at 1658-59; Ironpaper, *supra* note 198, (July 18, 2018), https://www.ironpaper.com/webintel/articles/smart-car-statistics-the-increasingly-digital-experience-of-the-connected-vehicle [https://perma.cc/BV4B-6QRY]; s*ee generally* Kerr, *supra* note 1, at 1561-67.

end.[305] In other words, simple access in the process of committing a crime or tort, such as John Doe using the navigation system to get to the chop shop, should not be a federal felony punishable by up to five years, even if Doe stole the car.[306] However, using personal information stored on that navigation system, such as a physical address, for criminal gain should be deterred, and such punishment aligns with the original purpose of the CFAA.[307]

305. 18 U.S.C. §§1030(a)(2)(C) and (c)(2)(B)(ii).
306. *See generally* Kerr, *supra* note 1, at 1561-67.
307. *Id.*

From One Sector to Another: Applying a Proactive Framework to the FCC's Network Resiliency Efforts

Benjamin Duwve*

TABLE OF CONTENTS

* J.D., May 2024, The George Washington University Law School; B.A., May 2021, Political Science and Public Policy Analysis, The Ohio State University. Thank you to the entire team on FCLJ for their incredible work to make this publication possible. I would also like to thank Professor Emily Hammond for their research guidance and support throughout the writing process.

I. INTRODUCTION

You wake up in the middle of the night to your spouse shaking you. The destructive storms that have become all too familiar in your life are once again requiring you to evacuate to the basement of your home. As you walk down the stairs, the electricity shuts off, and you can hear the winds screaming against the side of the house. Just as you come down the stairs, you remember the last time this happened required you to stay in the basement for hours longer than you anticipated. Your spouse hands you their phone, and it shows that service has once again been lost. How will you stay connected with first responders? Do the batteries still work in your emergency radio? Let's hope that this storm quickly passes through.

In advance of such a situation, federal officials can make decisions that will help ensure communities remain connected to the communications network during extreme weather events. The Federal Communications Commission (FCC), through its support of network resiliency across the United States, can act to ensure network providers build networks that provide resilient services. Given the changing dynamics of extreme weather in the United States, the FCC should act to identify communication networks that need more support before destruction occurs.[1]

The FCC may find inspiration under a statutory mandate of the Department of Energy to meet these upcoming demands on our communications network. The Energy Policy Act of 2005 requires the Department of Energy to analyze the electric grid every three years to provide insight into areas of the grid that may need strengthening.[2] Congress acted to provide mechanisms to build new electric grid infrastructure, particularly giving the Department of Energy the ability to designate areas of the electric grid as National Interest Electric Transmission Corridors (National Interest Corridor).[3] The Department of Energy, every three years, must review congestion data on the areas of the electric grid and designate a National Interest Corridor if an area is too congested.[4] This proactive approach could inform how the FCC reviews the resiliency of the communications network in the United States.

The increasing prevalence of extreme weather events caused by climate change has harsh consequences for the future of the network communications infrastructure if the United States does not prepare. Extreme weather events will cause increasing damage in the coming decades, which poses risks to communications network infrastructure across the continental

1. *See* Daniel G. Huber & Jay Gulledge, *Extreme Weather & Climate Change: Understanding the Link and Managing the Risk*, CTR. FOR CLIMATE & ENERGY SOLS., at 3 (Dec. 2011), https://www.c2es.org/document/extreme-weather-and-climate-change-understanding-the-link-and-managing-the-risk/ [https://perma.cc/7PU2-ZP54] (explaining how the "narrative of extreme events over recent decades provides a few snapshots of a larger statistical trend toward more frequent and intense extreme weather events").

2. *See* Energy Policy Act of 2005, 16 U.S.C. § 824p(a) (2005).

3. *See id.* § 824p(a)(2).

4. *See id.*

United States.[5] In addition to the increased number of extreme weather events, sea level changes may carry consequences for potential shifts in human population that which would affect network usage in coastline areas and thus increase the need to adjust infrastructure to maintain network resiliency as coastline populations are forced to move inland.[6]

The FCC's actions to update the communications grid in preparation for extreme weather events created by climate change are inadequate and threaten Americans with loss of communications service during extreme weather. The Department of Energy has acted in response to the exact same threats from climate change outlined above by reviewing the power grid on a consistent basis.[7] The FCC should adopt the proactive approach that the Department of Energy exercises in reviewing the electric grid in consultation with state governments and industry stakeholders. Proactive solutions are necessary as unpredictable extreme weather creates vulnerabilities in the communications network across the United States.

This Note will analyze how the FCC can pull ideas from the Department of Energy's actions mandated by the Energy Policy Act of 2005 to develop their own regulatory framework to strengthen the resiliency of the United States' communications network. Part II.A will provide factual background on how extreme weather events affect the stability of the communications network. Part II.B and II.C will provide background on the FCC's work on the resiliency of communication networks and the recent start on analyzing the geographical reach of the current communications network. Part II.D will discuss the Department of Energy's statutory responsibility to collect data on the electric grid. Part III.A will analyze how extreme weather events have highlighted the vulnerability of certain areas of the communications network and how the FCC's current efforts are inadequate to address the growing issue. Part III.B and III.C will continue with proposals on how the FCC can adopt proactive measures, like the Department of Energy's reviews of the electric grid, to address vulnerabilities in the communications network.

---

5. *See* Jessica Weinkle et al., *Normalized hurricane damage in the continental United States 1900-2017*, 1 NATURE SUSTAINABILITY 808, 811 (2018) (indicating that as economic growth continues, "the United States should thus expect much greater hurricane damage in its future"); Michael Goss et al., *Climate change is increasing the likelihood of extreme autumn wildfire conditions across California*, 15 ENV'T RSCH. LETTERS 1, 12 (2020) (stating that "climate change can thus be viewed as a wildfire 'threat multiplier' amplifying natural and human risk factors that are already prevalent throughout California").

6. Teddy Grant, *UN secretary-general wans of impact of sea level rise, could cause 'mass exodus' of populations*, ABC NEWS (Feb. 15, 2023, 6:35 PM), https://abcnews.go.com/US/secretary-general-warns-impact-sea-level-rise-cause/story?id=97231697 [https://perma.cc/Q4XQ-MSJD] (noting that "nearly 900 million people who live in coastal zones" are at high risk for rising sea elevations).

7. *See* OFF. OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY, U.S. DEP'T OF ENERGY, ANN. U.S. TRANSMISSION DATA REV. MAR. 2018, at 1 (2018), https://www.energy.gov/oe/articles/annual-us-transmission-data-review-march-2018 [https://perma.cc/FJ37-Q4Q2].

II. BACKGROUND

A. Extreme Weather Events Affect the United States' Communications Network

When severe weather strikes a community, costs to repair can be upwards of hundreds of millions of dollars and leave extensive damage to a communications network.[8] Scientific American reported in 2020 that Internet service "interruptions caused by extreme weather events sap billions of dollars annually from the global economy."[9] In 2017, Hurricane Maria's "heavy winds caused extensive damage to . . . communications, transportation, and energy infrastructure" in Puerto Rico.[10] Hurricane Maria alone brought "damage that resulted in millions of people experiencing wireless, broadband, cable, and other telecommunications outages for months."[11] The National Oceanic and Atmospheric Administration's Office for Coastal Management states that between 1980 and 2021, the U.S. spent approximately $2.6 trillion on damages from "weather and climate disasters" as of August 2023.[12] Companies providing network communications services have recognized the need to strengthen their equipment in response to extreme weather events brought on by climate change.[13] Damages from more frequent extreme weather events across the United States will continue to bring high repair costs over the coming decades.[14]

Certain areas of the continental United States are more vulnerable to weather-related disruptions in their communications network, given their proximity to coastlines or disaster-prone regions. For example, Louisiana's communications network was left in disrepair for weeks following Hurricane Zeta in October 2020 and left the local population vulnerable to life-

8. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-297, FCC ASSISTED IN HURRICANE MARIA NETWORK RESTORATION, BUT A CLARIFIED DISASTER RESPONSE ROLE AND ENHANCED COMMUNICATION ARE NEEDED 26 (2021), https://www.gao.gov/assets/gao-21-297.pdf [https://perma.cc/U27K-KMEH] (finding that the FCC spent $601 million dollars repairing Puerto Rico and the U.S. Virgin Islands in the years following Hurricane Maria).

9. Daniel Cusick, *Wireless Technology Could Help Climate-Proof the Internet*, SCI. AM. (July 3, 2020), https://www.scientificamerican.com/article/wireless-technology-could-help-climate-proof-the-internet/ [https://perma.cc/YJC6-D56Y].

10. *Extreme Weather and Climate Change*, CTR. FOR CLIMATE & ENERGY SOLS., https://www.c2es.org/content/extreme-weather-and-climate-change/ [https://perma.cc/RYF6-VUV5] (last visited Jan. 12, 2023).

11. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 8, at 23.

12. *Hurricane Costs*, NAT'L OCEANIC ADMIN.'S OFFICE FOR COASTAL MGMT., https://coast.noaa.gov/states/fast-facts/hurricane-costs.html [https://perma.cc/6DHY-6YDM] (last visited Nov. 8, 2023).

13. *See* Diana Goovaerts, *Here's how AT&T, Verizon, Consolidated are prepping their networks for climate change*, FIERCE TELECOM (Mar. 11, 2022, 11:00 AM) https://www.fiercetelecom.com/telecom/att-verizon-consolidated-dish-preparing-their-networks-climate-change [https://perma.cc/LS9R-G9AX] (discussing how AT&T, Verizon, and Consolidated Communications are all planning to update technology used to provide communications services in response to climate change).

14. *See generally* Weinkle et al., *supra* note 5, at 811.

threatening crises.[15] These outages not only brought economic implications for the region but also further reached social impacts by affecting hospitals, local schools, and emergency responses from first responders.[16] Even regions of the United States that currently have a low risk for natural disasters may become vulnerable to the loss of communications capabilities as extreme weather becomes more unpredictable if infrastructure is not upgraded.

While extreme weather will never be completely predictable, the strain on the United States communication networks is already present.[17] Extreme weather can leave communities without reliable wireless connection for periods of time after the storm has cleared, which only highlights the lasting impacts of a weak communications infrastructure.[18]

B. FCC's Past Work on Ensuring Network Resiliency

The FCC has historically focused on ensuring universal communication service to every corner of the United States.[19] The Communications Act of 1934 stated that its purpose is "to make available, so far as possible, to all people of the United States . . . a rapid, efficient, Nation-wide, . . . communication service with adequate facilities."[20] The FCC has created a resilient network to withstand natural disasters through creating resiliency designed funding programs for regions struck by extreme weather and instituting the Mandatory Response Initiative.[21] Further, the FCC has built reporting procedures for service providers when communications service is disrupted.[22]

---

15. *See* Bailey Basham, *The South's communication infrastructure can't withstand climate change*, SOUTHERLY (Jan. 8, 2021) https://southerlymag.org/2021/01/08/the-souths-communication-infrastructure-cant-withstand-climate-change/ [https://perma.cc/FR43-8BWU].

16. *See id.*

17. *See id.*

18. *See id.* (noting that a Louisiana resident had unreliable Internet connection for many weeks following Hurricane Zeta).

19. *See Universal Service*, FED. COMMC'NS COMM'N, https://www.fcc.gov/general/universal-service [https://perma.cc/WJS7-KXU5] (last visited Nov. 13, 2022).

20. Communications Act of 1934, 47 U.S.C § 151 (1934).

21. *Bringing Puerto Rico Together (Uniendo a Puerto Rico) Fund and the Connect USVI Fund*, UNIVERSAL SERV. ADMIN. CO. [hereinafter *Bringing Puerto Rico Together*], https://www.usac.org/high-cost/funds/bringing-puerto-rico-together-uniendo-a-puerto-rico-fund-and-the-connect-usvi-fund/ [https://perma.cc/TUE9-AW73] (last visited Nov. 10, 2022); *see* Resilient Networks, et al., *Report and Order and Further Notice of Proposed Rulemaking*, 37 FCC Rcd 8059, para. 23-25 (2022) [hereinafter *Resilient Networks Report & Order, FNRPM*].

22. *See Network Outage Reporting System (NORS)*, FED. COMMC'NS COMM'N, https://www.fcc.gov/network-outage-reporting-system-nors [https://perma.cc/FWU9-EBD3] (last visited Nov. 18, 2022).

1. Disaster Response

The FCC is responsible for promoting uniform industry best practices and ensuring proper procedures are followed after network disruption.[23] The unreliability of these networks following natural disasters was prominent in the aftermath of Hurricane Katrina, as outlined by a report sent to the FCC which reviewed the hurricane's disruption of communication networks.[24] However, with regards to network resiliency, the report recommended that the FCC streamline requirements for restoring service (without addressing how to upgrade equipment so that the need for restoration is less likely).[25] Reports of this magnitude show the importance that the FCC has placed on response to natural disasters, but also highlight the reactive nature of seeking improvements in the communications network infrastructure after it's too late.

For example, the wireless industry adopted a Wireless Network Resiliency Cooperative Framework, which was codified by the FCC in large part on July 6, 2022 as the Mandatory Disaster Response Initiative.[26] The July 2022 order requires all "facilities-based mobile wireless providers" to comply with this framework.[27] The mandatory framework includes "providing for reasonable roaming under disaster arrangements . . . fostering mutual aid among wireless providers during emergencies . . . and improving public awareness and stakeholder communications on service and restoration status."[28] The framework binds participants to: 1) improve roaming during natural disasters; 2) improve assistance to other wireless providers during disasters; 3) work with local authorities to develop plans for disasters; 4) work with consumer groups to improve knowledge of how consumers can prepare for disasters; and 5) improve communication lines to the public for restoration updates.[29] The FCC's step in the right direction here creates a flexible mandate for wireless providers to deal with natural disasters, but does not make clear what metrics the FCC will specifically use to ensure compliance with the framework.

Outside of the Mandatory Disaster Response Initiative, targeted responses to disruptions have been done on a case-by-case basis through the establishment of funding programs. The FCC has created funding programs designed to directly support areas where network infrastructure is already under threat from extreme weather, such as the Bringing Puerto Rico Together

23. *See id.*
24. *See* Letter from Nancy J. Victory, Chair, Indep. Panel Reviewing the Impact of Hurricane Katrina on Commc'ns Networks, to Kevin J. Martin, Chairman, Fed. Commc'ns Comm'n (June 12, 2006) https://transition.fcc.gov/pshs/docs/advisory/hkip/karrp.pdf [https://perma.cc/4VVW-S4SF] (noting "that lack of effective first responder communications after the storm revealed inadequate planning, coordination, and training on the use of technologies that can help restore emergency communications").
25. *See id.* at 33.
26. Resilient Networks Report & Order, FNRPM, *supra* note 21, at para. 23.
27. *Id*. at para. 3.
28. *Id*. at para. 5.
29. *See id*. at para. 5.

(Uniendo a Puerto Rico) Fund and Connect USVI Fund (PR/USVI Fund).[30] The PR/USVI fund helps "support the restoration, expansion and upgrade of fixed and mobile communications networks" in Puerto Rico and the U.S. Virgin Islands.[31] Since the fund's creation, the FCC has allocated over $1 billion to strengthen mobile networks in those two areas.[32] The funding, broken into two stages, has gone directly to carriers in a mix of emergency funding to restore service, and funding to ensure communications networks stay online during future extreme weather.[33]

To receive Stage 2 funding, a provider must have a Disaster Preparation and Response Plan, which includes "details on how a carrier will strengthen its infrastructure, ensure network diversity and backup power, monitor its network and plan for an emergency."[34] Requirements of this nature are a positive step for building resilient infrastructure and require providers to proactively plan for disasters. However, these funding programs have only been applied retroactively to at-risk areas.

To further the PR/USVI fund, the FCC adopted a Further Notice of Proposed Rulemaking ("FNPRM") on October 27, 2022, which proposed "extending universal service support for mobile and fixed service providers beyond 2023."[35] Following Hurricane Fiona's destruction, the FNPRM acknowledged that "infrastructure in areas prone to hurricanes must be built to withstand storm damage and have redundant capabilities."[36] However, this action to provide interim support to the region is limited to Puerto Rico and the U.S. Virgin Islands.[37] Here, the FCC is recognizing a need for additional support by providing resources after the destruction of critical network infrastructure. The FCC also commented on buildout requirements for resilient network infrastructure, requiring forty percent buildout by December 2024 and twenty percent for each year after for carriers who are awarded fixed support to build out their network infrastructure.[38] This demonstrates the challenges of upgrading the infrastructure in an expedient manner while also recognizing the burden that upgrades create on providers and local authorities.

These actions indicate that the FCC's approach to disaster control does not predominantly include proactive infrastructure requirements across the continental United States. Frameworks and funding have been adopted for some disaster-prone regions, but more is necessary to combat unpredictable extreme weather.

---

30. *See Bringing Puerto Rico Together*, *supra* note 21; *see also* The Uniendo a Puerto Rico Fund and the Connect USVI Fund, et al., *Order and Notice of Proposed Rulemaking*, 33 FCC Rcd 5404, para. 1 (2018).

31. *Bringing Puerto Rico Together*, *supra* note 21.

32. *See id*.

33. *See id*.

34. *Id*.

35. The Uniendo a Puerto Rico Rund and the Connect USVI Fund; Connect America Fund, *Further Notice of Proposed Rulemaking*, 37 FCC Rcd 13411, para. 15 (2022).

36. *Id.* at para 1.

37. *See id.* at para. 2.

38. *See id.* at para. 21.

2. Outage Reporting

In addition to responding to network disruptions following a disaster, the FCC has other mechanisms in place for reactively responding to outages to quickly reestablish service. The FCC has created a set of guidelines for service providers when responding to everyday outages. In 2004, the foundations of the FCC's Network Outage Reporting System (NORS) addressed "the critical need for rapid, complete, and accurate information on significant communications service disruptions."[39] Providers are required to report outages that affect 911 facilities within four hours, or any outage that potentially affects 900,000 user minutes and completely removes service within twenty four hours.[40] The FCC notes that the Public Safety and Homeland Security Bureau's Cybersecurity and Communications Reliability Division analyzes the received outage data to review for trends and provides solutions to prevent outages in the future.[41]

Besides NORS, the FCC has systems in place to allow for data transfer to occur as natural disasters create network outages. The FCC discusses a program known as the Disaster Information Reporting System (DIRS), which allows "service providers . . . to voluntarily report to the Commission their communications infrastructure status, restoration information, and situational awareness information specifically during times of crisis."[42] The FCC states that NORS and DIRS together are "vital public safety tools" which prepare the FCC to act quickly with federal and local authorities in emergency situations.[43] These programs together show the FCC's willingness to work with service providers and create the best mechanisms for data collection.

However, the FCC suggests that smaller providers have trouble participating in this program and states that providers report outage information in DIRS on a voluntary basis once the system is activated.[44] The FCC expressly sought comment on whether making DIRS mandatory is within their legal authority and recognized the potential burdens for providers to file their information while remaining focused on reconnecting service.[45] As of the time of this writing, the future of rulemaking proceedings considering changes to NORS remains pending. However, the FCC sought comment on how data collected from NORS could potentially identify "broadband outage trends," which may suggest their inclination to use this tool in the future to spot areas of the network infrastructure that need additional support.[46]

These outage reporting requirements provide data for the FCC to later review, especially on the when and where of network disruptions. While not

---

39. *See Network Outage Reporting System (NORS)*, *supra* note 22.
40. *See id*.
41. *See id*.
42. *See* Resilient Networks et al., *Notice of Proposed Rulemaking*, 36 FCC Rcd 14802, para. 5 (2021) [hereinafter *Resilient Networks NPRM*].
43. *Id.* at para. 27.
44. *Id.* at para. 27.
45. *Id.* at para. 29.
46. *Id.* at para. 30.

every disruption can be planned for, the guidelines for disruptions highlight that there is a continuous need for infrastructure improvements. Further, DIRS, even though it helps increase the FCC's awareness of the status of communication infrastructure during a disaster, does not help the FCC work proactively with service providers to alleviate strain on communication infrastructure.

C. FCC's Statutorily Mandated Efforts on Broadband Data Collection

The FCC has recognized "the need for accurate data pinpointing where broadband service is available, and where it is not available, has never been greater."[47] In 2019, the FCC began the Digital Opportunity Data Collection (later becoming the Broadband Data Collection), which aimed to "gather geospatial broadband service availability data specifically targeted towards advancing our universal service goals."[48] This data collection has evolved since its creation in response to, in the words of FCC Chairwoman Jessica Rosenworcel, "complaints that we lack detailed maps to tell us exactly where broadband is–and is not–available."[49]

1. Data Collection Process and a New Statutory Mandate

Congress, in response to a lack of organized data on the availability of broadband service, passed the Broadband Deployment Accuracy and Technological Availability Act (Broadband DATA Act) in March 2020 which required the FCC to create maps of broadband service across the United States.[50] These maps must be updated at least twice a year.[51] Congress likely intended for the Broadband DATA Act to boost the FCC's focus on providing broadband service to rural Americans.[52] However, the statute will benefit all

47. *Broadband Data Collection*, FED. COMMC'NS COMM'N, https://www.fcc.gov/BroadbandData [https://perma.cc/3CJL-QVPR] (last visited Nov. 6, 2022).

48. Establishing the Digital Opportunity Data Collection; Modernizing the FCC Form 477 Data Program, *Report and Order and Second Further Notice of Proposed Rulemaking*, 34 FCC Rcd 7505, 2 (2019) [hereinafter *Digital Opportunity Data Collection*].

49. Jessica Rosenwercel, *Status Update: Mapping Where Broadband Is–and Is Not–Available in the U.S.*, FED. COMMC'NS COMM'N (June 30, 2022), https://www.fcc.gov/news-events/notes/2022/06/30/status-update-mapping-where-broadband-and-not-available-us [https://perma.cc/L8WE-YXVC].

50. *See* Broadband Deployment Accuracy and Technological Availability Act, 47 U.S.C. §§ 641-46 (2020).

51. *See id.* § 642(c)(3) (requiring the FCC to "update the maps created . . . not less frequently than biannually using the most recent data").

52. *See Bill to Improve Broadband Data Maps Signed Into Law*, U.S. SENATE COMM. ON COM., SCI., & TRANSP. (Mar. 23, 2020), https://www.commerce.senate.gov/2020/3/bill-to-improve-broadband-data-maps-signed-into-law [https://perma.cc/F596-RKY2] (discussing how many rural communities lack access to broadband and how the DATA Act will "help deploy service to the estimated 20 million Americans without access to broadband").

stakeholders in the process and requires establishing a "crowdsourcing process" for the data collection efforts.[53]

The Broadband DATA Act mandates that the FCC create a process through which stakeholders "may submit specific information about the deployment and availability of broadband Internet access services in the United States on an ongoing basis."[54] The statute, thus, does not mandate input from certain stakeholder groups but requires the FCC to receive information from anyone who chooses to submit it. This part of the statute also highlights that Congress likely intended for this mandate to continue into the future. The goal of rural broadband access and expansion of universal service generally will need to be a continual goal that the FCC weaves into its broader actions. Finally, this section also leaves open how the FCC will choose to interact with these stakeholders and to define "specific."[55] This leaves service providers with an avenue to ensure their inputs are heard in the process and also leaves unclear what kind of information is required per the statute. The FCC could expand the scope of information collected from stakeholders to include information related to the climate resiliency of their infrastructure.

Following passage of the Broadband DATA Act, Acting Chairwoman Jessica Rosenworcel established a Broadband Data Task Force to lead the FCC's efforts on collecting and compiling data on broadband availability across the United States.[56] Since then, the Broadband Data Task Force held technical workshops to ensure that providers of data understood how to upload the information.[57] These workshops demonstrate the FCC's goals for collecting a broad set of data and encouraging as many industry stakeholders as possible to take part in the process as outlined by the Broadband DATA Act.

Following these trainings, the Broadband Data Task Force opened windows for facilities-based broadband service providers to file their data with the FCC.[58] The FCC's data collection previously relied on service providers, the public, and other governmental entities to provide information on broadband service availability directly to the FCC, and the new filing

53. *Id.*

54. 47 U.S.C. § 644(b)(1).

55. *Id.*

56. *See* Press Release, Federal Communications Commission, Acting Chairwoman Rosenworcel Establishes Broadband Data Task Force (Feb. 17, 2021), https://www.fcc.gov/document/rosenworcel-establishes-broadband-data-task-force [https://perma.cc/WYF8-ELPF].

57. *See* Federal Communications Commission, *Broadband Data Task Force Webinar*, YOUTUBE (Aug. 12, 2021), https://www.youtube.com/watch?v=G8Ov3nJxlnc [https://perma.cc/E6DQ-M7T3]; Federal Communications Commission, *Broadband Data Collection Tribal Governments' Technical Assistance Workshop*, YOUTUBE (Dec. 8, 2021), https://www.youtube.com/watch?v=MoZln03GT5w [https://perma.cc/FN3H-XVXF].

58. *See* Inaugural Filing Window for Broadband Data Collection Has Opened, *Public Notice*, 37 FCC Rcd 7656, 1 (2022) [hereinafter *Inaugural Filing Window*]; The Broadband Data Task Force Announces the Opening of the Second Broadband Data Collection Window, *Public Notice*, 37 FCC Rcd 15161, 1 (2022).

system continued each stakeholder's involvement.[59] The FCC does not reveal which stakeholders ended up submitting data, which may raise issues later if certain stakeholders are included less in the process than needed.

On November 18, 2022, the FCC created its first National Broadband Map, which is the "most detailed data on broadband availability the FCC has ever collected or released."[60] This map will meet Congress' needs as stated in the Broadband DATA Act but will surely lead to further decisions on the usage of this data and policy recommendations. The FCC states that the "Broadband Data Collection (BDC) program will give the FCC, industry, state, local, and Tribal government entities, and consumers the tools they need to improve the accuracy of existing maps."[61] The FCC has not clearly stated its own specific goals for the data; however, the FCC will surely use the Broadband Map to continue its mission of providing universal broadband service.

D. The Department of Energy's Statutorily Mandated Response to Instability in the Electric Grid

As a result of an unprecedented energy blackout, Congress passed the Energy Policy Act of 2005, which requires the Department of Energy to proactively study the electricity grid every three years.[62] The Department of Energy's Office of Electricity states that "a secure and resilient power grid is vital to national security, economic security, and the services Americans rely upon."[63] The regulation of the energy grid is complex and incorporates the Federal Energy Regulatory Commission ("FERC"), which regulates the interstate sale of electricity and transmission rates.[64] To ensure grid stability, especially as strain on the grid grows, Congress required the Department of Energy to identify places of concern on the grid in a proactive manner.[65]

59. *See* Digital Opportunity Data Collection, *supra* note 48, at 2; Inaugural Filing Window, *supra* note 58, at 1.

60. *FCC National Broadband Map*, FED. COMMC'NS COMM'N, https://broadbandmap.fcc.gov/home [https://perma.cc/D8TW-5DA9] (last visited Apr. 9, 2023); Press Release, Federal Communications Commission, National Broadband Map Fact Sheet, 1 (Nov. 18, 2022), https://www.fcc.gov/document/national-broadband-map-fact-sheet [https://perma.cc/PDL9-MJZM].

61. *Broadband Data Collection*, *supra* note 47.

62. *See* Energy Policy Act of 2005, 16 U.S.C. § 824p(a) (2005).

63. *Office of Electricity*, U.S. DEP'T OF ENERGY, https://www.energy.gov/oe/office-electricity [https://perma.cc/3SDW-J37N] (last visited Nov. 5, 2022).

64. *See What FERC Does*, FED. ENERGY REGUL. COMM'N, https://www.ferc.gov/what-ferc-does [https://perma.cc/V8UG-DFEB] (last visited Dec. 13, 2023).

65. 16 U.S.C. § 824p(a)(2).

1. History of the United States Electric Grid

The electric grid in the United States began as a collection of local electricity transmission lines in the late 19th century.[66] At the start of the 20th century, "AC and long-distance transmission encouraged the consolidation of electric utilities" and began the development of interstate transmission lines.[67] However, the localized operation of electric utilities changed rapidly, where "by the late 1920s, the sixteen largest electric power private holding companies, . . . controlled more than 75% of all U.S. generation."[68] The rapid growth of interstate power transmission led to confusion among the state regulatory utility commissions regarding which bodies could regulate certain flows of electricity, which resulted in the Supreme Court holding that states were unable to regulate interstate transmission under the dormant commerce clause.[69]

In response to the Supreme Court's decision, Congress passed the Federal Power Act in 1935 and assigned the Federal Power Commission, now FERC, the power to regulate interstate transmission of electricity.[70] FERC is "an independent agency that regulates the interstate transmission of electricity, natural gas, and oil."[71] FERC approves rates for sales of electricity in interstate commerce and aims to support investment in the nation's electricity grid infrastructure.[72] The energy grid is now also regulated through a collection of regional operators known as regional transmission organizations, which oversee the electric grid in their region and manage wholesale power sales.[73]

The United States recognized energy production as one of its top priorities in 2005 with the passage of the Energy Policy Act of 2005, and the

66. *See* Alexandra B. Klass, *The Electric Grid at a Crossroads: A Regional Approach to Siting Transmission Lines*, 48 U.C. DAVIS L. REV. 1895, 1910 (2015) (noting that San Francisco was the first city in the world in 1879 that had an electricity generating station which distributed electricity to numerous lamps in the city).

67. *Id.* at 1911.

68. *Id.* at 1914.

69. *See id.*; Pub. Utils. Comm'n of R.I. v. Attleboro Steam & Elec. Co., 273 U.S. 83, 89 (1927) (holding an order from the Public Utilities Commission of Rhode Island that created a schedule of prices for the interstate sale of electricity an "imposition of a direct burden upon interstate commerce, from which the state is restrained by the force of the commerce clause, it must necessarily fall, regardless of its purpose").

70. *See* Federal Power Act, 16 U.S.C. § 824(b)(1) (2012); Klass, *supra* note 66, at 1914.

71. *What FERC Does*, *supra* note 64.

72. *See Electric*, FED. ENERGY REGUL. COMM'N, https://www.ferc.gov/electric [https://perma.cc/8XCJ-U7CL] (last visited Jan. 17, 2023); *Electric Transmission*, FED. ENERGY REGUL. COMM'N, https://www.ferc.gov/electric-transmission [https://perma.cc/984B-FEUP] (last visited Jan. 17, 2023).

73. *See* Alexandra B. Klass & Elizabeth J. Wilson, *Interstate Transmission Challenges for Renewable Energy: A Federalism Mismatch*, 65 VAND. L. REV. 1801, 1808 (2012).

issue has continued as one of intense political debate.[74] Strains on the electricity grid affect everyday life through blackouts, which occur for a variety of reasons but can have serious consequences for end users who rely on electricity supply for safety reasons.[75] New sources of electric power are debated and are balanced with their cost and potential for strain on the electricity grid (among many other factors), especially as the effects of climate change bring attention to clean energy sources.

2. The Department of Energy's Framework in Establishing National Interest Electric Transmission Corridors

On August 14, 2003, the largest electricity blackout in the nation's history occurred after a group of power plants and transmission lines shut off.[76] Following this, the instability in the grid from the offline power plants and transmission lines resulted in additional power plant outages that grew to affect customers across the United States and Canada.[77] Some of the estimated 50 million customers lost power for only a few hours, but the power outages continued for several days in some areas.[78] The blackouts resulted in estimates of billions of dollars of lost productivity and revenue.[79] The catastrophe prompted Congress to request briefing on the causes of the incident, with the Government Accountability Office recommending greater regulation and security for the growing electricity markets in its report to the Committee on Governmental Affairs.[80] The severe consequences of the blackouts also prompted investigations from the federal government and state governments, including a joint U.S.-Canadian team.[81]

---

74. *See* Presidential Statement on Signing the Energy Policy Act of 2005, 41 WEEKLY COMP. PRES. DOC. 1267 (Aug. 8, 2005) https://www.govinfo.gov/content/pkg/WCPD-2005-08-15/pdf/WCPD-2005-08-15-Pg1267-2.pdf [https://perma.cc/TK9A-ZEGQ] (President Bush writing in his signing statement that "this legislation promotes dependable, affordable, and environmentally sound production and distribution of energy for America's future"); Energy Policy Act of 2005, 16 U.S.C. § 824p(a) (2005); *Presidential Debate at Belmont University in Nashville, Tennessee*, COMM'N ON PRESIDENTIAL DEBATES, https://www.debates.org/voter-education/debate-transcripts/october-22-2020-debate-transcript/ [https://perma.cc/CC6R-CW3N] (last visited Nov. 5, 2022) (Then President Donald Trump and then presidential candidate Joseph Biden debate over usage of evolving sources of energy and whether the United States is truly energy independent.).

75. U.S. GOV'T ACCOUNTABILITY OFF., GAO-04-204, ELECTRICITY RESTRUCTURING: 2003 BLACKOUT IDENTIFIES CRISIS AND OPPORTUNITY FOR THE ELECTRICITY SECTOR 9 (2003), https://www.gao.gov/assets/gao-04-204.pdf [https://perma.cc/B4UN-4FW8] (noting that the 2003 Blackout, at that point the largest in the nation's history, affected an estimated 50 million customers, air and ground transportation systems, water systems, 911 communications, and cellular networks).

76. *See id.* at 1-2.

77. *See id.* at 2.

78. *See id.* at 1-2.

79. *See id.* at 2.

80. *See id.* at 1-4.

81. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 75, at 9.

In response to the 2003 blackouts' wide impacts, Congress passed the Energy Policy Act of 2005, which stated the Department of Energy "in consultation with affected States, shall conduct a study of electric transmission congestion."[82] The statute allows the Secretary of the Department of Energy to label any area of the electricity grid as a National Interest Corridor as long as the area is currently experiencing or will experience "energy transmission capacity constraints or congestion."[83] The Secretary, in considering whether to label an area of the electricity grid as a National Interest Corridor, must consider, among other factors related to the energy security of the region, whether the region is "jeopardized by reliance on limited sources of energy."[84] Both the consideration of potential constraints and a review of the vulnerabilities of the electric grid emphasize the forward-looking nature of this study.

When the Department of Energy designates a National Interest Corridor, the Energy Policy Act of 2005 gives FERC the authority, after opportunities for notice and comment, to issue permits as a backstop to traditional state siting authority, the application for building the new transmission line does not serve-end users in the state, or when a state regulatory commission failed to act within one year on an application for new transmission lines.[85] While this regime does not allow FERC to immediately act following a National Interest Corridor designation, it provides an avenue for FERC to, in a reasonable time, act instead of the State commission if the construction of improved transmission lines is delayed.[86] FERC cannot unilaterally order the construction of new transmission lines but is given greater capacity to take actions to work towards decongestion of the grid if other actors in the process fail to do so.[87]

The initial study, released in 2006, shows how the FCC can better construct reviews of this kind. The study, as mandated by the Energy Policy Act of 2005, examined the electricity transmission across the entire country using historical analysis and modeling of transmission lines.[88] The study relied on a collection of data pulled from sources including testimony from regional transmission organizations, reports from FERC and the Department of Energy, staff reports from state public service commissions, and publicly available data from regional transmission organization and individual

82. Energy Policy Act of 2005, 16 U.S.C. § 824p(a)(1) (2005); *see* U.S. DEP'T OF ENERGY, NATIONAL ELECTRIC TRANSMISSION CONGESTION STUDY, v (2020), https://www.energy.gov/oe/articles/2020-national-electric-transmission-congestion-study [https://perma.cc/R4NE-XB6B].

83. 16 U.S.C. § 824p(a)(2).

84. *Id.* § 824(p)(a)(4) (this phrase has never been directly defined, but suggests the region is reliant on either relatively few sources of energy or unreliable sources of energy).

85. *See id.* § 824(p)(b).

86. *See id.*

87. *See id.*

88. *See* U.S. DEP'T OF ENERGY, NATIONAL ELECTRIC TRANSMISSION CONGESTION STUDY, vii (2006), https://www.energy.gov/sites/default/files/oeprod/DocumentsandMedia/Congestion_Study_2006-9MB.pdf [https://perma.cc/83EZ-LLA2].

transmission projects.[89] The modeling used in the study incorporated simulations of future estimated congestion at both the eastern and western halves of the country by looking at various years within the following decade.[90] The 2006 study even proposed areas where new sources of energy could be built to improve the "economy, and enhance the Nation's energy security and fuel diversity."[91] The Department of Energy sought comment on "any and all aspects of the study and the potential designation of National Corridors," in addition to: whether designating certain National Corridors would be in the public interest, how the Department of Energy should establish geographic boundaries for designated National Corridors, and how to best allocate costs of proposed transmission facilities.[92] Following the 2006 study, the Secretary of the Department of Energy designated the Mid-Atlantic National Corridor and the Southwest Area National Corridor as National Interest Corridors.[93]

Following the first National Electric Transmission Congestion Study in 2006 and its designation of two National Interest Corridors, stakeholders challenged the legal authority of the Department of Energy and FERC to act in response to their designations. The Fourth Circuit held that FERC did not have statutory authority to act after a state denied a permit within a one-year timeline, but only when "action on a permit application has been held back continuously for more than one year."[94] Here, FERC had issued a final rule following notice and comment rulemaking procedures, which was challenged by two state public service commissions and two community interest organizations.[95] This interpretation by the courts limited the ability of FERC to act quickly to build new transmission lines, with the Fourth Circuit holding that Congress would have directly stated if it intended to allow FERC to issue permits "*every time* a state commission denies a permit in a national interest corridor."[96] Additionally, this case further highlights how stakeholders will challenge rulemaking procedures that are unfavorable to their business.

Two years later, the Ninth Circuit vacated the Department of Energy's first National Interest Corridor designation, holding that the Department of Energy did not provide analytical models to state governments or directly solicit the input of state government leadership on the creation of the study as required by statute.[97] Here, the Court held that the Department of Energy

89. *See id.* at 95-103.

90. *See id.* at 27, 36.

91. *See id.* at 53, 55, 56, 58 (proposing areas for the development of wind energy in the Dakotas and Minnesota and proposing areas for the development of nuclear energy in the Southeastern United States).

92. *See id.* at 59-60.

93. *See* U.S. DEP'T OF ENERGY, NATIONAL ELECTRIC TRANSMISSION CONGESTION STUDY, vii (2009), https://www.energy.gov/sites/default/files/Congestion_Study_2009.pdf [https://perma.cc/AE37-HPZE].

94. Piedmont Env't Council v. Fed. Energy Regul. Comm'n, 558 F.3d 304, 315 (4th Cir. 2009).

95. *See id.* at 309.

96. *Piedmont Env't Council*, 558 F.3d at 314 (emphasis in original).

97. *See* Cal. Wilderness Coal. v. U.S. Dep't of Energy, 631 F.3d 1072, 1085-86, 1095 (9th Cir. 2011).

failed to meet the Energy Policy Act of 2005's mandate of preparing the study "in consultation with affected States" when the agency used a deliberate "decisionmaking process that was contrary to that mandated by Congress and one that deprived the Department of Energy of timely substantive information."[98] This case highlights that courts will likely look unfavorably upon agencies who do not work with state authorities when such cooperation is suggested by statute.

The Department of Energy, since the Energy Policy Act of 2005's inception, has continued to conduct congestion studies but has not designated a National Interest Corridor since the initial findings from the 2006 study.[99] In 2022, the Department of Energy garnered attention with its plan to use its revivified statutory authority under the Energy Policy Act of 2005 as modified by the Infrastructure Investment and Jobs Act.[100] The congestions studies are now referred to as a National Transmission Need Study and the Biden administration released a 2023 study in October 2023.[101] The recent statutory modifications, after mixed success in the past, suggests that proactive approaches of this kind will likely evolve as agencies struggle with responding to the climate change crisis if state regulatory bodies refuse to enact change.[102]

The Department of Energy has separately conducted annual transmission data reviews, which provide "an integrated summary of publicly available data and information on . . . factors affecting the U.S. transmission system."[103] The Department of Energy cites a "broad responsibility for developing and supporting the implementation of energy policies" as authority for these annual reports.[104] While these reviews give no conclusions

98. 16 U.S.C. § 824(p)(a)(1); *Cal. Wilderness Coal.*, 631 F.3d at 1095.

99. *See* U.S. DEP'T OF ENERGY, *supra* note 93, at vii; U.S. DEP'T OF ENERGY, NATIONAL ELECTRIC TRANSMISSION CONGESTION STUDY, 5 (2015), https://www.energy.gov/sites/default/files/2015/09/f26/2015%20National%20Electric%20Transmission%20Congestion%20Study_0.pdf [https://perma.cc/TAM7-PXSF]; U.S. DEP'T OF ENERGY, NATIONAL ELECTRIC TRANSMISSION CONGESTION STUDY, 2 (2020), https://www.energy.gov/oe/articles/2020-national-electric-transmission-congestion-study [https://perma.cc/8FE6-BZZ5].

100. *See* Daniel Moore, *States Balk at Permitting Plan's 'National Interest' Power Lines*, BLOOMBERG L. (Sept. 16, 2022, 5:30 AM), https://news.bloomberglaw.com/environment-and-energy/states-balk-at-permitting-plans-national-interest-power-lines [https://perma.cc/F3XQ-LU2P] (discussing how the designation of National Corridors could support the connection of new sources of clean energy and how statutory changes would permit FERC to issue construction permits); Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 429, 933-34, 939 (2021), https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf [https://perma.cc/NS44-8HWP].

101. U.S. DEP'T OF ENERGY, NATIONAL TRANSMISSION NEEDS STUDY, ii (2023), https://www.energy.gov/sites/default/files/2023-12/National%20Transmission%20Needs%20Study%20-%20Final_2023.12.1.pdf [https://perma.cc/B394-3QJX].

102. *See* Moore, *supra* note 100 (noting the Biden administration's sense of urgency with creating new electric transmission lines).

103. *See* OFF. OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY, U.S. DEP'T OF ENERGY, *supra* note 7, at 1.

104. *Id.* (the report specifically cites the Energy Policy Act of 2005's requirement for a study of the electric grid every three years as statutory support).

from the analyzed data, the reviews bring awareness to stakeholders of the operation costs and congested areas of the electric grid.[105] These reviews include an analysis of the constraints and costs of congestions for all of the regional transmission organizations.[106] In early 2022, the Department of Energy announced that new proactive studies of the electric grid would be used to inform designations of National Interest Corridors and incentives for building a resilient network.[107]

Together, these two methods of obtaining and relaying data to the public highlight the recent efforts to inform policymakers and the public on the nation's energy infrastructure. The data collection and posted studies also highlight that the Department of Energy is actively proposing solutions to meet incoming crises with our electricity grid. This proactive approach, if applied to the communications network, would help the FCC understand current vulnerabilities and ongoing changes in the network.

III. ANALYSIS

A. Extreme Weather Created by Climate Change Highlights the Urgency of Updating the Communications Network Through a Proactive Framework like the Department of Energy's

The increasing prevalence of extreme weather events in certain areas of the country highlights the stress that communications networks will bear in the coming decades. For example, the increasing economic impact of hurricanes shows the vulnerabilities of communications networks on coastlines across the southern and eastern borders of the continental United States.[108] The FCC has taken steps in the right direction with the creation of the PR/USVI Fund, which recognizes and responds to a vulnerable area of the communications infrastructure.[109] However, this fund retroactively responds to harm, and funds of this nature are not present in areas of the United States that will face a similar threat of damage from extreme weather in the coming decades.

The FCC's focus on coastline areas of the United States is necessary, but the FCC should also evaluate how to prevent high-cost repairs from destroyed communication networks before the damages occur. With the unpredictable nature of extreme weather, the scope of potential improvements should be nationwide but with a focus on current disaster-prone regions like southern coastlines. The FCC should continue retroactive response efforts to extreme weather events with a future focus, pursuant to the Broadband DATA

105. *See id.*

106. *See id.* at 45.

107. Building a Better Grid Initiative To Upgrade and Expand the Nation's Electric Transmission Grid To Support Resilience, Reliability, and Decarbonization, 87 Fed. Reg. 2769, 2771 (Jan. 19, 2022).

108. *See* Weinkle et al., *supra* note 5, at 811.

109. *See Bringing Puerto Rico Together*, *supra* note 21.

Act, on using forward-looking data to work with industry stakeholders to prevent damages to the nation's network infrastructure from extreme weather.

The harm to vulnerable regions, like the Virgin Islands, from extreme weather highlights the importance of building a resilient communications network in the United States and its territories. The FCC's recent actions are a step in the right direction, such as building a map of where service is available, but the FCC should also proactively consider the costs of ensuring a resilient communications infrastructure survives extreme weather events. For example, the FCC's efforts towards building up DIRS have allowed the flow of data when disaster strikes, but the data is not informing officials/the agency how to prevent outages under circumstances in which DIRS is activated.[110] As the effects of climate change disproportionately impact the communication networks of various regions of the country, especially coastal regions, the FCC's current framework should evolve to address the need for resilient networks in light of extreme weather.[111] More than ever, the importance of having the infrastructure present coincides with the need for the FCC to ensure that the current infrastructure is managed well during future extreme weather events.

The Energy Policy Act of 2005's statutory requirement for the Department of Energy to conduct three-year studies of the electricity grid provides a proactive framework for the FCC to apply in tackling the vulnerabilities of the communications network to extreme weather events related to climate change.[112] The Department of Energy studies' requirement for consultation with state stakeholders and a proactive approach to analyzing future congestion of the electric grid should be continually evolving in the FCC's Broadband Data Collection requirements under the Broadband DATA Act with an emphasis on network resiliency.[113] Not only will this bring long-lasting solutions, but the FCC should continuously evolve these parameters into their approach for reviewing the communications network going forward. The FCC's collection of stakeholder data during the open submission windows demonstrated how the focus can be evolved to account for a proactive approach with increased participation.[114] The FCC can then engage industry stakeholders in developing proactive solutions for the future of network resiliency as data is collected through open submission windows.

B. The FCC Should Adopt the Department of Energy's Strategy in Driving Proactive Solutions for Network Resiliency in Preparation for Extreme Weather

The Department of Energy's approach actively engages grid stakeholders in a comprehensive review of the nation's energy infrastructure to facilitate broad solutions to building grid reliability. The Department of

110. *See* Resilient Networks NPRM, *supra* note 42, at para. 34.

111. *See* Grant, *supra* note 6.

112. *See* Energy Policy Act of 2005, 16 U.S.C. § 824p(a) (2005).

113. *See* 16 U.S.C. § 824p(a)(1); Broadband Deployment Accuracy and Technological Availability Act, 47 U.S.C. §§ 641–646 (2020); *Cal. Wilderness Coal.*, 631 F.3d at 1095.

114. *See* Digital Opportunity Data Collection, *supra* note 48, at 2.

Energy's approach alone has not resulted in the new construction of transmission lines since the only designated National Interest Corridors later had the designations vacated by court judgment, but the overall approach has brought more awareness to properly managing the electric grid in the face of congestion.[115] While the Department of Energy's ability to act towards solutions has been hampered by the courts in the past, these efforts inform how the FCC should approach setting proactive standards for reviewing the nation's communications infrastructure and acting on funding solutions to build reliability in the face of extreme weather.

1. The FCC Should Proactively Study Areas of the United States Where Network Resiliency Will Be Compromised in Coming Decades

The FCC's ongoing Broadband Data Collection efforts should evolve to include efforts to proactively study areas of the country where network resiliency will change in the coming decades due to destructive weather events brought on by climate change. The Broadband DATA Act mandates that the FCC "shall prioritize implementing the fabric for rural and insular areas of the United States."[116] Within the statute, the "fabric" refers to locations where providers may install fixed broadband service.[117] The Broadband DATA Act statutorily mandated data collections provide a mechanism through which the FCC can focus on areas of the country that will be hampered by extreme weather in the coming decades. If the FCC carefully organizes the collected data and instates reoccurring reviews, it will see how the communications infrastructure changes over time. Following extreme weather, the FCC can review how the network is affected and use collected data to target funding towards strengthening vulnerable areas in the future.

Outside of collecting broadband data, the FCC should adopt the Department of Energy's strategy of using its broad statutory authority to conduct annual reviews of the communications network, like in the annual transmission reviews.[118] The FCC could specifically cite its requirement from Congress to create a process through which information can be submitted on an "ongoing" basis for annual reviews.[119] This solution will bring administrative costs, but Congress would likely support funding going toward a new proactive approach given the mission of the FCC and the Broadband DATA Act to provide universal, reliable service to the United States.[120]

---

115. *See Cal. Wilderness Coal.*, 631 F.3d at 1095.

116. 47 U.S.C. § 642(b)(1)(C).

117. Rosenwercel, *supra* note 49.

118. *See* OFF. OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY, U.S. DEP'T OF ENERGY, *supra* note 7, at 1.

119. *See* Broadband Deployment Accuracy and Technological Availability Act, 47 U.S.C. § 644(b)(1) (2020) (mandating that the FCC create a process for individuals to "submit specific information about the development and availability of broadband Internet access service in the United States on an ongoing basis").

120. *See Universal Service*, *supra* note 19; *Bill to Improve Broadband Data Maps Signed Into Law*, *supra* note 52.

Making these reviews publicly available would encourage providers to expand networks, highlight where service is lacking or at risk of damage from extreme weather, and encourage the FCC to seek to expand the communications network in conjunction with service providers and state regulatory agencies.

2. The FCC Should Continue to Work with Service Providers to Proactively Build Robust Communication Networks in Compromised Areas

The FCC should also inform service providers of findings from data collection efforts. State regulators can assist in carrying out this function, but future service needs should be continually assessed. Service providers will know best which sections of their network are vulnerable to damage from extreme weather. In the long term, the FCC should aim to ensure that data on the expansion and resiliency of the communications network flows both ways.

Outside of annual reviews, the FCC should improve the collection of its outage reporting data to understand where networks are most affected by outages, especially from extreme weather. Even if outages do not result from extreme weather, the FCC can use this information to rebuild aging networks in preparation for potential extreme weather in the future. Summarizing this data can also serve as a helpful tool for service providers, in addition to helping the FCC understand where potential funding opportunities exist to build network resiliency before extreme weather strikes.

The FCC could also create funds for vulnerable areas of the United States, like the coastlines, to proactively build network resiliency. Further, the FCC should apply the framework used in the Bringing Puerto Rico Together Fund and Connect USVI funds to require carriers across the United States (particularly in areas that will be affected by flooding and extreme weather over the coming decades) to submit Disaster Preparation and Response Plans.[121] Creating these plans has precedent from FERC, which initiated rulemaking to direct regional transmission organizations to submit one-time reports on how the providers will "determine exposure to extreme weather hazards, estimate the costs of impacts, and develop mitigation measures to address extreme weather risks."[122] The FCC could take similar actions to require service providers to set aside a current amount of their own funding or develop responsive strategies to extreme weather, at a minimum.

Service providers will argue against further requirements for building up their network without support or funding from the FCC. Service providers may also object to the FCC allowing any information on service outages or annual reviews to become public knowledge, as it may impact how consumers view the quality of their service provider. The FCC, to keep transparent communication lines open with service providers and other stakeholders,

121. *Bringing Puerto Rico Together*, *supra* note 21.

122. One-Time Informational Reports on Extreme Weather Vulnerability Assessments; Climate Change, Extreme Weather, and Electric System Reliability, 87 Fed. Reg. 39414, 39415 (July 1, 2022) (to be codified at 18 C.F.R. pt. 141).

would likely not self-select to make any of the information public if privacy concerns arise. However, service providers may opt to conform with FCC regulations to boost their image among customers as providing resilient service (especially for customers in vulnerable areas). Separately, building resilient service will work towards creating a new industry standard for the government and the private providers working together to build network resiliency.

C. The FCC Should Ensure State Regulators and Service Providers Across Vulnerable Regions are Included in Broadband Data Collection Efforts

Much like the Department of Energy's usage of public information to create the congestion studies mandated by the Energy Policy Act of 2005, the FCC's usage of broadband data from service providers will inform decisions on areas of the communication network that need upgrades.[123] The FCC does not have a statutory mandate to work with states in this manner in the Broadband DATA Act, but Congress (or service providers) may unfavorably respond if states disapprove of proposed solutions. Collecting this data from state regulators and service providers, especially those in vulnerable areas, should occur alongside their direct involvement in proposals for the best solutions. The FCC should ensure that the data reviews are accurate, done on a regular basis, and used to build network resiliency, which requires long-term opportunities for stakeholders to submit data on the communications network. The FCC has demonstrated its ability to convene industry stakeholders in the collection of data but should continuously improve its ability to drive solutions to build a resilient network in the face of extreme weather.

1. The FCC Should Proactively Aim to Ameliorate Concerns from Local Providers

For any policy change to remain effective and keep a court from overturning the agency's decisions, the FCC should continue to hear the concerns of local providers and stakeholders directly in the process. While the FCC has no statutory obligation under the Broadband DATA Act to work directly with stakeholder groups in the same way as the Energy Policy Act requires, the Department of Energy's studies have been held accountable for not properly considering state regulatory perspectives.[124] This suggests that the FCC should act to ensure that there are open communication channels with providers and state regulators. Working with stakeholder groups, especially those that may need funding in the near future, in conjunction with the established data collection efforts, may give legitimacy to proposed solutions to extreme weather and prevent future legal disputes.

123. *See* U.S. DEP'T OF ENERGY, *supra* note 88, at vii.
124. *See* Energy Policy Act of 2005, 16 U.S.C. § 824p(a)(1) (2005); *see also Cal. Wilderness Coal.*, 631 F.3d at 1085-86, 1095 (9th Cir. 2011).

The Department of Energy, in annual transmission reviews, has made sure to collect data from a variety of stakeholder groups.[125] The FCC should similarly work directly with state regulatory entities to ensure that broadband data, which can be used for furthering resiliency policies, is accurate. The FCC declined to make clear exactly which stakeholders submitted data during the two open submission windows, and doing so may provide more legitimacy to policies developed from the map in the future. Ensuring that submitting data is accessible to all stakeholders will bring a more cohesive response to the resiliency of our communication networks.

2. The FCC Should Build Mechanisms to Permit a Continual Flow of Data Between the Agency and Providers

One of the limitations of the Department of Energy's ability to designate National Interest Corridors is that the statutory language only mandates a study every three years.[126] With the rate of technology change and the need for rapid infrastructure strengthening given the urgency of extreme weather events, the FCC should liberally construe "ongoing" to build a continuous relationship with stakeholders as required in the Broadband DATA Act.[127] The statute leaves open how often the data submissions from service providers must be, and the FCC should follow the Department of Energy's framework in following a regular timeline for the exchange of information. The FCC has already taken steps to build a regular flow of information to the Broadband Data Map but should similarly build a regular review schedule to analyze the map for impacts from extreme weather.[128]

The Department of Energy's annual transmission studies recognize the rapidly changing nature of the electricity grid and provide updated data to stakeholders who drive solutions in the field. Now that the FCC has the mechanisms to create a map of broadband service in the United States, there is nothing preventing the FCC from reviewing the map on a more consistent basis, like the Department of Energy's annual transmission reviews, to identify areas in need of improvement to withstand extreme weather. Reviewing the map more than twice a year to draw conclusions is likely not feasible because the maps will only be updated twice a year per the statute,

---

125. *See* OFF. OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY, U.S. DEP'T OF ENERGY, *supra* note 7, at 2 (stating that the Department of Energy "identified, in consultation with industry stakeholders, specific information in regional sources that was appropriate to include").

126. *See* 16 U.S.C. § 824p(a).

127. *See* Broadband Deployment Accuracy and Technological Availability Act, 47 U.S.C. § 644(b)(1) (2020) (requiring a process through which stakeholders can submit "specific information about the deployment and availability of broadband Internet access service in the United States on an ongoing basis").

128. *Information for Filers*, FED. COMMC'NS COMM'N, https://www.fcc.gov/BroadbandData/filers [https://perma.cc/CK6W-7TBF] (last visited Nov. 11, 2023) (notifying filers that "data as of June 30th is due no later than the following September 1st, and data as of December 31st is due no later than the following March 1st").

but the FCC could develop mechanisms to invite comments on annual reviews of the data received from stakeholders. It is possible that if annual transmission reviews of the entire network require too much effort, reviews of focused areas, like around coastlines, may work best.

Given the evolving trends of technology in this area, the agency should continue to work with providers to create long-term plans for continual data transfer and analysis both ways. The continual transfer of this knowledge will also provide for better analysis from the FCC on long-term network instability trends. The Broadband DATA Act mandates the FCC "develop a process through which entities . . . may submit specific information about the deployment and availability of broadband Internet access service in the United States."[129] The Broadband DATA Act creates a mandate for a biannual update of the broadband maps at minimum, but FCC updates of the maps themselves may not lead to broader solutions since stakeholders will only have an awareness of the changes in their own data.[130] The Department of Energy's annual transmission reviews are helpful in this light; stakeholders can review the data and make their own long-term business decisions. Flows of data in both directions will help inform Congress of developments and raise awareness for challenges from extreme weather in the communications industry.

The FCC should thus follow the example of the Department of Energy in making publicly available annual reviews of the communications infrastructure data, which would help show stakeholders where construction or upgrade of infrastructure is needed. The data will be handed to the FCC on a biannual basis at minimum, so the FCC should aim to review the data as it is received from open submission windows. The FCC may push back on more regular reviews of the data since changing the map and conducting a data analysis could lead to high administrative costs. However, having these reviews publicly available for stakeholder review may prompt service providers to expand the durability and availability of service to customers. The FCC has the potential to continue the conversations it has started with data submission windows to drive forward-looking solutions in building up the grid in preparation for extreme weather across the country.

IV. CONCLUSION

The FCC should modify its current framework of retroactive response to network instability and embrace a framework of proactively working with stakeholders to solidify the resilience of our communications network in light of future extreme weather. The Department of Energy's mandated review of the electric grid provides inspiration for the FCC to continually review vulnerable areas of the communications network and provide proactive funding to needed areas. Further, it provides a framework for evaluating the communications network infrastructure of the United States on a habitual

129. *Id.*
130. *See* 47 U.S.C. § 642(c)(3).

timeline, which will encourage the participation of many stakeholders in the process.

The FCC has the capabilities to gather communications network data, evolve existing communication lines with state stakeholders on proactively creating solutions, and set aside funding for areas of the United States that will be disproportionately affected by extreme weather. The FCC's framework with the Puerto Rico Together (Uniendo a Puerto Rico) Fund and Connect USVI Fund sets a standard for recognizing and responding to critical needs for infrastructure upgrades in vulnerable areas of the United States. The FCC can use the Broadband DATA Act as a springboard for not only ensuring that wireless communications are available across the country but also strengthening a network infrastructure that will withstand damage from extreme weather.

Now, imagine how differently the earlier disaster scenario would end up if the FCC had planned for a devastating storm's impact on communication lines to local authorities. The FCC likely would have noticed the repeated outages from storms in the area and upgraded the strength of wireless towers in the affected area. A call to local authorities to inform them of your emergency situation would bring help to your home in a matter of minutes instead of waiting hours or days.

Reclaiming the Airwaves: An Analysis of Claims to Wireless Spectrum by Tribal Nations Based on Treaty Obligations and the Federal Trust Responsibility

Morgan Gray*

TABLE OF CONTENTS

* J.D. Candidate, The George Washington University Law School, 2024; Notes Editor, Federal Communications Law Journal, Volume 76; B.A., May 2016, Political Science, Texas A&M University; M.P.A, May 2018, Texas A&M University. I wish to express my most sincere gratitude to the community of tribal leaders, scholars, and practitioners who have supported me while writing this Note. I owe a special thanks to the Chickasaw Nation for the unwavering support afforded to me in my educational and professional endeavors, and for facilitating my introduction to the world of telecommunications. Thank you to the FCLJ editorial board for supporting the publication of this Note. Lastly, I owe all my gratitude to my ancestors for their determination and resilience, and to my family and friends for their encouragement and love.

I. INTRODUCTION

Nowhere is the digital divide more apparent than in Indian Country. An estimated thirty-five percent of residents lack access to the Federal Communication Commission's (FCC) definition of broadband at 25 mbps down and 3 mbps up.[1] Referred to as "the technology of freedom," the Internet connects communities to resources capable of improving overall quality of life, such as telehealth services, online learning, and remote employment opportunities.[2] The emergence of the COVID-19 pandemic highlighted our dependence on Internet access to complete even the most basic of tasks.[3] According to a Pew Research Center poll, fifty-three percent of surveyed Americans agreed that Internet access was essential to their ability to perform everyday tasks during the pandemic.[4] Despite the Biden-Harris Administration's intention to lift the public health emergency order in May of 2023,[5] the pandemic has left a lasting impact on Internet usage in America.[6]

---

1. 2018 Broadband Deployment Report, FCC 18-10, para. 50 (2018) https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2018-broadband-deployment-report [https://perma.cc/PJE5-U7FN] [hereinafter, 2018 Broadband Report]; Hansi Lo Wang, *Native Americans on Tribal Land Are 'The Least Connected' To High Speed Internet*, NAT'L PUB. RADIO (Dec. 6, 2018). https://www.npr.org/2018/12/06/673364305/native-americans-on-tribal-land-are-the-least-connected-to-high-speed-internet [https://perma.cc/BF7E-C8FL]; *see also* 18 U.S.C. § 1151 (establishing the definition of "Indian Country" as encompassing (a) land within an Indian reservation, (b) dependent Indian communities, and (c) Indian allotments).

2. Manuel Castells, *The Impact of the Internet on Society: A Global Perspective*, OPENMIND BBVA, https://www.bbvaopenmind.com/en/articles/the-impact-of-the-internet-on-society-a-global-perspective/ [https://perma.cc/U5DC-2GQP]; Darrah Blackwater, *For Tribal Lands Ravaged by COVID-19, Broadband Access is a Matter of Life and Death*, INTERNET SOC'Y (May 15, 2020), https://www.internetsociety.org/blog/2020/05/for-tribal-lands-ravaged-by-covid-19-broadband-access-is-a-matter-of-life-and-death/ [https://perma.cc/PZB2-PGZY].

3. Colleen McClain et al., *The Internet and Pandemic*, PEW RSCH. CTR. (Sept. 1, 2021), https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/ [https://perma.cc/P64X-BP2R].

4. Emily A. Vogels et al., *53% of Americans Say the Internet Has Been Essential During the Covid-19 Outbreak*, PEW RSCH. CTR. (Apr. 30 2020), https://www.pewresearch.org/internet/2020/04/30/53-of-americans-say-the-internet-has-been-essential-during-the-covid-19-outbreak/ [https://perma.cc/WSG4-2ZG2].

5. OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, SAP-H.R.-382-H.J.-RES.-7, STATEMENT OF ADMINISTRATIVE POLICY (2023), https://www.whitehouse.gov/wp-content/uploads/2023/01/SAP-H.R.-382-H.J.-Res.-7.pdf [https://perma.cc/PC4N-XHRZ].

6. *See, e.g.*, Kim parker et al., *Covid-19 Pandemic Continues To Reshape Work in America*, PEW RSCH. CTR. (2022), https://www.pewresearch.org/social-trends/2022/02/16/covid-19-pandemic-continues-to-reshape-work-in-america/ [https://perma.cc/D3L9-KJ2A] (attesting to the continued prominence of telecommuting arrangements two years after the public health emergency declaration); U.S. GOV'T ACCOUNTABILITY OFF., *Telehealth in the Pandemic – How Has it Changed Healthcare Delivery in Medicaid and Medicare?*, GAO WATCHBLOG (Sept. 29, 2022), https://www.gao.gov/blog/telehealth-pandemic-how-has-it-changed-health-care-delivery-medicaid-and-medicare [https://perma.cc/manage/create?folder=15737] (finding increased use of telehealth medicine services as a result of the COVID-19 pandemic).

It exacerbated an existing digital divide—namely the inequalities resulting from disparities between those with Internet access and those without.[7]

Lack of access to broadband in tribal communities is the result of a number of factors, including insufficient infrastructure, challenging topography that hinders infrastructure development, and an overall lack of financial incentive for telecommunications providers to invest in infrastructure.[8] Wireline options, such as fiber optic cable, are uniquely expensive to deploy in areas where the topography complicates the construction process.[9] Wireless solutions, such as Fixed Wireless Access (FWA), are often more feasible and can provide broadband Internet access to rural service areas.[10] Wireless Internet service requires access to spectrum: invisible radio waves divided into frequency channels that are used to transmit data and information over the air.[11]

The federal scheme governing the use of wireless spectrum disadvantages tribal communities and further warrants an inquiry as to why tribes lack access to the valuable resource in the first place.[12] Historically, the federal government has had a duty to act in a fiduciary capacity pursuant to a tribe's best interest, referred to as the federal trust responsibility ("trust responsibility").[13] By vesting the FCC with authority to assign access to wireless spectrum associated with tribal lands, the federal government arguably violated its trust responsibility. And, beyond the federal government's trust obligation, tribes were generally guaranteed protected access to valuable resources through treaties. While treaties entered into during the 18th and 19th centuries lack specific language guaranteeing a tribe's right to access wireless spectrum, language protecting resources considered valuable to tribes can be interpreted to imply access to spectrum.

This Note will analyze the legal claims to wireless spectrum tribes can assert as a result of both the failure of the federal government to uphold its trust obligation with respect to tribes' access to wireless spectrum licenses

---

7. *Digital divide*, MERRIAM WEBSTER, https://www.merriam-webster.com/dictionary/digital%20divide [https://perma.cc/7746-CJ9G] (last visited Dec. 5, 2022).

8. U.S. GOV'T ACCOUNTABILITY OFF., GAO-06-189, CHALLENGES TO ASSESSING AND IMPROVING TELECOMMUNICATIONS FOR NATIVE AMERICANS ON TRIBAL LANDS (2006), https://www.gao.gov/assets/gao-06-189.pdf [https://perma.cc/D35Y-7NSC].

9. Sophia Campbell et al., *The Benefits and Costs of Broadband Expansion*, THE BROOKINGS INST. (Aug. 18, 2021), https://www.brookings.edu/blog/up-front/2021/08/18/the-benefits-and-costs-of-broadband-expansion/ [https://perma.cc/WV4B-67HN].

10. CTIA, *5g Fixed Wireless Broadband: Helping Bridge the Digital Divide in Rural America* (2021), https://api.ctia.org/wp-content/uploads/2021/11/CTIA-Rural-HHs-mini-POV-V2-20211115.pdf [https://perma.cc/2BUR-UT7D].

11. *What Is Wireless Spectrum? Here's What You Should Know*, AURORA INSIGHT (Mar. 9, 2021), https://aurorainsight.com/what-is-wireless-spectrum-heres-what-you-should-know/ [https://perma.cc/5JLQ-A2L8].

12. Brian Howard, *Spectrum Airwaves: A Natural Resource Tribes Must Leverage*, AM. INDIAN POL'Y INST. (Oct. 16, 2019), https://aipi.asu.edu/sites/default/files/10.16.2019_aipi_fcc_spectrum_policy.pdf [https://perma.cc/WPU7-QHRH].

13. COHEN'S HANDBOOK OF FEDERAL INDIAN LAW § 5.04[3][a] at 412 (Nell Jessup Newton ed., 2012) [hereinafter, COHEN'S HANDBOOK].

and its failure to deliver on treaty promises to protect tribal access to valuable resources. Beginning with an overview of the regulatory scheme governing wireless spectrum allocation in the U.S., an explanation of the federal trust responsibility pertaining to the management of tribal property, and the federal government's obligations to honor Indian treaties, this Note further explores legal remedies available to tribes in addition to actions the FCC can adopt to increase tribal access to spectrum.

II. BACKGROUND

A. Wireless Spectrum Allocation in the United States

Access to wireless spectrum, or the radio waves necessary to transmit data for wireless Internet service, in the U.S. is governed by the Communications Act of 1934 (Communications Act).[14] The Communications Act authorizes the National Telecommunications and Information Administration (NTIA) to oversee federal spectrum use while authorizing the FCC to manage and assign all non-federal use of wireless spectrum.[15] Non-federal use includes spectrum use by state and local governments.[16] Title III of the Communications Act further establishes the overarching regulatory scheme by which wireless spectrum is governed and defines the tools at the FCC's disposal.[17]

The FCC may designate spectrum frequency bands for specific services and uses and may also determine methods for assigning licenses for particular frequencies. This authority is subject to the condition that the FCC discharge its duty in accordance with "the public convenience or interest or . . . public necessity."[18] Generally, the FCC designates spectrum frequencies as either licensed or unlicensed. While unlicensed spectrum allows service providers to access a valuable resource without the financial cost of obtaining a license, unlicensed bands are often subject to signal interference that lowers the quality of the wireless Internet connection.[19] Licensed spectrum, alternatively, guarantees a license holder exclusive use of a particular

14. The Communications Act of 1934, 47 U.S.C. § 151 (1934).

15. 47 U.S.C. § 305 (reserving to the President of the U.S. the right to assign federal use of spectrum frequencies); *see also Who Regulates the Spectrum*, NAT'L TELECOMMS. & INFO. ADMIN., https://www.ntia.gov/book-page/who-regulates-spectrum#:~:text=As%20shown%20above%2C%20the%20use,FCC%20manages%20all%20other%20uses [https://perma.cc/WNA7-X9X3] (last visited Nov. 6, 2023) (explaining that the President's authority to act under this section is currently delegated to the Administrator for the National Telecommunications and Information Administration).

16. *Radio Spectrum Allocation*, FED. COMMC'NS COMM'N https://www.fcc.gov/engineering-technology/policy-and-rules-division/general/radio-spectrum-allocation [https://perma.cc/A2XM-2LYA] (last visited Jan. 12, 2023).

17. 47 U.S.C. § 301.

18. 47 U.S.C. § 303(f).

19. SPECTRUM POLICY TASK FORCE, FCC, SPECTRUM POLICY TASK FORCE REPORT NO. 02-135 (Nov. 2002), https://docs.fcc.gov/public/attachments/DOC-228542A1.pdf [https://perma.cc/G4QN-WDR4].

spectrum band in a defined geographic area, allowing service providers greater control and autonomy over the quality of their connectivity.[20]

Historically, the FCC assigned spectrum licenses through a combination of comparative hearings and lotteries.[21] In 1993, Congress granted the FCC authority, for a limited time, to issue licenses via competitive bidding.[22] Congress has since extended this authority several times, most recently in the Consolidated Appropriations Act of 2023, which extended the FCC's auction authority through March 9, 2023.[23] While Congress failed to renew the FCC's spectrum auction authority for the first time in thirty years when it expired on March 10, 2023, FCC Chairwoman Rosenworcel and others have called on Congress to swiftly restore the FCC's authorization.[24]

The FCC conducts spectrum auctions under the theory that the auctions result in an efficient allocation of spectrum resources, with licenses going to the entities who will put them to their most valuable use.[25] Those interested in acquiring licenses are required to submit an entrance fee to gain access to the auction itself, and the licenses are ultimately awarded to the highest bidder at the auction's conclusion.[26] Incentive auctions leave lower-resourced parties, such as tribes, at a disadvantage against national wireless carriers who bid hundreds of millions of dollars in spectrum incentive auctions annually.[27] Since 1993, the FCC has conducted over 100 auctions generating approximately $230 billion in revenue.[28]

In 2019, the FCC adopted its Tribal Priority Filing Window for the 2.5 GHz band which gave tribes an unprecedented opportunity: they could obtain

---

20. Christopher Trick, *Licensed vs. Unlicensed Spectrum: Key Differences and 5G Use Cases*, TRENTON SYS. (Nov. 7, 2022), https://www.trentonsystems.com/blog/licensed-vs-unlicensed-spectrum [https://perma.cc/G3QU-VSZ9].

21. STUART MINOR BENJAMIN & JAMES B. SPETA, INTERNET AND TELECOMMUNICATION REGULATION § 5.C.2 (1st ed. 2019).

22. *About Auctions*, FED. COMMC'NS COMM'N https://www.fcc.gov/auctions/about-auctions [https://perma.cc/XN7D-XL5X]; *see also* JILL C. GALLAGHER & PATRICIA MOLONEY FIGLIOLA, CONG. RSCH. SERV., R47258, FCC SPECTRUM AUCTION AUTH.: BACKGROUND AND PROPOSALS FOR EXTENSION 1 (2022), https://crsreports.congress.gov/product/pdf/R/R47258#:~:text=On%20July%2027%2C%202022%2C%20the,auction%20authority%20through%20March%202024 [https://perma.cc/8DSM-HGN8] [hereinafter FCC Spectrum Auction Authority].

23. Gallagher & Figliola, *supra* note 22.

24. Tom Butts, *Congress Lets FCC's Spectrum Auction Authorization Lapse*, TV TECH. (Mar. 13, 2023) https://www.tvtechnology.com/news/congress-lets-fccs-spectrum-auction-authorization-lapse [https://perma.cc/M72X-W7KN.

25. *About Auctions*, *supra* note 22; *see also* FCC SPECTRUM AUCTION AUTHORITY (2022).

26. *How is an Auction Conducted?*, FCC https://www.fcc.gov/conducting-auctions [https://perma.cc/23U3-FHEW] (last visited Nov. 6, 2023).

27. Roslyn Layton, *Spectrum Auctions Have Raised $230 Billion; The FCC's Authority To Conduct Them Will Lapse Soon If Congress Doesn't Act*, FORBES (Apr. 29, 2022), https://www.forbes.com/sites/roslynlayton/2022/04/29/spectrum-auctions-have-raised-230-billion-the-fccs-authority-to-conduct-them-will-lapse-soon-if-congress-doesnt-act/?sh=126021c0908e [https://perma.cc/2U7A-GPZT].

28. *Id*.

unallocated spectrum in the 2.5 GHz band without paying for the licenses.[29] The FCC's Report and Order detailing its decision to adopt a priority filing window for tribes acknowledged its duty to tribal nations, noting that tribes were "eligible to receive certain protections by virtue of their federally-recognized status."[30]

B. Federal Trust Responsibility & Treaty Obligations

The federal government maintains a special relationship with Indian tribes and is obligated to act pursuant to their best interest.[31] This obligation is described as "the concept of a federal trust responsibility to Indians evolved from early treaties with tribes; statutes, particularly the Trade and Intercourse Acts; and opinions of the Supreme Court."[32] Despite this obligation, the government has regularly failed to uphold its trust responsibility.[33]

1. Supreme Court Jurisprudence on the Trust Responsibility

The Supreme Court first recognized a special relationship between the federal government and tribes with respect to resource and property management in *Johnson v. M'Intosh* when Chief Justice John Marshall concluded conquest by the U.S. divested tribes of the underlying fee title to their historic homelands.[34] While the United States' retention of legal title prohibited tribes from exercising the right to transfer their lands, tribes nonetheless retained the right of occupancy and use consistent with their status as sovereign entities.[35] The Court's analysis ultimately formed the foundation upon which the government's duty to protect tribal property and resources is based.[36]

A decade later, the Chief Justice described tribes as domestic dependent nations relying on the federal government for protection in *Cherokee Nation v. Georgia*.[37] The relationship between the two sovereigns was further described as that of a "ward to his guardian," and the Court concluded the

29. Transforming the 2.5 GHz Band, *Report and Order*, 34 FCC Rcd 5446 (2019); *see also 2.5 GHz Rural Tribal Window*, FED. COMMC'NS COMM'N, https://www.fcc.gov/25-ghz-rural-tribal-window [https://perma.cc/QAE2-78CE] (stating that successful applicants will be issued a license by the FCC and retaining the license is subject to meeting build-out requirements) (last visited Nov. 6, 2023).

30. Transforming the 2.5 GHz Band, *supra* note 29, at para. 49.

31. COHEN'S HANDBOOK § 5.04[3][a] at 412.

32. *Id*.

33. *See, e.g.*, Lone Wolf v. Hitchcock, 187 U.S. 553, 556 (1903); Tee-Hit-Ton Indians v. United States, 348 U.S. 272, 278 (1955); Menominee Tribe of Indians v. United States, 391 U.S. 404, 412 (1968); Sioux Tribe of Indians v. United States, 316 U.S. 317, 327 (1942); Lyng v. Nw. Indian Cemetery Protective Ass'n, 485 U.S. 439, 453 (1988).

34. Johnson v. M'Intosh, 21 U.S. 543, 573 (1823).

35. *Id*.

36. COHEN'S HANDBOOK § 5.04[3][a] at 413.

37. Cherokee Nation v. Georgia, 30 U.S. 1, 10 (1831).

federal government owed a duty of protection to tribes.[38] In *Worcester v. Georgia*, tribes were deemed distinct political communities with authority to exercise self-governance to the exclusion of state authority, but nevertheless remained under the protection of the national government.[39] These three cases, known as the Marshall Trilogy, establish the trust responsibility's foundation.

a. Courts on Congress's Obligation to Act Pursuant to the Trust Responsibility

The trust responsibility also serves as a foundational concept informing, and in some instances limiting, Congress's plenary power over Indian affairs.[40] Courts have relied upon Congress's plenary power to uphold federal action affecting a tribe's property interests.[41] Congress's plenary power derives from the same Constitutional sources as the trust responsibility—the Indian Commerce Clause and Treaty Clause—and is further reinforced by the federal government's duty of protection to tribes.[42] The Supreme Court acknowledges Congress's broad authority to legislate with respect to tribal nations. Since the Marshall Trilogy, the Court has upheld Congressional actions both beneficial and hostile towards tribal interests.[43]

For example, the Court in *United States v. Sioux Nation of Indians* (*Sioux Nation*) concluded that Congress violated the trust responsibility, despite its broad legislative authority over Indian affairs, when it divested the Great Sioux Nation of its treaty-protected claim to the Black Hills in South Dakota through legislation.[44] In contrast, courts have also upheld congressional actions to the detriment of tribal interests—such as diminishment and disestablishment of reservation boundaries guaranteed by express treaty language,[45] and termination of a tribe's federal recognition[46]—as valid exercises of both the trust responsibility and plenary power.

b. Courts Recognize the Executive Branch's Duty to Uphold the Trust Responsibility

The executive branch is equally required to uphold the trust responsibility. The Bureau of Indian Affairs (BIA) within the U.S.

38. *Id*.
39. Worcester v. Georgia, 31 U.S. 515, 557 (1832).
40. COHEN'S HANDBOOK § 5.02[1] at 391; United States v. Lara, 541 U.S. 193, 200 (2004).
41. *Lone Wolf*, 187 U.S. at 556.
42. *Lara*, 541 U.S. at 200.
43. *See, e.g.*, *Lone Wolf*, 187 U.S. at 556; *Tee-Hit-Ton Indians*, 348 U.S. at 278; *Menominee Tribe of Indians*, 391 U.S. at 412; *Sioux Tribe of Indians*, 316 U.S.at 327; *Lyng*, 485 U.S. at 453.
44. United States v. Sioux Nation, 448 U.S. 371, 416 (1980).
45. *Lone Wolf*, 187 U.S. at 556.
46. *Menominee Tribe of Indians*, 391 U.S. at 412; Menominee Tribe v. United States, 221 Ct. Cl. 506, 511-12 (1979) (rejecting Tribe's challenge to Termination Act based on violation of trust responsibility on jurisdictional grounds).

Department of the Interior may designate land into trust for the benefit of tribes and individual Indians[47] and is tasked with managing certain tribal assets, such as minerals and timber, by approving leases with private parties.[48] The BIA has promulgated extensive regulations governing their authority to oversee management of resources held in trust for the benefit of tribes and individual Indians.[49] Furthermore, many tribes who enacted constitutions pursuant to the Indian Reorganization Act of 1934 (IRA) require the Secretary of the Interior's approval before adopting constitutional amendments.[50]

The Court has upheld executive branch action detrimentally affecting tribal interests despite the duty to uphold the trust responsibility. Specifically, in *Lyng v. Northwest Cemetery Protective Association*, the Court upheld action by the U.S. Forest Service (USFS) in defiance of its impact on the religious and cultural practices of the Yurok, Karok, and Tolowa tribes in California.[51] The USFS sought to construct a road through a sacred site near the Hoopa Valley Reservation which would cause irreparable harm to the Tribes' use of the sacred site.[52] Despite the significant harm to the Tribes' ability to continue utilizing the site for religious and cultural purposes, the Court upheld the USFS's approval of the road's construction.

Notwithstanding the past failure to uphold the trust responsibility, courts, Congress, and the executive branch continue to acknowledge their duty to act as trusted stewards of tribal interests.[53]

2. Treaties as a Source of Specific Trust Responsibility Obligations

The federal government's authority to act with respect to Indian tribes derives from express provisions in the U.S. Constitution.[54] During the late 18th and early 19th centuries, Congress often exercised this power by entering into treaties pursuant to the Indian Commerce Clause and the Treaty Clause.[55] While distinct in their subject and provisions, most treaties contain promises

47. *See* Indian Reorganization Act, 25 U.S.C. § 465; *see also* 25 C.F.R. § 152 (1982).

48. *See* Indian Mineral Leasing Act, 25 U.S.C. § 396; *see also* 25 C.F.R. §§ 163, 200, 211, 212, 225 (2023).

49. *See, e.g.*, 25 C.F.R. § 163 (2023) (regulations pertaining to management of forest lands); 25 C.F.R. § 200 (2023) (regulations affecting coal leases on tribal lands); 25 C.F.R. § 211-212 (2023) (regulations for entering into leases for mineral development on tribal lands); 25 C.F.R. § 225 (2023) (regulations governing oil and gas, geothermal, and solid mineral agreements).

50. *See* Indian Reorganization Act, 25 U.S.C. § 5123.

51. *Lyng*, 485 U.S. at 453.

52. *Id*. at 442.

53. COHEN'S HANDBOOK § 5.04[3][a] at 412.

54. U.S. CONST. art. I, § 8, cl. 3; U.S. CONST. art. II, § 2, cl. 2; *see also* COHEN'S HANDBOOK §§ 5.01[1-3] at 383-89.

55. COHEN'S HANDBOOK § 5.01[2, 3] at 386-89.

by the government to protect a tribe's access to specific resources in exchange for a cession of land or other resources.[56]

The trust responsibility originates in part in the Supreme Court's interpretations of treaty provisions,[57] which highlighted the tribe's dependency on the federal government for protection after ceding land and other resources.[58] In fact, it was often this guarantee of protection that induced the tribes' assent to the treaties in the first place.[59] Many treaties included a government pledge to manage tribal affairs.[60] However, the duty to manage the affairs of tribes did not result in the loss of the tribe's inherent right to self-governance.[61] Instead, such language often set forth the government's duty to act as a trustee for the benefit of tribes: "For the benefit and comfort of the Indians . . . the United States in Congress assembled shall have the sole and exclusive right of . . . managing all their affairs in such manner as they think proper."[62]

A foundational concept of Indian treaty interpretation is the Reserved Rights Doctrine established by the Court in *United States v. Winans*.[63] The doctrine presupposes that tribes reserve all rights not expressly ceded in treaties. When describing the Treaty of 1855 with the Yakima Nation in *Winans*, the Court explained, "the [T]reaty was not a grant of rights to the Indians, but a grant of right from them – a reservation of those not granted."[64] The Court went on to explain that in executing the Treaty, the federal government did not grant the Tribe access to usual and accustomed fishing places. Rather, the Tribe continued to retain those rights by virtue of its sovereign status.[65]

A treaty promise can be established by an express grant of a right to a resource.[66] For example, the Stevens treaties entered with the tribes of the Pacific Northwest guaranteed the "right of taking fish, at all usual and accustomed grounds and stations."[67] However, treaty language is often not all-encompassing. When treaties are ambiguous, courts utilize the Canons of

---

56. *See, e.g.*, Treaty with the Cherokee, Cherokee-U.S., art. 4, 9, Nov. 28, 1785, 7 Stat. 18; Treaty with the Creeks, Creeks-U.S. art. 3, 5, 6, 8, 9, Aug. 16, 1856, 11 Stat. 699; Treaty with the Sioux-Brule, Oglala, Miniconjou, Yanktonai, Hunkpapa, Blackfeet, Cuthead, Two Kettle, Sans Arcs, and Santee-and Arapaho, 1868, April 29, 1868, art. 2, 15 Stat. 635 [hereinafter Treaty of Fort Laramie].

57. COHEN'S HANDBOOK § 5.04[a][3] at 412.

58. *Cherokee Nation*, 30 U.S. at 10 ; *see also* Mary Christina Wood, *Indian Land and the Promise of Native Sovereignty: The Trust Doctrine Revisited*, 1994 UTAH L. REV. 1471, 1496 (1994).

59. *Id.*

60. Treaty with the Cherokee, *supra* note 56, art. 9.

61. *Worcester*, 31 U.S. at 553-54.

62. Treaty with the Cherokee, *supra* note 56, art. 9.

63. United States v. Winans, 198 U.S. 371, 381 (1905).

64. *Id*.

65. *Id*.

66. Washington v. Wash. State Com. Passenger Fishing Vessel Ass'n, 443 U.S. 658, 668 (1979) [hereinafter Fishing Vessel] (concluding the Stevens Treaties protected the "right of taking fish, at all usual and accustomed grounds and stations" for the tribes named as signatories to the Treaty).

67. *Fishing Vessel*, 443 U.S. at 658; United States v. Washington, 827 F.3d 836, 841 (9th Cir. 2016).

Indian Treaty and Statutory Construction.[68] The Canons include construing ambiguities in the light most favorable to tribes and interpreting treaty language in the manner the tribe would have understood at the time of its creation.[69] Utilizing the Canons, the Supreme Court has interpreted treaties to obligate the federal government to protect tribal interests generally.[70] For example, the Court has interpreted treaty provisions to protect property interests, such as the scope of a tribe's reservation,[71] access to usual and accustomed hunting and fishing locations,[72] access to fish for subsistence and trade,[73] and access to water sources.[74]

The Court has also recognized *implied* property rights in the absence of express treaty language.[75] In *Winters v. United States*, the Court implied a right to water in an Act of Congress ratifying an 1888 executive order establishing the Fort Belknap Reservation despite no express language referencing water.[76] The Court based its conclusion on the purpose of creating the reservation, which was to establish a permanent homeland capable of supporting the tribe's survival. The Court explained that while the executive order lacked express language referencing water, access to water was implied by its necessity in establishing a sustainable homeland. Additionally, the Court referenced the Canons of Construction in its opinion, concluding that both the tribes and the federal government would have understood the agreement to guarantee water access at the time it was created.

Congress may abrogate treaty promises, but the courts require that it clearly state its intent to do so.[77] Courts are reluctant to infer such an intention absent express language.[78] This is illustrated by the Court's interpretation of the Treaty with the Creeks establishing the Muscogee Creek Nations' reservation in *McGirt v. Oklahoma*. In *McGirt*, the Court considered the extent to which Congress disestablished the Tribe's reservation in its subsequent actions, including allotment of lands within the reservation's boundaries and adoption of legislation aimed at limiting the Tribe's self-governance.[79] The Treaty defined geographical boundaries for the Tribe's newly reserved territory, "securing a country and permanent home to the whole Creek Nation of Indians."[80] While the Court explained that abrogation of a treaty provision establishing a tribe's reservation "never required any

68. COHEN'S HANDBOOK § 2.02[1] at 113.

69. *Id*.

70. *See, e.g.*, *Lone Wolf*, 187 U.S. at 556; *Tee-Hit-Ton Indians*, 348 U.S. at 278; *Menominee Tribe of Indians*, 391 U.S. at 412; *Sioux Tribe of Indians*, 316 U.S. at 327; *Lyng*, 485 U.S. at 453.

71. *See* McGirt v. Oklahoma, 140 S. Ct. 2452 (2020).

72. *Winans*, 198 U.S. at 378.

73. *Fishing Vessel*, 443 U.S. at 668.

74. Winters v. United States, 207 U.S. 564, 576 (1908).

75. *Id.* at 576; *Winans*, 198 U.S. at 381.

76. *Winters*, 207 U.S. at 576 (applying the Canons of Construction to a congressional act ratifying an agreement with the Tribe to establish the Tribe's reservation by executive order).

77. *Lone Wolf*, 187 U.S. at 556; *see also* COHEN'S HANDBOOK § 5.01[2] at 387.

78. 42 C.J.S. *Indians* § 27 (2022); *see also* Solem v. Barlett, 465 U.S. 463, 470 (1984) (concluding "diminishment will not be lightly inferred").

79. *McGirt*, 140 S. Ct. at 2465-67.

80. *Id.* at 2460 (quoting Treaty with the Creeks, *supra* note 56, art. XIV).

particular form of words," it must occur pursuant to a clear congressional statement indicated by express references "to cession or other language evidencing the present and total surrender of all tribal interests."[81] Finding no explicit reference to cession in any subsequent act of Congress, and therefore no clear statement, the Court concluded that Congress never disestablished the Muscogee Creek Nation's reservation.

Furthermore, courts also look for evidence that Congress considered the effect of the abrogation on the tribe's protected rights and chose to abrogate the treaty anyway.[82] When considering the effect of the Bald and Golden Eagle Protection Act (BGEPA) on the Yankton Sioux Tribe's 1858 Treaty provision guaranteeing the Tribe's right to hunt bald eagles, the Court in *United States v. Dion* explained that when analyzing congressional actions purporting to terminate treaty rights "what is essential is that Congress actually considered the conflict between its intended action on the one hand and the Indian treaty rights on the other, and chose to resolve that conflict by abrogating the treaty."[83] In *Dion*, the Court found the BGEPA's legislative history indicative of Congress's consideration of the BGEPA on both the Tribe's cultural and religious interests, but because Congress chose to adopt the legislation regardless, the Court found the Treaty right clearly abrogated. However, this principle could be applied to support a finding in favor of upholding treaty rights in future cases.

Despite Congress's plenary power over Indian affairs, courts continue to hold the federal government accountable to tribes for its treaty obligations.[84]

3. Statutes Articulating Obligations to Uphold the Trust Responsibility

Congress possesses plenary power over Indian affairs and has often spoken directly to the federal government's duty to Indian tribes by enacting legislation—such as the Northwest Ordinance, the Non-Intercourse Acts, and the Indian Child Welfare Act—expressly articulating this obligation.[85]

The Northwest Ordinance further formalized the federal government's fiduciary duty to act in good faith with respect to tribal property and resources and applies to tribes in modern-day Illinois, Indiana, Michigan, Wisconsin and portions of Minnesota.[86] It provides "the utmost good faith shall always be observed towards the Indians, their lands and property shall never be taken

81. *Id*.
82. United States v. Dion, 476 U.S. 734, 740 (1986).
83. *Id*.
84. *See, e.g.*, *Worcester*, 31 U.S. at 553; United States v. Mitchell, 463 U.S. 206, 225 (1983) [hereinafter Mitchell II]; Cobell v. Salazar, 573 F.3d 808, 815 (D.C. Cir. 2009).
85. Northwest Ordinance of 1787, art. 3; Non-Intercourse Act, 25 U.S.C. § 177 (1834); Indian Child Welfare Act, 25 U.S.C. § 1901 (1978).
86. Wood, *supra* note 58; *see also Historical Highlights: The Northwest Ordinance of 1787*, U.S. HOUSE OF REPRESENTATIVES https://history.house.gov/Historical-Highlights/1700s/Northwest-Ordinance-1787/ [https://perma.cc/2URZ-N6FS] (last visited Jan. 23, 2023).

from them without their consent; and in their property rights and liberty, they never shall be invaded or disturbed."[87] In 1977, the U.S. District Court for the Northern District of Indiana in *Swimming Turtle v. Board of County Commissioners of Miami County* held that Article III of the Ordinance prohibits the state (in this case, Indiana) from confiscating or taxing Indian property without consent.[88]

The Non-Intercourse Act of 1834 gave the federal government the exclusive authority of conducting trade with and acquiring land from tribes.[89] The purpose of the Act was to enforce recognized treaty protections in an effort to eliminate hostile and often unfair commercial interactions between Indians and non-Indians.[90] Courts have long recognized that the Act creates a fiduciary duty requiring the federal government to act as a trustee in the management of tribal lands.[91] The Second Circuit characterized it as both protecting a tribe's right of occupancy and "prevent[ing] the unfair, improvident, or improper disposition of Indian lands."[92] Furthermore, the Second Circuit has rejected the assertion that Congress at any point terminated that duty through subsequent actions.[93] Because the Non-Intercourse Act applies to "any . . . tribe of Indians," courts have construed it to apply to all tribes, regardless of federal recognition.[94]

Taken together, these Acts illustrate the federal government's fiduciary duty to tribal nations.[95]

4. Framework for Judicially Enforceable Remedies

While the trust obligation itself has a broad reach, the ability to recover damages for its breach is very limited. Recovery is restricted to circumstances in which a specific statute or regulation sets forth the government's obligation.[96] Historically, the U.S.'s sovereign immunity has limited tribes' ability to sue the federal government for failure to uphold trust obligations.[97] Tribes generally lacked a forum to bring such claims until Congress created the Indian Claims Commission (ICC) in 1946.[98] The ICC created a Court of Claims, which initially had jurisdiction to hear only land claims by tribes that accrued prior to the year 1946, and required these claims to be brought within

87. Wood, *supra* note 58.

88. Swimming Turtle v. Bd. of Cnty. Com'rs of Mia. Cnty., 441 F.Supp 374, 377 (N.D. Ind. 1977).

89. 25 U.S.C. § 177.

90. FRANCIS PAUL PRUCHA, THE GREAT FATHER 30 (1986).

91. Joint Tribal Council of the Passamaquoddy Tribe v. Morton, 528 F.2d 370, 379 (1st Cir. 1975).

92. *Id*. at 377.

93. *Id.* at 380.

94. *Id*. at 376-77.

95. Northwest Ordinance of 1787, art. 3; Non-Intercourse Act, 25 U.S.C. § 177.

96. United States v. Jicarilla Apache Nation, 564 U.S. 162, 166 (2011).

97. Vicki C. Jackson, *Suing the Federal Government: Sovereignty, Immunity, and Judicial Independence*, 35 GEO. WASH. INT'L L. REV. 521 (2003).

98. JUDITH ROYSTER ET. AL., NATIVE AMERICAN NATURAL RESOURCES LAW 186 (4th ed. 2018).

a six-year period.[99] Claims that accrued after 1946 can still be heard in the Court of Claims today pursuant to the Indian Tucker Act.[100]

Under the Indian Tucker Act, a tribe may bring a claim against the Government for breach of trust.[101] In *United States v. Mitchell* (*Mitchell II*), the Court considered the extent to which the BIA's alleged mismanagement of timber resources within the Quinault Reservation constituted a breach of the trust responsibility warranting damages. The BIA exercised "comprehensive control over the harvesting of Indian timber" pursuant to statutes and BIA regulations.[102] The Court explained that ". . . a fiduciary relationship arises when the Government assumes control over . . . property belonging to Indians," finding the BIA's actions and failure to uphold the trust responsibility warranted damages.[103]

Furthermore, the Court in *Mitchell II* found the existence of a fiduciary relationship supporting an Indian Tucker Claim "even though nothing is said expressly in the authorizing or underlying statute (or other fundamental document) about a trust fund, or a trust or fiduciary connection."[104] Generally, however, this precludes a tribe from seeking to enforce a trust obligation based on common law trust principles.[105] Utilizing the *Mitchell II* framework, claimants must show that the source of law upon which their claim is based "can fairly be interpreted as mandating compensation by the federal government for the damages sustained."[106]

Tribes have successfully sought redress for wrongfully abrogated treaty promises by showing that the harm warranted just compensation pursuant to the Fifth Amendment, as illustrated in *Sioux Nation*.[107] The procedures governing these actions are similar to those described previously for breach of trust actions in the Court of Claims under the Indian Tucker Act.[108] A successful takings claim must pass the Fort Berthold test set forth in *Sioux Nation*. The claim must demonstrate that Congress did not make a good faith effort to provide the tribe with compensation equal to the full value of the resource in question by transmuting the property interest from land to money.[109]

---

99. 28 U.S.C. § 1505; *see also* 28 U.S.C. § 2501 (establishing a six-year statute of limitations for claims brought in the U.S. Court of Federal Claims).

100. *Id*.

101. *Id*.

102. *Mitchell II*, 463 U.S. at 209; *see also* 25 U.S.C. §§ 406-07, 5109.

103. *Mitchell II*, 463 U.S. at 225 (quoting Navajo Tribe of Indians v. United States, 224 Ct. Cl. 171, 183 (1980)).

104. *Id.*

105. *Jicarilla Apache Nation*, 564 U.S. at 165.

106. *Mitchell II*, 463 U.S. at 216-17 (citing United States v. Testan, 424 U.S. 392, 400 (1976)).

107. *Sioux Nation*, 448 U.S. at 416.

108. *See* discussion *infra* Section III.B.4 "Framework for Judicially Enforceable Remedies".

109. *Sioux Nation*, 448 U.S. at 416.

III. ANALYSIS

A. Wireless Spectrum Law Analogized to the Law of Property

Generally, the physical characteristics of spectrum and, by extension, the property interests that accompany spectrum licenses can be analogized to those traditionally associated with land, such as the right to exclude and the right to transfer.[110] Historically, the concept of *cujus est solum ejus est usque ad coelum* (*ad coelum*), or the Latin phrase for "whoever owns land it is theirs up to the heavens and down to hell,"[111] was thought to extend a landowner's property rights to space above and below the land's surface.[112] While the Communications Act itself limits the comparison between wireless spectrum and land by defining the FCC's purpose to manage spectrum as ". . . provid[ing] for the use of such channels, but not the ownership thereof,"[113] licensees nevertheless retain the ability to exclude others and to transfer their interest to other parties, subject to FCC approval.[114]

Like land, wireless spectrum is a scarce resource.[115] Spectrum may differ from land in terms of its physical characteristics, but the basic property principles applicable to both remain similar. Rights to both resources are acquired via financial transactions, and property interest holders can expect to have their interests protected from intrusion by outside entities.[116] Landowners retain the right to file an action for trespass against an unwelcome entrant, and spectrum licenses inherently exclude those without a license from operating within a particular frequency.[117]

Furthermore, both landowners and spectrum license holders may transfer their property interest to another party.[118] Landowners may do so in part or in full, through easements or via a sale of the landowner's fee simple interest.[119] While the transfer of spectrum licenses is subject to FCC review and determination that the proposed transfer is consistent with the "public interest, convenience and necessity," the underlying right to transfer remains.[120] Other similarities exist as well such as the application of regulations that may affect a property interest, including zoning ordinances

---

110. John W. Berresford & Wayne A. Leighton, *The Law of Property and the Law of Spectrum: A Critical Comparison*, 13 COMMLAW CONSPECTUS 35, 36 (2009).

111. LAURA K. DONAHUE, WHO OWNS THE SKIES? AD COELUM, PROPERTY RIGHTS, AND STATE SOVEREIGNTY 1 (2021).

112. *See id*. at 1-3 (citing 2 WILLIAM BLACKSTONE, COMMENTARIES *18).

113. 47 U.S.C. § 301; *see also* Radio Act, 47 U.S.C. § 4 (1927) (establishing the basis for declaring wireless spectrum incompatible with private ownership).

114. *See* 47 U.S.C. § 309 (vesting the FCC with the authority to grant applications for spectrum licenses).

115. *See* Berresford & Leighton, *supra* note 110.

116. *Id* at 39.

117. *Id*.

118. *Id.* at 39-40; *see also Spectrum Leasing*, FED. COMMC'NS COMM'N, https://www.fcc.gov/wireless/bureau-divisions/technologies-systems-and-innovation-division/spectrum-leasing [https://perma.cc/SRY3-7QLT].

119. Berresford & Leighton, *supra* note 110, at 39-40.

120. *Id.* at 40 ; *see also* 47 U.S.C. § 301.

affecting land and designation of certain spectrum frequencies for particular uses.[121]

Both land and wireless spectrum are valuable resources. The value of wireless spectrum is relevant in two respects: First, tribes need access to wireless spectrum both to deploy broadband services within their respective territories and to leverage the licenses as revenue-generating assets. Both are essential to furthering federal and tribal interests in promoting tribal self-determination and economic development.[122] Second, the immense financial value associated with spectrum licenses underscores the severity of the tribe's loss as a result of the federal government's failure to protect tribal access to a valuable resource. For these reasons, it is crucial that tribes assert their rightful claim to the wireless spectrum corresponding to their respective tribal territories.

B. Federal Trust Responsibility Analysis

The federal government failed to fulfill its trust obligation to protect tribal access to wireless spectrum beginning with Congress' assignment of authority over all wireless spectrum in the U.S. to the FCC in the Communications Act and continuing today with the FCC's assignment of spectrum licenses over tribal territories to non-tribal entities.[123] As wireless spectrum resembles land in its property interests, the trust responsibility should be similarly interpreted as applicable to wireless spectrum where it corresponds to tribal territories.[124]

First, while the Court concluded tribes lack full fee simple ownership over their ancestral homelands, tribes were nevertheless recognized as retaining valuable property rights apart from the right to transfer.[125] When treaties set forth the physical boundaries of a tribe's reservation, the federal government recognized the rights of occupancy and use of the land, otherwise known as original Indian title, remained with the tribe.[126] The right of occupancy and use includes the right to utilize spectrum corresponding with tribal lands. A court should similarly conclude that the trust responsibility obligates the government to recognize similar property rights in wireless spectrum. All spectrum licenses corresponding to a tribe's reservation or territory should be included in the resources recognized as warranting protection.

Second, when Congress authorized the FCC in the Communications Act to manage all non-federal use of wireless spectrum in the U.S., it divested tribes of their rightful ownership of the spectrum associated with their

121. Berresford & Leighton, *supra* note 110, at 39-40.

122. *See* California v. Cabazon Band of Mission Indians, 480 U.S. 202, 203 (1987) (recognizing an inherent federal interest to promote tribal self-determination and economic development).

123. 47 U.S.C. § 301.

124. Berresford & Leighton, *supra* note 110, at 36.

125. *Johnson*, 21 U.S. at 573.

126. *Id.*

respective tribal territories.[127] This is illustrated by the Communications Act's reference to radio spectrum as a resource incompatible with ownership and instead directing the FCC to allocate spectrum licenses pursuant to the "public interest, convenience and necessity."[128] Congress expressly violated its trust responsibility by transforming wireless spectrum into a resource incapable of traditional ownership, ignorant of the reality that tribes at least retained the right of occupancy and use of the spectrum.[129] Today, those rights would be realized by a tribe's ability to retain spectrum licenses themselves rather than competing for licenses in incentive auctions, by excluding others from use in particular frequencies, and by exercising self-determination in making decisions about how best to utilize spectrum for the benefit of the tribal community.

Third, the federal government continues to act in opposition to the trust responsibility by not only refusing to amend the Communications Act to recognize tribal ownership of spectrum corresponding to tribal territories, but also by continuing to grant spectrum licenses within tribal territories to non-tribal entities.[130] While data on the number of tribes with wireless spectrum licenses is scarce, non-tribal ownership of licenses corresponding to tribal lands is demonstrated by comparing the list of published license winners following the conclusion of each incentive auction with the geographic boundaries of tribal communities.[131] Additionally, the FCC maintains a spectrum license search tool on its website that allows any user to quickly observe that wireless carriers unassociated with tribes retain spectrum licenses within tribal territories.[132] With each new approval of a license corresponding to a tribe's territory to a non-tribal entity, the federal government continues to act in defiance of its obligation to manage tribal resources for a tribe's benefit.

C. Treaty Analysis

Congress abrogated an implied treaty right to wireless spectrum when it transferred authority to manage wireless spectrum to the FCC in the Communications Act.[133] While treaties entered into with tribes lack an express guarantee to wireless spectrum access, courts could imply treaty rights to wireless spectrum.

---

127. *See* 47 U.S.C. § 301.

128. *Id.*; *see also* Radio Act, 47 U.S.C. § 4 (1927) (establishing the basis for declaring wireless spectrum incompatible with private ownership).

129. *Johnson*, 21 U.S. at 573.

130. *See License Search*, FED. COMMC'NS COMM'N, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchLicense.jsp [https://perma.cc/B33N-YUX4] (showing a list of incumbent license holders corresponding to all of the U.S., including tribal lands) [hereinafter FCC License Search].

131. *See, e.g.*, *id.*; Press Release, *FCC Announces Winning Bidders in C-Band Auction,* FED. COMMC'NS COMM'N (Feb. 24, 2021), https://docs.fcc.gov/public/attachments/DOC-370267A1.pdf [https://perma.cc/5PNG-PJGD].

132. *See* FCC License Search, *supra* note 130.

133. *See* 47 U.S.C. § 301.

U.S. courts have yet to recognize an implied right to wireless spectrum based on treaty language. However, the idea is not without precedent. The Waitangi Tribunal in New Zealand concluded that the Treaty of Waitangi protected the Maori's *rangatiratanga*, or right to exercise self-determination, pertaining to its radio spectrum allocation.[134] The Tribunal further held that the English Crown was obligated under the Treaty's Article II provisions to recognize and protect the Maori's claim to radio spectrum; this not only prohibited the Crown from transferring the Maori's property interest to another party without the express consent of the tribe, but also guaranteed the Maori's full autonomy to manage its spectrum interests.[135] The Tribunal's determination was based on its characterization of wireless spectrum as a natural resource, and was further informed by the following language:

> Her Majesty the Queen of England confirms and guarantees to the Chiefs and Tribes of New Zealand and to the respective families and individuals thereof the full exclusive and undisturbed possession of their Lands and Estates Forests Fisheries and other properties which they may collectively or individually possess so long as it is their wish and desire to retain the same in their possession . . . [136]

Specifically, the Tribunal found the language guaranteeing "full exclusive and undisturbed possession" informative of the Crown's duty to recognize and respect the Maori's property interests in natural resources existing within the Maori territory.[137] The Tribunal characterized spectrum as such a resource and further recognized its potential to contribute to the preservation of Maori culture and language.[138]

Tribes in the U.S. can argue an implied treaty right to wireless spectrum exists on two grounds. First, as discussed above, tribes can point to the purpose for which their treaties were entered into, to create a home for the tribe, to support their claim.[139] While neither the tribes nor the federal government were aware of the physical properties of wireless spectrum and its future value at the time treaties were entered into, tribes can attest to the fact that Internet access has since become, like other natural resources, an essential component of making a home sustainable.[140]

Second, language similar to the Waitangi Treaty can be found in treaties negotiated between the U.S. and tribes such as the Arapaho and Sioux tribes, including the Brule, Oglala, Miniconjou, Yanktonai, Hunkpapa, Blackfeet,

---

134. WAITANGI TRIBUNAL, REPORT OF THE WAITANGI TRIBUNAL ON CLAIMS CONCERNING THE ALLOCATION OF RADIO SPECTRUM 9 (1990).

135. *Id*.

136. Treaty of Waitangi, NZ-Waitangi, art. 2 [1840] 1840 NZTS 04 ("signed 2 June 1840, entered into force 2 June 1840").

137. WAITANGI TRIBUNAL, *supra* note 134.

138. *Id*.

139. *See Winters*, 207 U.S. at 565 (explaining that the purpose of creating the reservation was to establish a permanent home for the Tribe, and concluding the Treaty impliedly guarantees the Tribe access to waterways to effectuate that purpose).

140. *See* McClain et al., *supra* note 3.

Cuthead, Two Kettle, Sans Arcs, and Santee that were parties to the Fort Laramie Treaty of 1868.[141] Article II of the Treaty "set apart for the absolute and undisturbed use and occupation of the Indians herein named" the Great Sioux Reservation in exchange for ceding thousands of other valuable acres to the U.S.[142] Utilizing the Waitangi Tribunal's analysis, tribes can argue that language similar to the phrase highlighted in the Fort Laramie Treaty protects a tribe's property interests in wireless spectrum.

Upon finding an implied treaty right to spectrum, the Reserved Rights Doctrine further strengthens a tribe's claim to spectrum as tribes inherently reserve all rights not expressly ceded in treaties.[143] Because treaties lack express language referencing spectrum, it necessarily follows that tribes did not cede their spectrum rights in treaties and retain those rights today.

Congress may only abrogate treaty promises subject to an explicit intention to do so and upon evidence that it considered the effect of abrogation on the tribe's protected rights and chose to abrogate anyway.[144] One could argue that the Communications Act is itself a clear statement by Congress to abrogate an implied treaty right to wireless spectrum by virtue of its assignment of authority to the FCC to manage spectrum. However, the Communications Act lacks any express language referring to a tribe's claims to spectrum, and in fact, the word "tribe" does not appear in the Communications Act at all.[145] Therefore, this argument would be based on an implied abrogation, pursuant to the language conferring onto the FCC the authority to manage all non-federal use of spectrum. An implied abrogation argument hardly passes the clear statement standard. There is no evidence that Congress considered the effect of the Communications Act on a tribe's spectrum interests, as evidenced by the fact that the Act does not refer to tribes or tribal governments once.[146] Absent additional evidence that Congress contemplated the consequences of stripping tribes of their spectrum property interests, abrogation that meets the clear statement standard cannot be inferred.

However, tribes asserting this argument must address the U.S. District Court for the District of South Dakota's holding in *Alltell Communications, LLC v. Oglala Sioux Tribe*, which rejected the Tribe's claim that the Treaty of Fort Laramie vested the Tribe with a property interest in the spectrum corresponding to the Tribe's territory.[147] The court considered the claim by

141. Treaty of Fort Laramie, *supra* note 56, art. 2; *see also* Treaty of Fort Laramie, NAT'L ARCHIVES, https://www.archives.gov/milestone-documents/fort-laramie-treaty#:~:text=In%20the%20spring%20of%201868,and%20Santee)%20and%20the%20Arapaho. [https://perma.cc/X8NH-GXJG] (last visited Nov. 9, 2023) (identifying the list of tribes that were parties to the Treaty).

142. *Id*.

143. *Winans*, 198 U.S. at 381.

144. *Lone Wolf*, 187 U.S. at 556 (establishing Congress's authority to abrogate treaty promises); *see also Dion*, 476 U.S. at 740 (explaining the requirement that Congress must consider the effect of the abrogation on tribal interests).

145. *See* 47 U.S.C. § 151.

146. *Id*.

147. Alltell Commc'ns, LLC. v. Oglala Sioux Tribe, No. 10-5011-JLV, 2011 WL 796409, at *6 (D.S.D. Feb. 28, 2011).

analogizing spectrum to land rather than a natural resource, framing the inquiry as the extent to which the spectrum constituted part of the land upon which the Tribe exercised undisturbed use and occupation.[148] The Court inaccurately concluded on two grounds: (1) the Treaty's recognition of the Tribe's undisturbed use and occupation of the territory did not extend to the spectrum above[149]; (2) even if the Tribe's property interest in land did include spectrum, the FCC's current regulation of the spectrum does not interfere with the Tribe's undisturbed use and occupation of its territory.[150]

Tribes within the court's jurisdiction or signatories to the Treaty of Fort Laramie can attack both conclusions as follows. In support of its first conclusion, the court rejected *ad coelum* as a justification for finding a claim to the physical property both above and below the surface of the Tribe's territory.[151] The Court declined to recognize the maxim as applicable here, articulating a concern that such recognition would necessarily lead to troubling practical implications, including tribes initiating trespass actions against parties, such as aircraft, unlawfully violating the airspace above tribal land.[152] These concerns, however well-intentioned, are misplaced and fail to recognize that the property interest vested in spectrum license holders today is limited to the frequency associated with the license.[153]

First, the re-recognition of a tribe's claim to wireless spectrum could similarly be limited to the use of the spectrum in the deployment of telecommunications services, not extending to trespass or any other claim unrelated to the use of the spectrum for telecommunications purposes. This type of limited-use property claim is consistent with Indian title, or a tribe's recognized right of occupancy and use, over its land.[154] Second, the court could have evaluated the Tribe's claim by comparing spectrum to a treaty-protected natural resource, rather than by considering whether the Tribe's land rights extended to it a claim to the airspace above. A natural resource-based analysis would follow the reasoning employed by the Waitangi Tribunal in its evaluation of the Maori's claim to spectrum and could be further bolstered by a reference to the *Winans* implied rights doctrine.[155] Lastly, the court's emphasis on wireless spectrum's incompatibility with private ownership accepts without question the harm at the very issue of this inquiry.[156] It is precisely Congress' transformation of spectrum into a resource inconsistent with private ownership that injured tribes in the first place, divesting them of access to a valuable resource. Instead of accepting as lawful the FCC's regulatory authority over spectrum associated with tribal lands, courts must reevaluate each spectrum claim at the harm's origin or beginning

148. *Id.* at *4.
149. *Id*.
150. *Id.* at *6.
151. *Id*. at *4.
152. *Id.*
153. *See* Trick, *supra* note 20.
154. *See Johnson*, 21 U.S. at 573.
155. *See* discussion i*nfra* IV.C "Treaty Analysis."
156. 47 U.S.C. § 301; *see also* Radio Act, 47 U.S.C. § 4 (1927) (establishing the basis for declaring wireless spectrum incompatible with private ownership).

with the recharacterization of spectrum as incompatible with private ownership.

Regarding its second finding, the court rationalized that the Tribe could still access and use the spectrum associated with its territory through participation in the FCC's regulatory scheme, or by simply purchasing and competing for licenses like any other prospective licensee.[157] In fact, the court referenced actions taken by the Tribe, including submissions made to the FCC, in concluding the Tribe suffered no actual harm by the FCC's regulation of the spectrum corresponding to its territory.[158] However, in so holding the court ignores the reality that spectrum licenses can only be acquired at an immense financial cost.[159] A treaty-protected right to spectrum lawfully empowers tribes to use the spectrum without expending unnecessary financial resources to gain access to it in the first place. Additionally, the Tribe's efforts to gain access to spectrum through compliance with the FCC's regulations should not be construed as the Tribe's recognition that the current regulatory scheme is lawful. The court's decision penalizes the Tribe for taking action to bolster Internet access within its territory, relying on these actions to justify barring the Tribe from challenging the FCC's authority to regulate access to spectrum in the future.

Despite the court's holding, tribes retain valid claims to wireless spectrum and must consider adjudicating these claims in court.

D. Judicial Claims

Prior to addressing each independent statutory source, it is important to note that a claim purely based on Congress's assignment of authority over spectrum in the Communications Act will likely be time-barred as a result of the ICC's requirement that all claims accruing before 1946 be brought within five years of the ICC's establishment.[160] Congress could, if it wished, pass a special jurisdictional act waiving sovereign immunity and granting tribes the opportunity to seek redress.

However, even in the absence of such action, tribes can file a claim under the Indian Tucker Act based on the FCC's assignment of spectrum licenses to non-tribal entities after 1946 subject to a six-year statute of limitations.[161] To demonstrate a judicially enforceable claim against the Government under the Indian Tucker Act under the *Mitchell II* framework, tribes must point to Acts of Congress, statutes, regulations or other sources of law independent from the Indian Tucker Act itself that establish a duty fairly determined to warrant damages.[162] Taken together, (1) the Communications

157. *Alltell*, 2011 WL 796409, at *6.
158. *Id*.
159. *See* Layton, *supra* note 27.
160. Indian Claims Commission Act, 25 U.S.C. § 2A (1946).
161. Indian Tucker Act, 28 U.S.C. § 1505; *see also* 28 U.S.C. § 2501 (establishing a six-year statute of limitations for claims brought under Indian Tucket Act).
162. *Mitchell II*, 463 U.S. at 216.

Act itself, (2) the Non-Intercourse Act of 1834, and (3) the Northwest Ordinance warrant damages to tribes.[163]

Alternatively, tribes can assert a claim for wrongful taking in violation of the Fifth Amendment utilizing the analysis in *Sioux Nation* and by satisfying the Fort Berthold test.[164]

1. Breach of Trust Claim

a. The Communications Act of 1934

The language set forth in the Communications Act provides for the taking of wireless spectrum ownership from tribes in favor of the FCC.[165] Utilizing the *Mitchell II* framework, a court could conclude that the FCC's control over wireless spectrum assets belonging to tribes creates a judicially enforceable fiduciary duty.[166] While the statutes at issue in *Mitchell II* concerned managing timber harvests for the benefit of Tribe, the Court's conclusion was based in large part on the fact that the BIA had assumed comprehensive control over tribal assets.[167]

The comprehensive control exercised by the FCC over all non-federal use of wireless spectrum likely satisfies the *Mitchell II* standard and thus imposes a fiduciary responsibility capable of supporting an action under the Indian Tucker Act. While the Communications Act fails to set forth a duty to manage wireless spectrum on behalf of tribes expressly, the *Mitchell II* framework does not require an express reference to a fiduciary duty to warrant damages.[168] Consequently, a fiduciary relationship should nevertheless be implied as a result of the robust and comprehensive control exercised by the FCC over spectrum assets belonging to tribes.[169]

b. The Non-Intercourse Act of 1834

Failure to protect a tribe's wireless spectrum access similarly violates the trust responsibility under the Non-Intercourse Act of 1834 to dutifully manage tribal lands.[170] While the Non-Intercourse Act imposes a fiduciary duty on the federal government with respect to tribal land, it remains the law today[171], and courts could extend its applicability to wireless spectrum given the similarity in property rights between land and spectrum discussed previously.

---

163. 47 U.S.C. § 151; Northwest Ordinance of 1787, art. 3; Non-Intercourse Act, 25 U.S.C. § 177 (1834).
164. *Sioux Nation*, 448 U.S. at 407.
165. *See* 47 U.S.C. § 301.
166. *Mitchell II*, 463 U.S. at 225-26.
167. *Id*. at 224.
168. *Id*.
169. *See* 47 U.S.C. § 151.
170. *See* 25 U.S.C. § 177 (establishing a duty to duly manage tribal lands).
171. *Id*.

c. The Northwest Ordinance of 1787

Because the Ordinance only applies to a small subset of states, only tribes within that area would be able to rely on it. Tribes can point to the U.S. District Court for the for the Northern District of Indiana's conclusion in *Swimming Turtle* that the Ordinance prohibits government interference with property owned by tribal members.[172] This precedent could easily enable a court to recognize an analogous prohibition against seizure of a tribe's spectrum access in the Ordinance's pledge to observe and respect a tribe's property rights.

Considered together, the Communications Act, the Non-Intercourse Act of 1834, and the Northwest Ordinance of 1787 establish the basis for a judicially enforceable breach of trust claim warranting compensation.[173]

2. Fifth Amendment Takings Claim

Assuming Congress did not successfully abrogate a tribe's implied treaty right to wireless spectrum, the treaty right itself remains a judicially enforceable property interest.[174] Therefore, the remedy would be similar to a breach of trust action under the Indian Tucker Act:[175] tribes can point to *Sioux Nation* to assert a claim for an unconstitutional taking in violation of the Fifth Amendment and argue that, at the very least, the taking of their wireless spectrum assets required just compensation.[176]

Much like the right to the Black Hills, the right to spectrum is similarly guaranteed by treaties, either impliedly by the necessity of Internet access for tribes to sustain a home or by specific language similar to the Treaty of Fort Laramie.[177] However, the federal government's actions do not pass the Fort Berthold test, as no attempt whatsoever to compensate the tribes for its divestiture of their spectrum assets has been made.[178] Just as the Court concluded the federal government failed to exercise a good faith effort to compensate the Sioux Nation for the taking of the Black Hills, so should a court conclude that the taking of a tribe's wireless spectrum interests warrants just compensation. While many tribes would rather have their claims to spectrum restored, spectrum is an incredibly valuable resource, and tribes should at least be compensated at a rate equivalent to the value of spectrum licenses sold at auction.

---

172. *See Swimming Turtle*, 441 F.Supp. at 377.

173. *See* 47 U.S.C. § 151; Northwest Ordinance of 1787, art. 3; *see also* Non-Intercourse Act, 25 U.S.C. § 177 (1834).

174. *See* COHEN'S HANDBOOK § 5.01[2] at 387.

175. *See* discussion *infra* section IV.D "Judicial Claims."

176. *Sioux Nation*, 448 U.S. at 407-08.

177. *See* Treaty of Fort Laramie, *supra* note 56, art. 2.

178. *See Sioux Nation*, 448 U.S. at 416.

IV. ADDITIONAL REMEDIES

A. Actions by the FCC

The FCC has the authority to determine the method and manner by which spectrum licenses are allocated, assigned, and used.[179] While these actions must serve the "public interest, convenience, and necessity," the FCC can take a number of actions to restore—or, at the very minimum, increase—a tribe's access to spectrum.[180] Doing so would serve the public interest by equipping tribal communities with infrastructure capable of supporting robust broadband solutions.

1. Immediate Reassignment of Spectrum Licenses

From a practical standpoint, the greatest challenge to restoring tribal claims to wireless spectrum is the reality that many licenses corresponding to tribal territories have since been assigned to third-party entities unaffiliated with the tribes themselves.[181] These entities were likely either awarded the license via auction or acquired the license in an after-market transaction from an incumbent license holder. Regardless of the method, purchasing spectrum licenses often requires a significant financial investment and constitutes a property interest that any license holder would endeavor to keep. However, the fact that non-tribal entities now own these licenses does not change the reality that the spectrum was stolen from tribes in the first place, nor does it negate a tribe's rightful claim to its use.

Although it would be well within the authority of the FCC to do so, it is unlikely the FCC will elect to unilaterally reassign spectrum licenses to tribes for fear of enduring litigation, including a potential challenge to the agency's action under the Administrative Procedures Act (APA).[182] Tribes are nevertheless entitled to receive exclusive licenses to operate within every spectrum band corresponding to their respective tribal territories, and the FCC should reassign such licenses to tribal nations in an effort to right the wrongs of the past.[183]

The FCC may or may not consider compensating incumbent licensees for an amount equal to the cost of acquiring the license, whether at auction or by third-party transaction. Compensating licensees would require extensive financial resources to execute, but it would restore the license holders to their financial position prior to obtaining the license. Additionally, licensees may argue that their reliance interests warrant additional compensation related to the revenue they anticipated generating from putting their license to use. This

179. 47 U.S.C. § 303(y).

180. *Id*.

181. *See* FCC License Search, *supra* note 130 (showing list of licensees corresponding with tribal lands).

182. Administrative Procedures Act, 5 U.S.C. § 706(2)(a) (1966).

183. *See* discussion *infra* section IV.B "Federal Trust Responsibility Analysis."

may result in additional litigation that the federal government is likely to avoid.

2. Reassignment of Spectrum Licenses After Current Licenses Expire

Because spectrum licenses are limited in their duration to a set number of years, licensees must eventually seek renewal of their license from the FCC.[184] The FCC retains the right to elect not to renew a particular license if it finds that renewal will be contrary to the "public interest, convenience, and necessity." For reasons similar to those highlighted above, the FCC should consider electing not to renew licenses corresponding with tribal lands at the end of their term. The difficulty here is similarly demonstrating how nonrenewal will serve the public interest when the public encompasses both the interests of tribes and incumbent licensees. However, the federal trust obligation is a compelling interest worthy of sustaining a challenge to an agency's decision not to renew. If the FCC chooses to renew incumbent licenses regardless, tribes are nevertheless still owed compensation, and the FCC should dedicate a percentage of their license proceeds to compensating tribes whose spectrum is leased by a non-tribal entity.

3. Spectrum Sharing

Should the FCC elect not to reassign spectrum licenses to tribes, the FCC should adopt a spectrum-sharing policy allowing tribes to share access to a particular band of spectrum with the incumbent licensee. The goal of spectrum sharing is to utilize spectrum more efficiently while also minimizing interference between multiple users.[185] The feasibility of spectrum sharing is dependent upon the physical properties of each frequency itself.[186] Therefore, the FCC would likely need to evaluate frequencies for compatibility with a spectrum sharing solution, and further develop use rules to minimize interference between the incumbent licensee and the tribe.[187] This solution does not restore a tribe's exclusive access to spectrum, but it would at least provide tribes with some access to a resource critical to the successful deployment of broadband solutions.

4. Assignment of Unallocated Spectrum to Tribes

Finally, the FCC should immediately assign all unallocated spectrum, or whitespace, in every band associated with tribal territories to tribes. The FCC took similar action with regard to the 2.5 GHz band, assigning all unallocated spectrum associated with tribal territories to tribes at no cost.[188]

184. *See* 47 U.S.C. § 303.
185. Benjamin & Speta, *supra* note 21, at 123.
186. *Id.*
187. *Id.*
188. *See* Transforming the 2.5 GHz Band, *supra* note 29, at para. 47.

In doing so, the FCC acknowledged the duty of protection owed to tribes by the federal government.[189] This solution avoids the issue associated with taking a license away from an incumbent licensee because the spectrum in question is unassigned. Furthermore, assigning unallocated spectrum to tribes results in a more efficient use of spectrum overall, as otherwise, the spectrum remains unused and its benefits unrealized.

While the FCC assigned 2.5 GHz licenses to tribes without seeking payment for the license itself, it required tribes to comply with build-out requirements to retain the license long-term. The requirements include the tribe demonstrating that it can serve up to fifty percent of the population within its service area two years after acquiring the license.[190] This percentage increases to eighty percent at five years.[191] Meeting the FCC's build-out requirements will necessarily require a significant financial investment to purchase equipment and material to build infrastructure capable of providing Internet service. Access to capital continues to function as a barrier to infrastructure deployment within tribal communities. Therefore, the FCC should decline to include build-out requirements for future allocations of unassigned spectrum to tribes. Tribes should be given full autonomy to decide how and when to utilize their spectrum assets free of government oversight.

V. CONCLUSION

The history of the federal government's dealings with tribes is rife with empty promises and failure to uphold its trust obligation. Congress, the courts, and the FCC have the opportunity to address the wrongs committed against tribal nations by taking action to restore each tribe's claim to the wireless spectrum associated with their respective tribal territories. By pursuing the solutions explored, the U.S. can ensure that tribal nations are no longer left behind without the resources necessary to bridge the digital divide in tribal communities.

189. *Id*. at para. 49.
190. *See 2.5 GHz Rural Tribal Window*, *supra* note 29.
191. *Id*.