EDITOR'S NOTE

The Federal Communications Law Journal is proud to present the second Issue of Volume 75. We are the nation's premiere communications law journal and the official journal of FCBA: The Tech Bar hosted at The George Washington University Law School. We are excited to feature a practitioner Article and four student Notes which provide analysis and insight into a range of policy questions facing the telecommunications field today.

This Issue begins with an Article written by Kal Raustiala, a Promise Institute Distinguished Professor of Comparative and International Law and the Director of the UCLA Burkle Center for International Relations. Raustiala explains why the Obama administration chose to relinquish formal federal government control over the naming and numbering system of the Internet, surrendering this authority to the non-profit Internet Corporation for Assigned Names and Numbers ("ICANN"). Raustiala goes on to detail the implications for multistakeholder governance throughout international law.

The first student Note, written by John Bogert, takes a market approach to stopping misinformation. Bogert proposes a statutory cap for social media market mergers under the Clayton Antitrust Act and argues against current proposals for reforming Section 230. In the second Note, author Julia Wells provides an overview of telehealth services—an industry that became increasingly important during the pandemic. Wells argues both that the FCC should be given broader authority to regulate these services and that HIPAA should be reformed to increase flexibility and prevent data breaches.

The third Note, authored by Nicolas Florio, explains how current bankruptcy law can provide a guide for strengthening the FCC and FTC's collection of consumer fraud penalties. Florio proposes modifications to the way consent decrees are drafted which would strengthen the agencies' enforcement powers and ultimately improve security across the telecommunications industry. The final Note in this Issue, written by Rebecca Roberts, presents the benefits and potential harms that arise with the use of post-mortem digital cloning. Roberts explores this unique intersection of probate law and artificial intelligence and argues that requiring explicit, affirmative consent from a decedent prior to their death is the best way to protect against unauthorized use of this technology.

The Editorial Board of Volume 75 would like to thank the FCBA and The George Washington University Law School for their continued support of our Journal. We would also like to acknowledge the contributions of the authors and editors who worked on 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.

Julia Dacy
Editor-in-Chief

Federal Communications Law Journal

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

As the official journal of the Federal Communications Bar Association, the *Journal* is distributed to over 2,000 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 Joe Christensen, Inc.

Citation: Please cite this issue as 75 FED. COMM. L.J. ___ (2023).

FEDERAL COMMUNICATIONS LAW JOURNAL

THE TECH JOURNAL

GW LAW VOLUME 75 ISSUE 2 fcba THE TECH BAR

JANUARY 2023

ARTICLES

The Internet is the most significant global political and economic resource of our time. States increasingly seek to control it and bend it to their purposes. Nonetheless, in a surprising and controversial move in 2016, the Obama administration yielded control over the architecture of domain names and IP numbers that makes the Internet work to the Internet Corporation for Assigned Names and Numbers ("ICANN"), a non-profit organization headquartered in California. This action creates a puzzle for theories of international law and organization. Existing accounts of international organization often focus on theories of delegation and principal-agent models to explain why international organizations are created and how they work. Using these theoretical lenses, this Article explores the unusual case of ICANN and in particular its "multistakeholder" regulatory model, in which a wide variety of actors, not just governments, regulate central aspects of the complex global resource we know as the Internet. This Article argues that while ICANN began as a standard story of delegation to a regulatory agency, it morphed into something much closer to a trusteeship model. In part, this evolution was driven by the fear that multilateral control of the Internet—that is, control via a conventional state-led international organization such as the International Telecommunications Union—would throttle the Internet as we know it. The federal government, fearing this multilateral outcome, chose to relinquish its control and double down on multistakeholder regulation. The experience of ICANN is not only important for understanding the present and future of Internet regulation; it is also relevant for broader shifts underway in international law from multilateral processes to multistakeholder processes.

NOTES

This Note frames online misinformation as a symptom of an anticompetitive social media market, one where powerful firms exploit their market power and Section 230 protection to avoid addressing the spread of misinformation on

technology manipulates currently existing media of a person to create a hyper-realistic digital replica manifested as a video, audio clip, chatbot, or hologram. The digital replicas can be programmed to do and say things that their real counterpart has never done or said and are sometimes so incredibly lifelike, it seems as though they are real. Due to the high volume of digital media taken and accumulated during one's lifetime, these digital clones can even be produced post-mortem—in essence, digitally resurrecting someone and putting words in their mouth that they never said while still alive. This technology is distinctly new. Aside from a few state statutes criminalizing certain extreme instances of deepfake technology, any kind of potential remedy against unauthorized digital cloning remains unknown and untested. Many of these potential remedies would require an invasion of privacy or showing of harm. However, courts have consistently held that privacy rights and harm are not retained after death. Even with the few possible remedies that could protect against unauthorized digital cloning, none would protect against unauthorized post-mortem digital cloning. This Note argues that modern estate planning should include a digital legacy clause, dictating how one's digital assets should be used after they die. Legislators should also extend existing probate statutes to require explicit permission from someone, prior to death, to allow for post-mortem digital cloning.

Multistakeholder Regulation and the Future of the Internet

Kal Raustiala*

TABLE OF CONTENTS

* Kal Raustiala is the Promise Institute Distinguished Professor of Comparative and International Law at UCLA Law School and the Director of the UCLA Burkle Center for International Relations.

I. INTRODUCTION

International organizations are a mainstay of contemporary international law. Rare a century ago, today there are thousands of such organizations, ranging from the United Nations to the International Bureau of Weights and Measures.[1] International organizations can be bilateral, such as the International Joint Commission governing the North American Great Lakes, or trilateral, such as the North American Commission on Environmental Cooperation.[2] But the vast majority are multilateral, and often comprise a very large number of parties. Some, such as the International Telecommunications Union, date back to the 19th century.[3] Yet, as a tool of multilateral cooperation, international organizations became especially prominent in the years after the Second World War, when major organizations such as the World Bank, the International Monetary Fund, and the UN were established via multilateral treaties.[4]

There is a vibrant debate among international lawyers and political scientists about why governments create and use international organizations. A central part of this debate concerns the important role of delegation. As Joel Trachtman writes: "the essence of an international organization is the delegation of decision-making authority from individual states to the organization."[5] Delegation is, in a sense, essential to a functioning international organization. States are the primary units of the international legal system, and international organizations are created by states. To perform its functions and achieve its purpose, the powers of an international organization must come from the states who create it. Indeed, a systematic empirical study of international legal agreements found, unsurprisingly, that "delegation is widespread."[6]

---

1. See *Yearbook of International Organizations 2022-2023*, UNION OF INT'L ASSOCS. (2022) (updated annually), for recent data on international organizations. For political, legal, and historical overviews of the growth and role of international organizations, see GLOBAL GOVERNANCE IN A WORLD OF CHANGE (Michael N. Barnett et al. eds., 2021); MICHAEL N. BARNETT & MARTHA FINNEMORE, RULES FOR THE WORLD: INTERNATIONAL ORGANIZATIONS IN GLOBAL POLITICS (2004); JOSÉ E. ALVAREZ, INTERNATIONAL ORGANIZATIONS AS LAW-MAKERS (2006); AKIRA IRIYE, GLOBAL COMMUNITY: THE ROLE OF INTERNATIONAL ORGANIZATIONS IN THE MAKING OF THE CONTEMPORARY WORLD (2002).

2. *History of the IJC*, INT'L JOINT COMM'N, https://www.ijc.org/en/who/history [https://perma.cc/8NRH-9TJV] (last visited June 27, 2022); COMM'N FOR ENV'T COOP., STRATEGIC PLAN 2021-2025: RENEWING OUR TRILATERAL COMMITMENT AND IMPLEMENTING THE NEW FREE TRADE AGREEMENT AND ITS SUPPORTING ENVIRONMENTAL COOPERATION AGREEMENT 4 (2020), http://www.cec.org/files/documents/strategic_plans/cec-strategic-plan-2021-2025.pdf [https://perma.cc/JZ4E-JMJQ].

3. *Discover ITU's History*, ITU, https://www.itu.int/en/history/Pages/DiscoverITUsHistory.aspx [https://perma.cc/W4MG-V9NB].

4. *See generally* Michael Barnett et al. eds., *supra* note 1, at 1-47.

5. Joel P. Trachtman, *The Economic Structure of the Law of International Organizations*, 15 CHI. J. INT'L L. 162, 164 (2014).

6. Barbara Koremenos, *When, What, and Why Do States Choose to Delegate?*, L. & CONTEMP. PROBS., Winter 2008, at 151.

One prominent strand of research on international organizations emphasizes theories of principal-agent relationships in explaining the existing patterns of delegation of law-making and regulatory powers.[7] This approach draws on literature regarding domestic administrative agencies, in which Congress delegates powers to an agency to regulate, say, environmental protection. As applied to the international level, governments (principals) delegate power and authority to international organizations (agents) in order to more effectively cooperate with other states and manage global challenges.

From the perspective of American law, an international delegation "is the transfer of constitutionally assigned federal powers—treaty-making, legislative, executive, and judicial powers—to an international organization."[8] Governments may delegate regulatory authority to international organizations for a number of reasons: to better manage policy externalities; to gain from specialization and expertise; to facilitate collective decision-making; and to enhance policy credibility.[9] At the core of these theories of delegation to international organizations is the notion that principals ultimately control agents. Every act of delegation involves "a contingent grant of authority."[10] Agents may enjoy some degree of discretion, but as a conceptual matter, what defines principals as principals is that they

7. *See generally* Darren G. Hawkins et al., *Delegation Under Anarchy: States, International Organizations, and Principal-Agent Theory*, *in* DELEGATION AND AGENCY IN INTERNATIONAL ORGANIZATIONS 3, 3 (David G. Hawkins et al. eds., 2006); Tana Johnson & Johannes Urpelainen, *International Bureaucrats and the Formation of Intergovernmental Organizations: Institutional Design Discretion Sweetens the Pot*, 68 INT'L ORG. 177 (2014). For a similar application to non-binding legal bodies, *see* Laurence Helfer & Timothy Meyer, *The Evolution of Codification: A Principal-Agent Theory of the International Law Commission's Influence*, *in* CUSTOM'S FUTURE: INTERNATIONAL LAW IN A CHANGING WORLD 305, 305 (Curtis Bradley ed., 2016); Curtis A. Bradley & Judith G. Kelley, *The Concept of International Delegation*, LAW & CONTEMP. PROBS., Winter 2008, at 1; Oona A. Hathaway, *International Delegation and State Sovereignty*, LAW & CONTEMP. PROBS., Winter 2008, at 115; Neal S. Siegel, *International Delegations and the Values of Federalism*, LAW & CONTEMP. PROBS., Winter 2008, at 93; Kenneth W. Abbott et al., *Two Logics of Indirect Governance: Delegation and Orchestration*, 46 BRIT. J. POL. SCI. 719 (2016); Roland Vaubel, *Principal-Agent Problems in International Organizations*, 1 REV. INT'L ORGS. 125, 125-26 (2006); Jon C.W. Pevehouse & Inka von Borzyskowski, *International Organizations in World Politics*, *in* THE OXFORD HANDBOOK OF INTERNATIONAL ORGANIZATIONS 3, 9-10 (Jacob Katz Cogan et al. eds., 2016); Jan Klabbers, *The EJIL Foreword: The Transformation of International Organizations Law*, 26 EUR. J. INT'L L. 9, 24-26 (2015); Koremenos, *supra* note 6.

8. Julian G. Ku, *The Delegation of Federal Power to International Organizations: New Problems with Old Solutions,* 85 MINN. L. REV. 71, 72 (2000); *see generally* Lori Fisler Damrosch, *Sovereignty and International Organizations*, 3 U.C. DAVIS J. INT'L L. & POL'Y 159 (1997).

9. Hawkins et al., *supra* note 7; *see also* Pevehouse & von Borzyskowski, *supra* note 7, at 10; Bradley & Kelley, *supra* note 7.

10. David Lake & Mathew McCubbins, *The Logic of Delegation to International Organizations*, *in* DELEGATION AND AGENCY IN INTERNATIONAL ORGANIZATIONS 341 *passim* (David G. Hawkins et al. eds., 2006).

retain final control over the terms of their delegation to agents.[11] In short, delegation of authority, it is said, is not the abdication of authority.[12]

This Article considers when governments in fact choose abdication over delegation in the international context. To do so, this Article examines an unusual case, one that despite being increasingly prominent has received relatively little attention from scholars of international law and organization: the regulation of key aspects of the Internet. Over the last several decades, the Internet has transformed economic, social, and political life around the globe. The U.S. has played a central role in this process. California is the birthplace of the Internet[13] and home to many of the most powerful technology firms.[14] The federal government has long had an outsized role in both the creation of the Internet and its governance.[15] Originally a Defense Department-funded project known as the Arpanet, for many years the entire Internet resided within the continental U.S.[16] This history gave the federal government enormous control over many aspects of the Internet, including the central issue of the naming and numbering system that ensures the Internet works as a means of communication. The regulation of names and numbers is at the core of Internet governance; for decades the federal government—or its delegates—regulated this key feature.[17]

In 2016, nearly a half century after the Internet's birth, then-President Barack Obama controversially ended the last vestige of formal federal

11. *See generally* D. RODERICK KIEWEIT & MATHEW MCCUBBINS, THE LOGIC OF DELEGATION: CONGRESSIONAL PARTIES AND THE APPROPRIATIONS PROCESS (Benjamin I. Page ed., 1991).

12. *See, e.g.*, *id.* at 3.

13. JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 27 (2008) (describing how the first message sent over the Internet was between two California universities: "The UCLA programmers typed "log" to begin logging in to the Stanford computer. The Stanford computer crashed after the second letter, making "Lo" the first Internet message.").

14. Apple, Google (Alphabet), Facebook (Meta), Intel, Cisco, and many other leading technology firms are all based in Northern California. *See generally* MARGARET O'MARA, THE CODE: SILICON VALLEY AND THE REMAKING OF AMERICA (2019).

15. Adam Segal, *When China Rules the Web: Technology in Service of the State*, FOREIGN AFFS. (Sept./Oct. 2018), https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web [https://perma.cc/LDZ3-HFDA] ("For almost five decades the United States has guided the growth of the Internet.").

16. *See, e.g.*, MILTON L. MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE 74-75 (2004) (providing a broad history of the Internet); *see* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 23 (2006).

17. *See infra* Part II.

government control over the naming and numbering system.[18] As *The Economist* wrote at the time,

> Barring any last-minute hiccups, something remarkable will happen on October 1st. Nearly two decades after it created the Internet Corporation for Assigned Names and Numbers, the body which oversees the internet's address system, America's government will let lapse a contract that gives it control over part of ICANN. This means that a crucial global resource will henceforth be managed by an organisation that is largely independent of national governments.[19]

As *The Economist* predicted, the U.S. successfully ceded its authority over the naming and numbering system that lies at the core of the Internet to the organization known as Internet Corporation for Assigned Names and Numbers ("ICANN").[20] Why did the Obama administration choose to do this? That is the central question this Article addresses. ICANN, a non-profit incorporated under California law, was initially delegated regulatory authority over Internet naming and numbering in 1998.[21] This was structured under a contract with the U.S. Commerce Department, and that contract was periodically renewed, with minor changes, until 2016.[22] President Obama's decision terminated that contractual relationship and freed ICANN to regulate in its traditional areas of Internet governance without any direct federal oversight.[23]

ICANN's distinguishing features are its high level of technocratic expertise and its "multistakeholder" governance model; that is, state actors do not dominate ICANN's governance. ICANN instead employs a complex structure in which both state and private actors jointly play key decision-making roles.[24] The multistakeholder approach reflects the complex history

---

18. *See, e.g.*, L. Gordon Crovitz, *The Battle over Obama's Internet Surrender*, WALL ST. J. (June 13, 2016, 10:08 AM), https://www.wsj.com/articles/the-battle-over-obamas-internet-surrender-1465770111 [https://perma.cc/Z7GA-HB77]; Press Release, Ted Cruz, Senator, Don't Let Obama Give Away the Internet (Aug. 30, 2016), https://www.cruz.senate.gov/?p=press_release&id=2782 [https://perma.cc/2LC3-TY2F]; L.S., *Why Is America Giving up Control of ICANN?*, ECONOMIST (Sept. 30, 2016), https://www.economist.com/the-economist-explains/2016/09/29/why-is-america-giving-up-control-of-icann [https://perma.cc/N6ZE-MYBZ]; Dave Lee, *Has the US Just Given Away the Internet?*, BBC NEWS (Oct. 1, 2016), https://www.bbc.com/news/technology-37527719 [https://perma.cc/3RMK-Q863].

19. L.S., *supra* note 18.

20. *See* Lee, *supra* note 18.

21. *Bylaws for Internet Corporation for Assigned Names and Numbers–A California Nonprofit Public-Benefit Corporation*, ICANN, at Art. 4 [hereinafter *ICANN Bylaws*], https://www.icann.org/resources/pages/governance/bylaws-en/#article2 [https://perma.cc/4HAJ-8FWP] (last amended June 2, 2022).

22. *See generally* ICANN, www.icann.org [https://perma.cc/KP4S-88RQ] (last visited June 27, 2022); Jonathan Weinberg, *ICANN and the Problem of Legitimacy*, 50 DUKE L.J. 187 (2004); Peter K. Yu, *The Origins of ccTLD Policymaking*, 12 CARDOZO J. INT'L & COMPAR. L. 387 (2004).

23. Lee, *supra* note 18.

24. *See generally* ICANN, *supra* note 22.

of the Internet, in which universities and other private actors played key early roles.[25] Many of these private actors have traditionally favored the freedom and openness that has characterized the Internet since its birth.[26] While the mythology of cyberspace as a sovereignty-free zone is highly misleading, it is true that from its origins through the present day many of the actors most engaged with the Internet have preferred a generally light regulatory hand with limited state intervention.[27] ICANN is also not a typical international organization: it is a nonprofit public benefit corporation established under California law.[28]

The initial choice by the federal government to delegate aspects of Internet regulation to ICANN is, as this Article will detail below, readily explained via existing principal-agent theories. ICANN possesses substantial technical expertise; delegating certain regulatory tasks to it made sense both in terms of policy and politics. But why would a government with jurisdiction over a valuable global resource choose to then irrevocably cede control over that resource to a non-state entity? And what significance does this choice of abdication of authority have for theories of international law and global governance generally?

This Article first provides a brief overview of Internet governance.[29] Much of this governance is technical; for example, IP addresses and domain names, such as .edu or .com, must be standardized and uniform to work effectively as a means of communication. Control over these processes, while complex, has important legal and political implications. This Article then describes multistakeholder governance and argues that the decision of the U.S. to grant full control over the naming and numbering, or "IANA," function to ICANN was a deliberate strategy to help ensure that the contemporary Internet did not fall under the sway of multilateral organizations such as the ITU and remained relatively open and free of government control and censorship.

---

25. *See* MUELLER, *supra* note 16, at 74-75.

26. *See id.*

27. *See* ZITTRAIN, *supra* note 13, at 97-99; GOLDSMITH & WU, *supra* note 16, at 23. *See generally* Mark Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925 (2001); Tim Wu, *Cyberspace Sovereignty?–The Internet and the International System*, 10 HARV. J.L. & TECH. 647 (1997); David Johnson & David Post, *Law and Borders–The Rise of Law in Cyberspace*, 48 STAN. L. REV 1367 (1996).

28. *ICANN History Project*, ICANN, https://www.icann.org/history [https://perma.cc/7Q35-M3PR] (last visited June 27, 2022); Paul Rosenzweig, *On the Issue of "Jurisdiction" over ICANN*, LAWFARE (Apr. 8, 2015, 9:56 AM), https://www.lawfareblog.com/issue-jurisdiction-over-icann [https://perma.cc/VT89-748S%5d].

29. Internet governance has many characteristics of what social scientists term a "regime complex." *See* JOSEPH S. NYE, JR., GLOB. COMM'N OF INTERNET GOVERNANCE, THE REGIME COMPLEX FOR MANAGING CYBER ACTIVITIES 7 (2014), https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf [https://perma.cc/8W28-VWKB%5d]; Kal Raustiala & David G. Victor, *The Regime Complex for Plant Genetic Resources*, 58 INT'L ORG. 277, 277 (2004) (introducing the original concept of regime complex). Because ICANN's governance role is critical and receives a significant amount of political attention, I focus on it here.

This struggle between multilateralism and multistakeholderism has long historical roots. From the Internet's initial boom in the 1990s, it grew increasingly dominated by private firms and commercial interests, a shift the U.S. supported. Yet, the Internet also grew far more global in the 2000s.[30] There were soon increasingly insistent efforts to assert multilateral control over Internet governance as more governments began to appreciate the new technology's economic, social, and political impacts.[31] This push for multilateralism was at odds with the multistakeholder traditions of the Internet. Faced with growing global efforts to multilateralize Internet governance, often led by authoritarian governments, the U.S. chose instead to devolve power to a body in which governments by design had only a limited role and private actors a large voice. In short, the Obama administration's decision favored *multistakeholder* governance over *multilateral* governance.

This Article considers this decision through the lens of principal-agent theory and argues that U.S. strategy toward the Internet was designed to better entrench long-term American interests. But it was a strategy more consistent with concepts of trusteeship than with conventional principal-agent theory.[32] ICANN today is more like a trustee—a body deliberately granted independent authority to use professional judgment—than an agent under the control of a principal.

The decision to cede authority to ICANN muted pressures to multilateralize Internet governance by removing the hand of the federal government from direct control. ICANN was a trusted organization that would, in the American view, preserve the fundamental values of the Internet. A more open, multistakeholder Internet also benefited American firms and American actors, who tended to dominate the digital space, especially as Google, Facebook, Amazon, and others grew enormously powerful around the world. In short, and paradoxically, by ceding *power* the U.S. better preserved its *preferences*.

Part I of this Article introduces the foundational issues. Part II offers a brief history of the Internet and ICANN to ground the inquiry and explores theories of international organization and multistakeholder governance. Part III explains the threat posed by multilateral governance of the Internet. Part

30. *See* Max Roser et al., *Internet*, OUR WORLD IN DATA (2015), https://ourworldindata.org/internet [https://perma.cc/SP39-QRGM].

31. *See generally* Wu, *supra* note 27.

32. Karen Alter, *Agents or Trustees? International Courts in Their Political Context*, 14 EUR. J. INT'L RELS. 33, 35 (2008) (explaining the broad concept of trusteeship, one common in international law); *see, e.g.,* Jeremy Waldron, *Are Sovereigns Entitled to the Benefit of the International Rule of Law?*, 22 EUR. J. INT'L L. 315, 325 (2011) ("[S]tates are recognized . . . as trustees for the people committed to their care."); *see also* Eyal Benvenisti, *Sovereigns as Trustees of Humanity: On the Accountability of States to Foreign Stakeholders*, 107 AM. J. INT'L L. 295, 308 (2013). Madison in *The Federalist Papers* likewise noted that "the federal and State governments are in fact but different agents and trustees of the people." THE FEDERALIST NO. 46 (James Madison). In the law of trusts, conventional legal definitions focus much more narrowly on property entrusted to a trustee. *See, e.g.*, Robert H. Sitkoff, *Fiduciary Principles in Trust Law*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW 41, 41 (Evan J. Criddle et al. eds., 2019) ("A trust . . . is a fiduciary relationship with respect to property . . . subjecting the [trustee] to duties to deal with it for the benefit of charity of one or more persons." (quoting RESTATEMENT (THIRD) OF TRUSTS § 2 (AM. L. INST. 2003))).

IV explains the decision to relinquish authority over the IANA function through theories of delegation and theories of trusteeship and explores the implications for multistakeholder governance in international law more broadly. Part V concludes.

II. THE RISE OF THE INTERNET

A. A Brief History of the Internet

The Internet began during the Cold War as an effort by the federal government to link together a few mainframe computers. Initiated by the [Defense] Advanced Research Projects Agency ("ARPA" or "DARPA"), a then-newly created arm of the Department of Defense ("DoD"), this was the genesis of the original "Arpanet."[33] The first Arpanet communication was sent on October 29, 1969, from UCLA to Stanford University.[34] That history is significant because virtually every major aspect of the next fifty years of the Internet is linked to the U.S., and indeed ICANN, and many of the top technology firms, are still today headquartered in California.

The early Internet was tiny and dominated by a small tribe of computer scientists and engineers, many based at American universities. As computing technology expanded rapidly, however, so too did the reach of the DARPA/Internet.[35] In 1972, email was first developed, and the Internet's utility as a communications platform came into sharper focus.[36] The DoD had the Arpanet but also, later, the Military Network ("MILNET").[37] As this suggests, the practice for much of the 1970s and 1980s was not a single comprehensive network, but instead a series of distinct, purposive networks that comprised like-minded users. Nearly all such users were at large institutions, often universities and research labs, since the personal computer, such as the Apple 1, was only first developed in the mid-1970s.

The National Science Foundation's ("NSF") 1985 network program ("NSFNET") was the first to explicitly endeavor to link the entire academic community in a single network.[38] DARPA and NSF ensured that their respective networks were interoperable.[39] The Internet as we now know it was beginning to form, and the complexities of governance were growing.[40] Politics, property rights, and commercialization were not high priorities in this era. Governance was informal and, until it became apparent that website

33. Mitch Waldrop, *DARPA and the Internet Revolution*, *in* DEF. ADVANCED RSCH. PROJECTS AGENCY, DARPA: 50 YEARS OF BRIDGING THE GAP 78, 78 (2008).

34. ZITTRAIN, *supra* note 13, at 27.

35. See MUELLER, supra note 16, at 74-75.

36. BARRY LEINER ET AL., INTERNET SOC'Y, BRIEF HISTORY OF THE INTERNET 4 (1997), https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf [https://perma.cc/PPN2-QR9B].

37. *Id.*

38. *Id.*

39. *Id.*

40. The ARPANET itself was decommissioned in 1990. ROBERT E. KAHN & VINTON G. CERF, INTERNET POL'Y INST., WHAT IS THE INTERNET (AND WHAT MAKES IT WORK) 9 (1999), http://www.policyscience.net/cerf.pdf [https://perma.cc/9P5X-5UHX].

names (e.g., "amazon.com") had real value, relatively uncontested. The primary focus of Internet governance was on developing interoperable technical standards that allowed for larger communication networks and choosing among competing visions for solutions to technical problems. In short, technical people largely treated Internet governance as a technical problem.

The Internet, however, was rapidly outgrowing this technically-minded community. In the early 1990s, the U.S. created the Federal Networking Council to better coordinate its Internet activities.[41] In the same period, the non-governmental Internet Engineering Task Force, founded in 1986, and the Internet Society, founded in 1992, emerged.[42] These new bodies reflected the growing value of the Internet, as competing interests organized and jockeyed for position and power. (The locus of activity, however, remained largely in the United States.)[43]

Still, the Internet retained a surprisingly small-town feel for a long time. Indeed, until the late 1990s, the work of awarding domain names and IP addresses—what is known as the IANA function, for "Internet Assigned Numbers Authority"—was largely handled by one person: Jon Postel, a computer scientist first based at UCLA and then later at USC.[44] Postel was so central to the Internet's early functioning that *The Economist* declared in 1997 that if "the Net does have a god, he is probably Jon Postel."[45] The IANA function is critical because it is what ensures that the Internet actually works as intended; that when you type in www.google.com your browser actually goes to Google's site. It is also what allows us to type in "google" rather than a string of numbers. Domain names have an important communications function but also a political aspect. Powerful governments have interests in promoting, or suppressing, certain domain names. To see this, consider the political implications of .crimea, .catalonia, or even .xxx.

Internet growth exploded during the 1990s. This was the period in which the World Wide Web was invented, which, coupled to the home computer revolution, made the Internet accessible to ordinary people.[46] In 1994, *Today Show* host Bryant Gumbel could ask on live television, "what is the Internet, anyway?"[47] (After debating the meaning of the @ symbol, he asked "what, do you write to it like mail?" An offscreen producer offered up:

---

41. Barry M. Leiner et al., *Introduction* to BRIEF HISTORY OF THE INTERNET, *supra* note 36, at 2.

42. *Introduction to the IETF*, INTERNET ENG'G TASK FORCE, https://www.ietf.org/about/introduction/ [https://perma.cc/587T-DM7N] (last visited Nov. 12, 2022); *Our History*, INTERNET SOC'Y, https://www.internetsociety.org/history/ [https://perma.cc/4Y72-8KWX] (last visited Nov. 12, 2022).

43. *See* Leiner et al., *supra* note 41, at 2.

44. U.S. GOV'T ACCOUNTABILITY OFF., OGC-00-33R, DEPARTMENT OF COMMERCE: RELATIONSHIP WITH THE INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS 3 (2000), http://www.gao.gov/assets/90/89949.pdf [https://perma.cc/6E3P-FLXR].

45. *Postel Disputes*, ECONOMIST, Feb. 8, 1997, at 116.

46. *A Short History of the Web,* CERN, https://home.cern/science/computing/birth-web/short-history-web [https://perma.cc/JY9W-7T95].

47. The Today Show, *What Is the Internet, Anyway?*, YOUTUBE (Jan. 28, 2015), https://www.youtube.com/watch?v=UlJku_CSyNg [https://perma.cc/G3MM-EL6P].

"Internet is the massive computer network—the one that's becoming really big now.")[48] In the years that followed, millions of Americans (and increasing numbers of non-Americans) obtained email addresses and dial-up modems.[49] By 2000, the first big dot com crash had occurred and nearly every American had heard of the Internet.[50] In short, in the late 1990s the Internet as we know it was born. And as the public began to merge en masse onto the information superhighway, so too did commercial actors. This began a critical change in the politics of the Internet—one reflective of the federal government's policy preferences. As two key players recounted:

> For a long time, the federal government did not allow organizations to connect to the Internet to carry out commercial activities . . . . [but eventually] Congress passed legislation allowing NSF to open the NSFNET to commercial usage. Shortly thereafter, NSF determined that its support for NSFNET might not be required in the longer term and, in April 1995, NSF ceased its support for the NSFNET. By that time, many commercial networks were in operation and provided alternatives to NSFNET for national level network services.[51]

The Internet's character transformed in this era; in simple terms, from science to commerce and from specialists to the general public. The Clinton Administration supported this change, increasingly viewing the Internet as a new and valuable economic resource.[52] But this raised novel challenges. As more commercial actors moved online, for instance, it became clear that website names could be a valuable form of property. Myriad ownership disputes ensued. These "included not only questions of who owned a given domain name, but also—and most importantly—who controlled the right to award names."[53] In other words, the IANA function began to seem like a critical economic and legal regulator and a growing source of valuable property rights.

Yet the Internet had evolved organically, with little thought that it could become largely commercial and implicate fundamental concepts of property. As a result, basic questions of ownership were unclear. Indeed, in response to a 1995 Internet Society proposal to revamp the domain name process, a U.S. official asked, "Is [the Internet Society] claiming that it has jurisdiction and overall responsibility for the top-level address and name space? If yes, how did [it] obtain this responsibility; *if no, then who does own it*?"[54]

---

48. *See id.*
49. Roser et al., *supra* note 30.
50. *See generally* JOHN CASSIDY, DOT.CON: THE GREATEST STORY EVER SOLD (2002).
51. KAHN & CERF, *supra* note 40, at 10.
52. *See, e.g.*, Ira Magaziner, *Creating a Framework for Global Electronic Commerce*, 6 FUTURE INSIGHTS no. 1, July 1999.
53. Kal Raustiala, *Governing the Internet*, 110 AM. J. INT'L L. 491, 492 (2016). For brevity, I leave out the role of Network Solutions, LLC.
54. MUELLER, *supra* note 16, at 136 (emphasis added).

That U.S. officials could ask these basic questions in the 1990s underscored how novel a resource the Internet was. In 1995, NSF called a conference to try to clarify ownership and control.[55] The assembled stakeholders had wildly divergent views. The Pentagon, however, made clear its view: DoD had funded the creation of the Arpanet and still funded the work of Jon Postel; therefore DoD owned the IANA function.[56] Indeed, U.S. officials in this period, concerned to keep control, warned that "any attempt to manipulate the root without the U.S. government's permission would be prosecuted as a criminal offense."[57] (The "root" is, in essence, the top-level domain name system.) Underlying all these claims "was a belief that, in the end, the United States government and no one else possessed ultimate authority over the Internet's deep structure, including naming and numbering authority."[58]

Yet, what was the basis of this asserted authority? Though plainly a funder and progenitor of the early Internet, the federal government did not appear to possess legal title over the Internet. Much of the infrastructure was private—and increasingly global.[59] This uncertain legal foundation became even more significant later, as the Internet became a central focus of many governments around the globe.

Still, the federal government in the 1990s acted as if it possessed ownership and control, and this made some sense. The Internet began as a DARPA project; much of it was administered from California; key firms were nearly all American; and many of the root servers were physically based in the U.S.[60] The U.S.' "position at the center of the global Internet brought it major economic, military, and intelligence benefits."[61] But the claim to "own" the Internet was not actually well-grounded. Too many private actors, universities, and other non-state entities owned or controlled the hardware, software, and other components that the Internet comprised. Moreover, in this period, the tension between the appearance of American control and the reality that the Internet was increasingly global became more acute. Consequently, for the U.S. to act as the *primus inter pares* with regard to other states was unlikely to be accepted for long—not least because other governments' preferences over the kind of Internet they wanted were beginning to diverge, often radically, from those of the U.S. and its chief allies. Governing the Internet was no longer just the domain of engineers and technicians but, increasingly, was imbued with deep political overtones.

In short, by the end of the 1990s, the contemporary Internet—mass use, largely for personal and commercial purposes, and global—had supplanted the early research-based networks of the past. The Internet's increasingly private orientation was no accident: as political scientists Jonathan Aronson

55. *See generally id.*
56. *See generally id.*
57. *Id.* at 162.
58. GOLDSMITH & WU, *supra* note 16, at 41.
59. ZITTRAIN, *supra* note 13, at 27.
60. *Root Servers*, IANA, https://www.iana.org/domains/root/servers [https://perma.cc/UCS3-LEQU] (last visited Oct. 31, 2022).
61. Segal, *supra* note 15.

and Peter Cowhey argued, "the Internet's ultimate commercial triumph was . . . a product of the specific political economy context of the United States government."[62] The Internet grew rapidly in this new guise. Indeed, by 1999 there were roughly 200 million users—a huge change from a decade earlier, but a number soon to be an order of magnitude higher.[63] In this new world, novel regulatory and legal approaches were required.

B. International Organizations and Multistakeholder Global Governance

International organizations are today central to international law. Writing some two decades ago, Julian Ku argued that "the new international law has been developed in large part by the rise of a new legal creature: the international organization. These organizations have varying levels of authority, ranging from technical administrative coordination to regulation of political interaction among states."[64] While international organizations date to the 19th century, the rise of these organizations as key features of the international legal system began with the end of the Second World War and accelerated thereafter.[65] In the seventy-five years since the war ended, international organizations have proliferated, ranging from the United Nations and the World Bank to the Asian Infrastructure Investment Bank and the League of Arab States.[66] Indeed, "in the early 21st century, it is difficult to think of international law and the governance of international affairs in isolation from international organizations."[67]

Central to the study of international organizations is why they exist and what specific functions they serve. Joel Trachtman, for example, has asked "why are formal international organizations created, and why is formal legal power delegated from states to international organizations?"[68] Andrew Guzman argues that "States create [international organizations] with the hope of enhancing international cooperation beyond what can be achieved by states alone."[69] This argument—that international organizations are created and delegated power by states in order to facilitate and further cooperation—is common to both the international law and international relations traditions.[70]

Jose Alvarez defines international organizations as organizations established by agreements between states, having at least one organ capable

62. PETER F. COWHEY & JONATHAN D. ARONSON, TRANSFORMING GLOBAL INFORMATION AND COMMUNICATION MARKETS: THE POLITICAL ECONOMY OF INNOVATION 209 (2009).

63. Roser et al., *supra* note 30.

64. Ku, *supra* note 8, at 83.

65. *See* Barnett et al. eds., *supra* note 1, at 1.

66. *See* Mark Copelovitch & Jon C.W. Pevehouse, *International Organizations in a New Era of Populist Nationalism*, 14 REV. INT'L ORGS. 169, 170 (2019); *see generally* ALVAREZ, *supra* note 1 (providing history).

67. Klabbers, *supra* note 7, at 15.

68. Trachtman, *supra* note 5, at 172.

69. Andrew Guzman, *International Organizations and the Frankenstein Problem*, 24 EUR. J. INT'L L. 999, 1000 (2013).

70. *See, e.g.*, Pevehouse & von Borzyskowski, *supra* note 7, at 7*;* Klabbers, *supra* note 7, at 17-18.

of operating separately from member states, and operating under international law.[71] By this definition, ICANN is not a classic international organization; indeed under the traditional terms of international law, it is not an international organization at all but rather a non-profit corporation created pursuant to U.S. domestic law.[72] This legal status has been at times controversial and the subject of debate over whether ICANN's location should be altered.[73] Yet, ICANN's role and structure are similar to many features of international organizations: it has many states as members; it regulates a global resource of shared interest to many nations; and it holds regular conferences and meetings around the globe. As one scholar of ICANN notes, while ICANN is not technically an international organization, "it is international in the sense that its Articles of Incorporation and Bylaws mandate cooperation with organizations and persons in many countries as well as governments."[74] For these reasons, many of the arguments about the role of delegation to international organizations can be fruitfully applied to ICANN.

ICANN's signature feature is its multistakeholder structure. Multistakeholderism is not unique to the governance of the Internet.[75] But neither is it widely used in international law. Multistakeholder governance has been defined by Mark Raymond and Laura DeNardis "as two or more classes of actors engaged in a common governance enterprise concerning issues they regard as public in nature, and characterized by polyarchic authority relations constituted by procedural rules."[76] In simple terms, it

71. ALVAREZ, *supra* note 1, at 1.

72. *Amended and Restated Articles of Incorporation of Internet Corporation for Assigned Names and Numbers*, ICANN (Oct. 3, 2016), https://www.icann.org/resources/pages/governance/articles-en [https://perma.cc/S8FS-PNZP]; *Getting to Know the Internet Corporation for Assigned Names and Numbers (ICANN)*, ICANN, https://www.icann.org/en/system/files/files/quick-look-icann-01nov13-en.pdf [https://perma.cc/D3FF-AB48] (last visited June 6, 2022).

73. *See, e.g.*, Milton Mueller, *What "Jurisdiction" Does ICANN Belong To?*, INTERNET GOVERNANCE PROJECT (Nov. 7, 2017), https://www.internetgovernance.org/2017/11/07/jurisdiction-icann-belong/ [https://perma.cc/FE2M-33V4]; ICANN, CCWG-ACCOUNTABILITY WS2 JURISDICTION SUBGROUP DRAFT RECOMMENDATIONS OCTOBER 2017 (2017), https://community.icann.org/display/WEIA/Jurisdiction?preview=/59643282/71602752/CCWG-Accountability-WS2-Jurisdiction-Report%20to%20Plenary%20v1.0.docx [https://perma.cc/LS4B-4XDA].

74. Emily M. Weitzenboeck, *Hybrid Net: The Regulatory Framework of ICANN and the DNS*, 22 INT'L J.L. & INFO. TECH. 49, 50 (2014).

75. For example, COVAX is a multistakeholder group established to be the vaccine distribution arm of another multistakeholder body called the Access to Covid-19 Tools Accelerator (ACT). *See* HARRIS GLECKMAN, TRANSNAT'L INST. & FRIENDS OF THE EARTH INT'L, COVAX: A GLOBAL MULTISTAKEHOLDER GROUP THAT POSES POLITICAL AND HEALTH RISKS TO DEVELOPING COUNTRIES AND MULTILATERALISM (Gonzalo Berrón & Letícia Paranhos M. de Oliveira eds., 2021), https://longreads.tni.org/wp-content/uploads/2021/03/COVAX_EN_WEB_NEW.pdf [https://perma.cc/5PST-7HJ4].

76. Mark Raymond & Laura DeNardis, *Multistakeholderism: Anatomy of an Inchoate Global Institution*, 7 INT'L THEORY 21, at 572-73 (2015); *see also* PETER F. COWHEY & JONATHAN D. ARONSON, DIGITAL DNA: DISRUPTION AND THE CHALLENGES FOR GLOBAL GOVERNANCE (2017); Joe Waz & Phil Weiser, *Internet Governance: The Role of Multistakeholder Organizations*, 10 J. TELECOMM. TECH. L. 331 (2012).

means lawmaking via a mix of government actors, firms, interested non-governmental organizations, indigenous peoples, and even individuals. The core idea is for all the relevant stakeholders in a given issue-area to have a say and a role, even if some may have greater power or play different regulatory roles than others. Multistakeholder approaches vary in scale, scope, and approach but can be found in global health (e.g., The Global Fund to Fight AIDS, Malaria, and Tuberculosis[77]); the UNAIDS program;[78] sustainable development;[79] and even small arms regulation.[80] Aronson and Cowhey argue that multistakeholder governance is particularly useful for international cooperation to regulate technology, where private sector expertise is high and technical knowledge important.[81]

The line between inclusive forms of multilateral cooperation and full multistakeholder cooperation can be blurry. The key dimension is the character of state power: whether governments are ultimately in control (multilateral) or whether nonstate actors share power in broadly equal ways (multistakeholder). For example, many multilateral treaties within the international legal system have moved to include greater numbers of non-state actors.[82] The International Telecommunications Union, for example, has 193 member governments and some 900 non-voting "sector members" drawn from academia, industry, and the like.[83] Within the United Nations, NGOs can obtain consultative status through the Economic and Social Council that allows them access to many meetings, treaty processes, and the like.[84] Still, however active non-state actors may be in multilateral settings, governments remain in control of these processes and often meter participation by nonstate

77. THE GLOBAL FUND, COUNTRY COORDINATING MECHANISMS: GOVERNANCE AND CIVIL SOCIETY PARTICIPATION (2008), https://web.archive.org/web/20220414133731/https://www.theglobalfund.org/media/5472/ccm_2008thematiccivilsocietyparticipation_report_en.pdf [https://perma.cc/EXQ2-46Z9].

78. *About: Governance*, UNAIDS, https://www.unaids.org/en/whoweare/governance [https://perma.cc/NWY6-7TM6] (last visited June 24, 2022).

79. *See generally* Karin Bäckstrand, *Multi-Stakeholder Partnerships for Sustainable Development: Rethinking Legitimacy, Accountability and Effectiveness*, 16 EUR. ENV'T 290, (2006); MINU HEMMATI, MULTI-STAKEHOLDER PROCESSES FOR GOVERNANCE AND SUSTAINABILITY: BEYOND DEADLOCK AND CONFLICT (2002).

80. *See generally* Deborah Avant, *Netting the Empire: US Roles Governing Small Arms and Military and Security Services*, *in* THE NEW POWER POLITICS: NETWORKS AND TRANSNATIONAL SECURITY GOVERNANCE 103 (Deborah Avant & Oliver Westerwinter eds., 2016).

81. COWHEY & ARONSON, *supra* note 62, at 2.

82. *See generally,* JONAS TALLBERG ET AL., THE OPENING UP OF INTERNATIONAL ORGANIZATIONS: TRANSNATIONAL ACCESS IN GLOBAL GOVERNANCE (2013).

83. *About International Telecommunication Union (ITU),* ITU, https://www.itu.int/en/about/Pages/default.aspx [https://perma.cc/ZQ6E-X4ZD] (last visited June 24, 2022).

84. U.N. Charter art. 71; *see also Consultative Status with ECOSOC and Other Accreditations*, U.N. DEP'T OF ECON. & SOC. AFFS., NGO BRANCH, https://esango.un.org/civilsociety/displayConsultativeStatusSearch.do?method=search&sessionCheck=false [https://perma.cc/TCZ3-65AS] (last visited Dec. 20, 2022).

actors as they see fit.[85] Multistakeholder governance systems, by contrast, do not give any one group control or the power to exclude.

ICANN's governance structure deeply reflects multistakeholder principles. It has a government advisory council composed of state representatives.[86] Yet governments have no veto powers over ICANN generally and cannot control or direct decisions even if they can find consensus on a particular position.[87] Indeed, the government advisory council is just one of several councils representing stakeholder groups, each of which feeds input up to the ICANN board of directors, the ultimate decisionmaker.[88] This system reflects the long history of non-state actors in the informal governance processes of the past, but also the desire on the part of many interested parties to ensure that governments do not seize control of a system that has long been marked by an ethos of openness and freedom

To be sure, multistakeholder governance has a buzzy quality today. As Raymond and DeNardis rightly note, "Actors seem eager both to talk about engaging in multistakeholderism and to engage in it—whether by speaking about it or in other ways."[89] The use of the term "multistakeholder" is itself relatively novel. Based on Google Ngram data, in English the term first appears in the 1970s—about the same time the Internet was effectively launched.[90] By 1988 multistakeholder was used in .0000000460% of sources.[91] Twenty years later usage had increased 10,000%.[92] "Multilateral" exhibits a quite different pattern. Common even in the 1940s, by the 1970s—multistakeholder first appears in the Ngram search in 1976—for every one use of multistakeholder, multilateral was used 107,000 times.[93] Three decades later the situation was markedly different; there were now only eighty usages of multilateral for each mention of multistakeholder.[94] To provide context, consider the term "global governance." As the graph below shows, it is (unsurprisingly) used far more frequently than "multistakeholder" but also shows a marked upward shift starting in the 1990s.

85. Kal Raustiala, *The Role of NGOs in Treaty-Making*, *in* THE OXFORD GUIDE TO TREATIES 173, 192 (Duncan Hollis ed., 2012); Kal Raustiala, *States, NGOs, and International Environmental Institutions*, 41 INT'L STUD. Q. 719, 720 (1997).

86. *ICANN Bylaws*, *supra* note 21, at Art. 4.

87. *Bylaws for Internet Corporation for Assigned Names and Numbers*, ICANN (last amended June 2, 2022), https://www.icann.org/resources/pages/governance/bylaws-en [https://perma.cc/ZHK4-ZH7E].

88. *Getting to Know the ICANN Board of Directors*, ICANN, https://www.icann.org/resources/pages/chart-2012-02-11-en [https://perma.cc/468U-L7PL] (last visited Dec. 20, 2022).

89. Raymond & DeNardis, *supra* note 76, at 21.

90. *Infra* Figure 1.

91. *Id.*

92. *Id.*

93. *Id.*

94. *Id.*

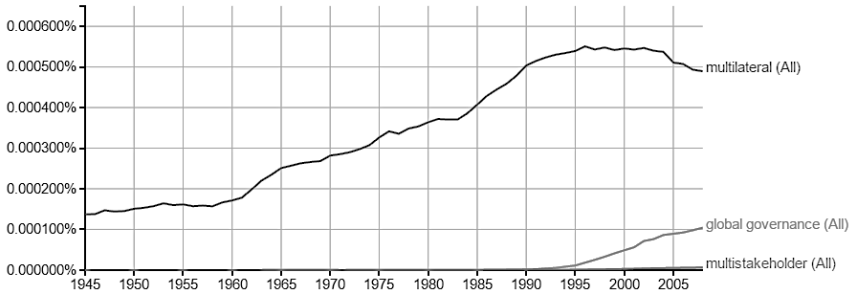

Figure 1. Changes in Nomenclature Over Time

It is hard to draw precise inferences from this data. The relationship between discussions of multistakeholder governance and its actual political significance is uncertain. But it is clear that the way actors talk about global governance has changed, plausibly reflecting some combination of legitimacy concerns and shifting ideas about effective governance. Terms like "stakeholder" and "governance" are inclusive, process-oriented, and seem to elide the role of power. "Multistakeholder governance" is friendly, open, and maybe messy; "multilateral negotiations" have a harder, more competitive edge. This dynamic characterizes the regulation of the Internet, where insiders have long been proponents of multistakeholderism and quite wary of multilateralism. But whatever the rhetorical implications, the appeal of multistakeholderism to the U.S government was largely grounded in more concrete concerns.

III. THE POLITICS OF INTERNET GOVERNANCE

A. The Threat of Multilateralism

The Internet rapidly expanded across the world in the 1990s. As it did, the notion that such a significant global resource would be subject to control by a single state, especially a state that was widely viewed in this era as not just a superpower but a "hyperpower," struck many other governments as increasingly problematic.[95] This led to various efforts to assert multilateral control—many of which emanated from agencies of the UN. Most notable was the International Telecommunications Union. Founded in 1865, and a United Nations specialized agency since 1947, the ITU has long had a central role in global communications law and policy.[96] Because the ITU operates on a one-nation one-vote system, and because so many governments in the world prefer to control communication extensively, the organization has often been at odds with liberal democracies.

The ITU saw the Internet as a logical extension of its traditional ambit over communication. And the ITU was critical of what it believed was the

95. SAMANTHA BRADSHAW ET AL., GLOB. COMM'N OF INTERNET GOVERNANCE, THE EMERGENCE OF CONTENTION IN GLOBAL INTERNET GOVERNANCE 10 (2015).

96. Peter F. Cowhey, *The International Telecommunications Regime: The Political Roots of Regimes for High Technology*, 44 INT'L ORG. 169, 169 (1990).

Internet's informal approach to regulation.[97] But as Milton Mueller explains in his authoritative history of the Internet:

> A deeper agenda underlay the ITU's interest in domain name issues. As the intergovernmental organization that had presided for decades over a regime of state-owned telephone monopolies, the ITU was uncertain of its role and status in a new, liberalized order. With the Internet on the rise, private-sector-led standards forums proliferating, and the days of traditional, circuit-switched telephone service seemingly numbered, the ITU needed to assert a role for itself in internet governance . . . . The governance debates presented it with an opportunity to establish itself as an actor in that arena.[98]

There were strong pressures within the ITU to both assert authority over its putative regulatory domain and to ensure that ITU member governments retained (or reasserted) maximal state control over national telecommunications markets. While telecommunications firms had often been nationalized, the Internet had created a new communications ecosystem. The leading digital firms were American. Many governments saw the potential for political disruption in the Internet, but also for greater American control of communication both globally and locally. Neither was appealing. In short, the communications revolution wrought by the Internet had deep political as well as economic ramifications. Multilateral control via the ITU provided an attractive way to rein in the Internet—and American power over it.

On the other side was the informal multistakeholder tradition that had in practice, and without much in the way of explicit decision, managed the Internet since its birth. Proponents of multistakeholderism believed knowledgeable parties, generally understood as engineers and other insiders, should govern the Internet collectively. And rather than formal rules and procedures, they preferred inclusive deliberation and rough consensus. While these loose methods had worked acceptably well in the past, the Internet had, by the mid-1990s, long since become a different and far more global and diverse entity. In 1996 a group of non-state actors—including the Internet Society, the World Intellectual Property Organization (WIPO), and the ITU—tried to create an encompassing framework that would rationalize governance of the Internet. These various groups negotiated an international agreement on "generic Top Level Domains," such as .com or .edu. The agreement was known as the "gTLD-Memorandum of Understanding."[99]

As Daniel Drezner has argued, the gTLD accord "proposed assigning governance functions to an entity housed in the ITU."[100] Though legally non-

97. *See* Pekka Tarjanne, ITU Sec'y-Gen., ITU, Keynote Address on Internet Governance: Towards Voluntary Multilateralism (Apr. 29, 1997).

98. MUELLER, *supra* note 16, at 138.

99. Tarjanne, *supra* note 97.

100. Daniel Drezner, *The Global Governance of the Internet: Bringing the State Back In*, 119 POL. SCI. Q. 477, 494 (2003).

binding, the ITU "arranged a 'formal' signing ceremony in Geneva in March 1997 to give the agreement the trappings of an international treaty."[101] At the signing ceremony, the ITU Secretary-General hailed the accord, stating that the current Internet:

> . . . is too dependent on the goodwill of a small group of people who are doing the job largely by historical accident, because they were in the right place at the right time; the most popular gTLDs are handled by an organization which holds a monopoly over the registration and award of those domain name . . . . *The current system is dominated by actors in just one country, the United States, to the exclusion of others*; It does not give adequate attention to the protection of trademarks and other intellectual property; It lacks formal structure and legitimization.[102]

The ITU effort came as an unhappy surprise to the United States. Then-Secretary of State Madeline Albright blasted the ITU "for acting 'without authorization of member governments' to hold a 'global meeting involving an unauthorized expenditure of resources and concluding with a quote international agreement unquote.'"[103]

The ITU's effort nonetheless signaled an important step in the global regulation of the Internet. Rival governments and multilateral organizations were jockeying for position and seeking greater control. The U.S. understood that attempts at greater multilateral regulation were not blips but instead an ongoing—and likely growing—threat to an open Internet. Moreover, this threat was rising just as the Internet was becoming more commercial in nature. For the Clinton Administration, it appeared the bright future of the Internet as a social and economic platform could be squelched by these moves toward greater multilateral governance.

The U.S. thus faced a crucial choice: It could accede to the growing global demands for multilateralism , or it could embrace even more firmly the existing tradition of multistakeholderism—which, not coincidentally, was dominated by American actors. The choice was easy. As a White House official stated at the time: "As the Internet grows up and becomes more international, these technical management questions should be privatized, and there should be a *stakeholder-based, private international organization* set up for that technical management."[104] What the U.S. sought to create, in sum, was a more formalized version of the existing system of multistakeholderism.

Less than four months after the ITU's attempt to gain greater control of key aspects of Internet governance, President Clinton directed the Commerce Department to spin off the management of the naming and numbering

---

101. *Id.*

102. Tarjanne, *supra* note 97 (emphasis added).

103. Milton Mueller, *ICANN and Internet Governance: Sorting Through the Debris of "Self-Regulation"*, 1 INFO 497, 502 n.17 (1999) (quoting Memorandum from the Madeleine Albright, U.S. Sec'y of State, to the ITU (April 23, 1997)).

104. Magaziner, *supra* note 52 (emphasis added).

system.[105] The federal White Paper on the proposal noted that the Internet had become far more commercial: "as Internet names increasingly have commercial value, the decision to add new top-level domains cannot be made on an ad hoc basis by entities or individuals that are not formally accountable to the Internet community."[106] Most significantly, however, the White Paper expressly rejected multilateralism as an appropriate form of governance:

> While IOs may provide specific expertise or act as advisors to the new corporation, the U.S. continues to believe, as do most commenters, that *neither national governments acting as sovereigns nor intergovernmental organizations acting as representatives of governments should participate in management of Internet names and addresses*.[107]

B. The Creation of ICANN

After a call for proposals issued by the U.S. Commerce Department, in 1998, ICANN was selected, created, and finally delegated authority over the naming and numbering system.[108] ICANN is an unusual hybrid of non-governmental organization and an international organization. There is no treaty creating it, it enjoys no host agreement with the US (as does, for instance, the United Nations), and its staff lacks diplomatic immunities. It is legally a 501(c)(3) organization, incorporated under California law[109]. Still, ICANN has many features of an international organization. It governs a global resource, generates new rules and policies, has governments as members, and has an international ambit.

ICANN initially operated pursuant to a contract issued by the U.S. Department of Commerce.[110] This contract directly delegated to ICANN the ability to generate and assign new top-level domain names and the power to designate who adjudicates disputes over website names.[111] This latter power reflected the increasing value of domain names and websites, both in their own right and as they relate to trademarks and other forms of intellectual

105. *See generally* Management of Internet Names and Addresses, 63 Fed. Reg. 31741 (June 10, 1998).

106. NTIA, *Statement of Policy on the Management of Internet Names and Addresses*, Dkt. No. 980212036-8146-02 (June 5, 1998), https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses [https://perma.cc/P6L7-NF45].

107. *Id.* (emphasis added).

108. *ICANN History Project*, *supra* note 28.

109. *See generally* Waldrop, *supra* note 33.

110. NTIA, *Contract Between the U.S. Dep't of Commerce and ICANN*, Cont. No. SA1301-12-CN-0035 (Oct. 1, 2012), https://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf [https://perma.cc/8JT8-CCRB].

111. *See id.*

property.[112] The legal basis of the relationship between ICANN and the U.S. government rested on three agreements: *The Memorandum of Understanding Between the US Department of Commerce and [ICANN]*, ICANN's *Cooperative Research and Development Agreement*, and a contract governing the naming and numbering function and assignment of IP numbers.[113]

As explained above, ICANN has a highly-articulated system of multistakeholder governance, in which non-state actors are numerous and policy proposals are open for public comment. ICANN's governance structure does not mean that governments lack any control over the Internet—as many governments around the world have demonstrated. ICANN's powers are limited. But while access to websites can be blocked within certain states, as China does with the so-called "Great Firewall," and India did recently with regard to Kashmir, without "control over the global assigning of names and numbers, comprehensive censorship of the Internet as a whole is inhibited."[114] What occurs elsewhere on the Internet can still have powerful effects, and technical workarounds, from virtual private networks to satellite-based systems, offer entry points from the larger world that are difficult to block. This gives ICANN an important degree of power that makes it a source of irritation for some governments and continues to spur efforts to shift regulatory authority to multilateral settings such as the ITU.[115]

As the Internet grew ever more global in the 2000s, the pressure to multilateralize Internet governance continued. In 2009, the federal government and ICANN reset their delegation arrangement via an agreement they termed an "Affirmation of Commitments." In it, ICANN pledged to maintain "robust mechanisms for public input, accountability"—and also to remain headquartered in the U.S.[116] This final requirement reflects efforts on ICANN's part to explore a change in its legal basis. A 2007 internal ICANN report considered whether the organization was limited by "its legal personality being based in a specific jurisdiction."[117] As Michael Froomkin explained, "from ICANN's viewpoint, the prospect of international status

112. *See, e.g.*, Laurence Helfer, *International Dispute Settlement at the Trademark-Domain Name Interface*, 29 PEPP. L. REV. 87 (2001); David Simon, *An Empirical Analysis of Fair-Use Decisions Under the Uniform Domain-Name Dispute Resolution Policy*, 53 B.C. L. REV. 65 (2012).

113. A. Michael Froomkin, *Almost Free: An Analysis of ICANN's 'Affirmation of Commitments'*, J. ON TELECOMM. & HIGH TECH. L. 192, 192 (2011).

114. Raustiala, *supra* note 53, at 492. A split or splintered Internet is possible and maybe even probable—but would defeat much of what makes the Internet, the Internet. Rose Wong, *There May Soon Be Three Internets. America's Won't Necessarily Be the Best*, N.Y. TIMES (Oct. 15, 2018), https://www.nytimes.com/2018/10/15/opinion/internet-google-china-balkanization.html [https://perma.cc/P6GE-UJX8]; Sean McDonald & An Xiao Mina, *The War-Torn Web*, FOREIGN POL'Y (Dec. 19, 2018), https://foreignpolicy.com/2018/12/19/the-war-torn-web-internet-warring-states-cyber-espionage/ [https://perma.cc/JAN8-TX4U].

115. *About International Telecommunication Union (ITU)*, *supra* note 83.

116. *Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers*, ICANN (Sept. 30, 2009) [hereinafter *Affirmation of Commitments*], https://www.icann.org/resources/pages/affirmation-of-commitments-2009-09-30-en [https://perma.cc/8EVG-H75N]. Froomkin argues this is not a contract due to lack of consideration. Froomkin, *supra* note 113.

117. Froomkin, *supra* note 113.

certainly seemed to offer everything ICANN's critics feared ICANN most wanted: immunity from suit in the U.S., international stature, a lack of outside supervision and control, no need to have a 'membership' or file California and U.S. tax returns . . . ."[118] ICANN in the end did not pursue this option, and the Affirmation of Commitments with the federal government pledged that it would stay within the territorial jurisdiction of the U.S.[119]

Then, in 2014, the federal government announced a major policy change: it would cede control to ICANN permanently.[120] In doing so, the U.S. shed the last vestige of the American role as the key regulator of the core of the Internet. As with the decision to create ICANN in 1998, this was a juncture in which the federal government decisively moved Internet governance in its preferred direction. The Obama Administration stated its "intent to support and enhance the multistakeholder model . . . and maintain the openness of the Internet."[121] There was one central criterion, however: The U.S. "will not accept a proposal that replaces the NTIA role with a government-led or an inter-governmental organization solution."[122]

C. Two Visions of the Internet

A critical factor in the U.S. decision to relinquish control was the growing divergence in global views about regulation of the Internet. The federal government's preferences over Internet governance—and for outcomes such as general openness, few barriers to digital flows, and limited censorship—were broadly shared by most American allies.[123] But many other governments, most notably China and its authoritarian partners, had different views. This divide on what kind of Internet was desirable was summed up in a memorable phrase from French President Macron. Speaking in 2018, Macron said, "To be very politically incorrect,"

118. *Id.*

119. *Affirmation of Commitments*, *supra* note 116.

120. Craig Timberg, *U.S. to Relinquish Remaining Control over the Internet*, WASH. POST (Mar. 14, 2014), https://www.washingtonpost.com/business/technology/us-to-relinquish-remaining-control-over-the-internet/2014/03/14/0c7472d0-abb5-11e3-adbc-888c8010c799_story.html [https://perma.cc/M4RA-PAVM].

121. Press Release, NTIA, NTIA Announces Intent to Transition Key Internet Domain Name Functions (Apr. 2, 2014), https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions [https://perma.cc/T676-2ZDG].

122. *Id.*

123. Karen Kornbluh, *The Internet's Lost Promise – And How America Can Restore It*, FOREIGN AFFS., Sept./Oct. 2018.

> we are seeing two types of Internet emerge . . . *there is a Californian form of Internet, and a Chinese Internet*. The first is the dominant possibility, that of an Internet driven by strong, dominant, global private players, that have been impressive stakeholders in this development, that have great qualities and with which we work, but which at the end of the day are not democratically elected . . . . On the other side, there is a system where governments have a strong role, but this is the Chinese-style Internet: an Internet where the government drives innovations and control . . . . And so in that Internet, the state has found its place, but it is hegemonic.[124]

In the 1990s, President Clinton had famously lampooned Chinese efforts to regulate digital flows, reflecting the then-widely held view in the West. "We know how much the Internet has changed America," said President Clinton in a speech in 2000.[125] "Imagine how much it could change China. Now there's no question China has been trying to crack down on the Internet. Good luck! That's sort of like trying to nail Jell-O to the wall."[126] Yet, President Clinton was wrong; China proved very adept at regulating the Internet. And while it was not the only state interested in securing that control, it was certainly the most powerful. Authoritarian governments' interest in the Internet accelerated rapidly in the 21st century. As populations around the world moved online and began using digital means to share information and organize politically, many governments sought ever harder to multilateralize and thus better control the Internet. (And along the way, cabin perceived American power.) Existing international organizations such as the ITU provided a seemingly-neutral platform for which to pursue this goal. The 1997 "g-TLD" effort at creating a non-legally-binding accord over domain names, while doomed, was indeed a harbinger of the future.

In 2003, for instance, the ITU held the first "World Summit on the Information Society," or WSIS. WSIS resulted in the creation of a follow-on Working Group on Internet Governance, as well as a later "WSIS+10" process in 2015.[127] The "Tunis Agenda" that emerged from WSIS decisively favored the Chinese vision over the Californian, declaring that:

---

124. Emmanuel Macron, President, Fr., Speech at the 2018 Internet Governance Forum (Nov. 12, 2018), https://www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron [https://perma.cc/Y32D-D5W2] (emphases added); *see also* Eric Rosenbach & Shu Min Chong, *Governing Cyberspace: State Control vs. the Multistakeholder Model*, BELFER CTR. FOR SCI. & INT'L AFFS. (2019), https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model [https://perma.cc/W58C-K2LJ].

125. *Clinton's Words on China: Trade Is the Smart Thing*, N.Y. TIMES, Mar. 9, 2000, at A10.

126. *Id.*

127. INTERNET SOC'Y, UNDERSTANDING THE WSIS+10 REVIEW PROCESS (2015), https://www.internetsociety.org/wp-content/uploads/2017/08/WSISplus10-Overview.pdf [https://perma.cc/ZR6M-T7GL].

> [t]he Internet has evolved into a global facility available to the public and its governance should constitute a core issue of the Information Society agenda. The international management of the Internet should be multilateral, transparent and democratic . . . . *Policy authority for Internet-related public policy issues is the sovereign right of States*.[128]

This same document led to the creation of a UN-led Internet Governance Forum, or IGF.[129] The IGF has little operational control over the Internet, but it does provide an alternative, more state-centric platform for debating Internet policy.

Adding to global pressure, the period from WSIS to WSIS+10 was one in which American firms, such as Facebook, Google, and Twitter, began to dominate the Internet even more. In short, in the years leading up to the decision to cede greater authority to ICANN, the Internet was in some respects becoming ever more American, even as the user base became increasingly global. These twin developments increased tensions and rising calls for greater state control—either at the national level or via multilateral arrangements—naturally followed.

In the fall of 2011, for example, the government of India issued a call to "place Internet governance under the auspices of the UN, or, as some have characterized it, 'in a box with a UN label stamped on the side.'"[130] Shortly after, the Organization for Economic Cooperation and Development ("OECD"), composed mainly of Western industrialized democracies, countered with a *Communique on Principles of Internet Policy-Making* that endorsed multistakeholderism: "due to the rapidly changing technological, economic and social environment within which new policy challenges emerge," the OECD statement declared, "multi-stakeholder processes have been shown to provide the flexibility and global scalability required to address Internet policy challenges."[131]

The battle between multilateralism and multistakeholderism reached a peak at the 2012 World Conference on International Telecommunications, again convened by the ITU.[132] Authoritarian governments, led by Russia and China, sought an agreement that would decisively strengthen multilateral

128. World Summit on Info. Soc'y, *Tunis Agenda for the Information Society*, WSIS-05/TUNIS/DOC/6 (Rev. 1)-E (Nov. 18, 2005), https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html [https://perma.cc/2MRD-Z77S] (italicized text bolded in original source).

129. *Id.*

130. Waz & Weiser, s*upra* note 76, at 332.

131. OECD, COMMUNIQUÉ ON PRINCIPLES FOR INTERNET POLICY-MAKING 4 (2011), https://www.oecd.org/digital/ieconomy/48387430.pdf [https://perma.cc/5B9R-LJ84].

132. *World Conference on International Telecommunications (WCIT-12)*, ITU, https://www.itu.int/en/wcit-12/Pages/default.aspx [https://perma.cc/9WAD-2J4P] (last visited Nov. 12, 2022).

regulation.[133] Republican members of Congress in particular spoke out strongly in favor of ICANN despite—or perhaps because—of its vaguely countercultural-sounding "multistakeholder model."[134] Some seemed to view the existing multistakeholder approach as desirable precisely *because* the government role was cabined. For example, Representative Greg Walden, a Republican, noted that the Internet "has prospered under a multistakeholder model absent the heavy-hand of government regulation."[135] "If we are not vigilant," he declared, the "[UN forum] just might break the Internet by subjecting it to an international regulatory regime designed for old-fashioned telephone service."[136] Views from the private sector were similar. Vinton Cerf, one of the most influential early creators of the Internet, declared the prospect of multilateral ITU control over Internet governance "potentially disastrous."[137] As leader of its delegation to the World Conference on International Telecommunications, the U.S. chose not a State Department or Commerce official, but Terry Kramer, an executive at Vodaphone with extensive experience in the telecommunications business.[138]

The U.S., Australia, India, Israel, Japan, and most of Europe refused to sign an agreement at the conference.[139] The U.S. declared that it would not support a treaty "that is not supportive of the multistakeholder model."[140] Two years later, the U.S. reiterated that it was "crystal clear we would not accept a replacement that would be government-led or be an intergovernmental organization."[141] Nonetheless, the pressure for change continued from other governments. This was fueled in part by the incendiary revelations about NSA

133. Violet Blue, *WCIT-12 Leak Shows Russia, China, Others Seek to Define 'Government-Conrolled Internet',* ZDNET, https://www.zdnet.com/article/wcit-12-leak-shows-russia-china-others-seek-to-define-government-controlled-internet/ [https://perma.cc/J6R9-WRQB].

134. Multistakeholderism in this domain tapped interestingly into the preferences of both parties. Republicans liked the private sector orientation, and often saw it as an attractive alternative to government regulation. Democrats saw multistakeholderism as progressive, incorporating all (or most) effected interests and featuring extensive public input. Both liked that American companies were highly dominant worldwide.

135. *International Proposals to Regulate the Internet: Hearing Before the Subcomm. on Commc'ns & Tech. of the H. Comm. on Energy & Commerce*, 112th Cong. 1-4 (2012) (statement of Greg Walden, Chair, Subcomm. on Commc'ns & Tech.).

136. *Id.*

137. *Id.* at 78 (statement of Vinton Cerf, Vice President & Chief Internet Evangelist, Google, Inc.).

138. ITU, *ITU Interview @ WCIT – 12: H.E Terry Kramer, Ambassador, Department of State, USA*, YOUTUBE (Dec. 9, 2012), https://www.youtube.com/watch?v=HXWvlSbGRE4 [https://perma.cc/NZ4Z-WQPF].

139. *See World Conference on International Telecommunications (WCIT-12)*, *supra* note 138.

140. Eric Pfanner, *U.S. Rejects Telecommunications Treaty*, N.Y. TIMES (Dec. 13, 2012), https://www.nytimes.com/2012/12/14/technology/14iht-treaty14.html [https://perma.cc/ER7D-29B8].

141. *Future of Internet Governance*, C-SPAN (Apr. 4, 2014), http://www.c-span.org/video/?318699-1/internet-governance&start=239 [https://perma.cc/ZRV6-RBPT] (recording of panel held at the Hudson Institute in Washington, D.C.).

spying by Edward Snowden in 2013.[142] NSA espionage had no direct connection to Internet governance, but Snowden's disclosures raised hard questions about how much foreigners could trust the U.S. The Snowden affair nudged the U.S. to diminish its overt role in Internet governance still further.[143]

Meanwhile, China continued to lead efforts for greater global focus on "cyber sovereignty."[144] At the Chinese-organized World Internet Conference in 2015, Xi Jinping stated that "There should be no unilateralism" with regard to the Internet.[145] In a barely-veiled swipe at the U.S., he declared, "decisions should not be made with one party calling the shots or only a few parties discussing among themselves."[146] (China's World Internet Conference, considered at first a sideshow, has only grown in significance, with tech luminaries such as Tim Cook of Apple and Sundar Pinchai of Google attending over the years.)[147] This was a precis of Macron's "Chinese Internet"—substantial sovereign control with, if necessary, international coordination occurring via traditional state-centered multilateralism.

This jockeying reflected a conceptual divide between the U.S. and China. To American officials, ICANN's rule-making processes were properly reflective of the views of myriad stakeholders, especially from the private sector. To China and its allies, the fact that so many ICANN participants were tied to the U.S. and that ICANN was located in California meant that ICANN's supposed multistakeholderism was simply a mask for U.S. power. This view was especially prevalent because to many Chinese observers, the line between public and private is far blurrier than it appears from the vantage point of Washington, D.C. And indeed, the preferences of the U.S.—an open Internet, with powerful private firms, and disproportionately American players—were largely supported by multistakeholderism, since so many of the participants share these preferences. The only realistic alternative to multistakeholderism, *The Economist* argued, was one China enthusiastically endorsed: "governments bringing the Internet under their control."[148]

---

142. Tim Walker, *NSA Whistleblower's Leaks Prompt US to Make Control of Internet Truly Worldwide*, INDEPENDENT (March 19, 2014, 2:01 AM), https://www.independent.co.uk/tech/edward-snowden-nsa-whistleblower-s-leaks-prompt-us-to-make-control-of-internet-truly-worldwide-9200578.html [https://perma.cc/XQ2T-SFPX]; BRADSHAW ET AL., *supra* note 95, at 3; Jack Goldsmith, *The Tricky Issue of Severing US "Control" over ICANN,* HOOVER INST. (Feb. 24, 2015), https://www.hoover.org/research/tricky-issue-severing-us-control-over-icann [https://perma.cc/Z8AN-RLRB].

143. Walker, *supra* note 142; BRADSHAW ET AL., *supra* note 95, at 3; Goldsmith, *supra* note 148.

144. *China Internet: Xi Jinping Calls For 'Cyber Sovereignty'*, BBC NEWS (Dec. 15, 2015), https://www.bbc.com/news/world-asia-china-35109453 [https://perma.cc/2U97-KWJA].

145. *Id.*

146. *Id.*

147. Segal, *supra* note 15, at 17.

148. *In Praise of Chaos: Governments' Attempts to Control the Internet Should Be Resisted*, ECONOMIST (Oct. 1, 2011), https://www.economist.com/leaders/2011/10/01/in-praise-of-chaos [https://perma.cc/PE74-AJP8].

In short, the specter of growing state control over the Internet formed a critical underpinning to the decision by the U.S. to hand full authority over the naming and numbering function to ICANN. To be sure, this decision was not without domestic political controversy. Indeed, it was denounced by some Republicans as a giveaway akin to the transfer of the Panama Canal under President Carter.[149] These politicians preferred that the U.S. retain unilateral control as much as possible. Senator Ted Cruz of Texas declared that "since the internet's inception, the United States government has stood guard over critical internet functions."[150] Legal efforts to halt the transfer of power to ICANN ensued—none were successful.[151] ICANN became fully autonomous on October 1, 2016.[152]

IV. DELEGATION AND TRUSTEESHIP

A. Explaining the Transfer of Authority to ICANN

What led the United States to relinquish its unique position over the Internet, cease contracting with ICANN, and transfer important powers—permanently? To reverse a famous locution about delegation theory, why did the U.S. choose to abdicate, not delegate?[153]

The dominant approach to the delegation of authority to international organizations builds off of principal-agent theories. These theories, widely deployed to explain legislative delegation to bureaucracies, also have been deployed to understand the relationship between governments and international organizations.[154] But because they generally rest on the assumption that every act of delegation involves a "contingent grant of authority" from principal to agent, their fit for transfers of power that are permanent is uncertain.[155]

As applied in the international context, principal-agent theory treats governments as principals who, in order to better manage policy externalities, facilitate law-making, and enhance policy credibility, delegate defined powers to international organizations (agents). Agents in turn enjoy varying

149. Jonathan Zittrain, *No, Barack Obama Isn't Handing Control of the Internet over to China*, NEW REPUBLIC (March 24, 2014), https://newrepublic.com/article/117093/us-withdraws-icann-why-its-no-big-deal [https://perma.cc/S34Q-R9M4].

150. Cecilia Kang & Jennifer Steinhauer*, Ted Cruz Fights Internet Directory's Transfer; Techies Say He Just Doesn't Get It*, N.Y. TIMES (Sept. 15, 2016), https://www.nytimes.com/2016/09/16/us/politics/ted-cruz-internet-domain-names-funding.html [https://perma.cc/MC9V-98JK].

151. *See* DOTCOM Act of 2014, H.R. 4342, 113th Cong. (2014).

152. *Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends*, ICANN (Oct. 1, 2016), https://www.icann.org/en/announcements/details/stewardship-of-iana-functions-transitions-to-global-internet-community-as-contract-with-us-government-ends-1-10-2016-en [https://perma.cc/56SJ-42C2].

153. *See generally* KIEWEIT & MCCUBBINS, *supra* note 11.

154. Hawkins et al., *supra* note 7; Alter, *supra* note 32; Johnson & Urpelainen, *supra* note 7.

155. *See generally* LAKE & MCCUBBINS, *supra* note 11.

degrees of autonomy and "slack."[156] The degree to which agents exercise autonomy is a point of contestation in the scholarly literature. But all students of international organizations agree they enjoy *some* autonomy—indeed, the logic of creating them often rests on this fact, else they are simply (and sometimes costly and epiphenomenal) extensions of state power and their usefulness limited.

Many scholars have made the case that governments do not fully control the international organizations they create. Michael Barnett and Martha Finnemore, for example, claim that "the rational-legal authority that [international organizations] embody gives them power independent of the governments that created them and channels that power in particular directions."[157] Moreover, they argue, international organizations "are constrained by governments, but the notion that they are passive mechanisms with no independent agendas of their own is not borne out by any detailed empirical study of an IO that we have found."[158] Roland Vaubel, using a different nomenclature and approach, asserts a similar position: "the principal-agent problem is due to the fact that the IO has vested interests which differ from the preferences of the voters and that the voters cannot effectively control the IO because they are rationally ignorant of most of its activities and/or lack the power to impose their will."[159]

Principal-agent theory examines the structure and strategy inherent in the ways that governments and international organizations interact. The type of delegation, or the powers delegated, can include legislative, adjudicative, enforcement, and regulatory delegation. At the highest level of abstraction, the claim is that there are systematic ways that principals control agents; while autonomy exists, it is generally cabined even if the precise mechanisms by which the principal exercises control are obscured to the ordinary observer. As a leading work in this strand of research defines the relationship between principals and agents:

> Delegation is a conditional grant of authority from a Principal to an Agent in which the latter is empowered to act on behalf of the former. This grant of authority is limited in time or scope and must be revocable by the Principal. Principals and agents are, in the language of constructivism, mutually-constitutive . . . . the actors are defined by their relationship to each other.[160]

The creation of ICANN in 1998 was clearly an act of delegation consistent with this theoretical approach. ICANN was directly delegated powers to regulate key aspects of the governance of the Internet. Whereas

156. *See generally* Mathew McCubbins et al., *Administrative Procedures as Instruments of Political Control*, 3 J. LAW, ECON., & ORG. 243 (1987).

157. *See generally* Michael N. Barnett & Martha Finnemore, *The Politics, Power, and Pathologies of International Organizations*, 53 INT'L ORG. 699 (1999).

158. *See id.*

159. Vaubel, *supra* note 5, at 126.

160. Hawkins et al., *supra* note 7, at 7; *see generally* Liesbet Hooghe & Gary Marks, *Delegation and Pooling in International Organizations,* 10 REV. INT'L ORGS. 305 (2014).

many agents in international relations have only metaphoric contracts and amorphous principals, ICANN had a literal contract from a well-defined and powerful principal, the U.S. federal government. And while ICANN is technically not an international organization, it in many respects performs the functions of one. The contract with ICANN was renewable and revocable. And the U.S. did, over time, adjust the contract, through such measures as the 2009 "Affirmations of Commitments,"[161] in ways that seemed aimed at minimizing or forestalling certain forms of autonomous behavior (such as moving out of American territory). The creation of ICANN in 1998 is, as a result, broadly consistent with principal-agent accounts of delegation.[162] The U.S. sought to delegate a residual power it held, or plausibly held, over a central aspect of the regulation of the Internet to a third-party actor.[163] The Commerce Department elicited bids from putative agents who would carry out the desired work and subject its chosen agent to a contract that specified performance.[164]

From the perspective of the U.S., this act of delegation had several benefits. It removed the federal government from the direct supervision of the Internet and allowed for an easier incorporation of private actors into the governance process. For example, had the U.S. sought to create an equivalent multistakeholder process via an existing federal agency, perhaps in the Commerce Department, many statutory and administrative rules and procedures governing lobbying, notice and comment, and the Administrative Procedures Act would have kicked in.[165] These procedures are important but time-consuming, cumbersome, and at times politically unpredictable. The creation of and delegation to ICANN streamlined that process, allowing a swift transfer by the Clinton Administration of a crucial regulatory function.

Moreover, transferring authority to ICANN was politically beneficial; it rewarded American technology and telecommunications firms, which were ascendant in the U.S. economy, and was consistent with President Clinton's broad "third way" commitment to privatization more generally. Indeed, as early as 1994 the federal government's commitment to privatizing the Internet was widely discussed. While ICANN was not yet in existence (or even contemplated) in 1994, contemporaneous press reports noted that, "[h]aving succeeded beyond its wildest dreams in nurturing the Internet computer web into a vital national communications system, the Federal Government has begun turning over to the private sector the job of operating and maintaining the network's major arteries."[166] By involving private firms in the day-to-day operation of the Internet, the federal government began creating the Internet

161. *Affirmation of Commitments*, *supra* note 116.

162. Hawkins et al., *supra* note 7, at 7; *see generally* Hooghe & Marks, *supra* note 160.

163. I say residual because, as discussed above, in practice Jon Postel and his team was carrying out the IANA function, but the U.S. government claimed—and plausibly held—the power to revoke that any time.

164. *See* preceding paragraph.

165. *See generally* Jon D. Michaels, *Privatization's Pretensions*, 77 U. CHI. L. REV. 717, (2010).

166. Peter H. Lewis, *US Begins Privatizing Internet's Operations*, N.Y. TIMES, Oct. 24, 1994, at D1.

as we know it today. The creation of ICANN was the next logical step in this evolution.

In sum, the initial creation of ICANN and the early dynamic between the U.S. and ICANN fit well within received ideas about principal-agent theory in the international domain. As with many administrative agencies, delegation was a rational choice that enhanced policymaking and maximized expertise. The Obama Administration's decision two decades later to fully hand over power to ICANN, however, is less easily reconciled with delegation theory.

While the original ICANN contract was revocable and adjustable over time, its termination is not. It is an elementary principle of contract theory that contracts are valid only when willingly entered into by the parties.[167] Once a contract ends, any future contract requires the consent of all parties. The termination of the contract with ICANN is, thus, a legally irrevocable act by the U.S., violating one of the core strands of a principal-agent relationship. Consequently, the federal government today has limited regulatory jurisdiction over ICANN, which remains a California-incorporated non-profit corporation subject to the full protections of California law.[168] This is perhaps one reason the U.S. insisted that ICANN remain sited within American territory—though ICANN, possibly with this eventuality in mind, has set up smaller satellite offices in Istanbul, Singapore, Montevideo, and Brussels.[169] Putting extreme and arguably fanciful scenarios to one side, the revocation of the prior Commerce Department contract means ICANN is effectively no longer an agent and the U.S. no longer its principal.

The U.S. decision to grant ICANN full autonomy is, thus, at best an uneasy fit for conventional models of principal-agent theory. Is ICANN instead more like a trustee? Karen Alter has argued that principal-agent theory can be fruitfully extended by understanding that some putative agents are in fact not best understood as agents, but rather as trustees.[170] Unlike agents, trustees are deliberately intended to be highly independent of the principal's specific wishes. In Alter's terms:

167. *See e.g.* E. ALLAN FARNSWORTH & ZACHARY WOLFE, FARNSWORTH ON CONTRACTS, § 3.01 (4th ed. 2019) ("What requirements must the bargaining process meet if it is to result in a contract? . . . The first requirement that of assent, follows from the premise that contractual liability is consensual.").

168. I stress *limited* because, while extreme, the U.S. could conceivably reassert some limited forms of control over ICANN and its regulatory function through, say, a declaration of national emergency or invocation of the International Emergency Economic Powers Act. International Emergency Economic Powers Act, Pub. L. No. 95-223, 91 Stat. 1626 (1977).

169. *ICANN's Global Expansion*, ICANN, https://www.icann.org/en/history/global-expansion [https://perma.cc/4B8M-YT4H], (last visited Nov. 13, 2022).

170. Alter, *supra* note 32, at 35.

> Trustees are (1) selected because of their personal reputation or professional norms, (2) given independent authority to make decisions according to their best judgment or professional criteria, and (3) empowered to act on behalf of a beneficiary.[171]

The purpose of delegation to a trustee, in this account, is to "harness the authority of the Trustee so as to enhance the legitimacy of political decision-making."[172] While a principal-trustee relationship shares similarities with a principal-agent relationship, the core distinction is that trustees are intended to have greater autonomy and, typically, have built-in protections against short-term control by principals.[173]

Judicial institutions are the paradigmatic example of trustees. Most courts are intended—perhaps required—to have a meaningful degree of independence and autonomy. Courts, however, do face political control, even if that control is designed to be attenuated and to operate at a temporal distance. For example, the U.S. judicial system is widely seen as independent and legitimate. Independence largely flows from the fact that federal judges have life tenure; yet they are subject to both *ex ante* and *ex post* forms of political control. Presidential nomination and Senate confirmation serve as *ex ante* controls; impeachment as an *ex post* control.[174] Moreover, Congress possesses plenary power over the federal courts' jurisdiction, a rarely-exercised power that allows Congress both to create (or terminate) all courts inferior to the Supreme Court and to curtail jurisdiction subject to the Exceptions Clause.[175] In practice, however, these controls have limited impact. This gives federal judges substantial, almost untrammeled, autonomy on individuals decisions, even if, ultimately, they remain subject to *ex ante* approval and *ex post* recall by their political masters. In all these ways, political procedures over the judiciary allow the political branches some measure of control, but that control is so limited and distinctive as to merit a different nomenclature: trustee rather than agent.

Likewise, international courts can be understood as trustees subject to a host of political controls; in many respects these controls are more powerful than those domestic courts face. Governments create international courts via treatymaking. Judges are chosen for specific periods (not for life, as in the federal courts) and international courts' jurisdiction is subject to state consent, which can be revoked *ex post*.[176] Governments can also withdraw altogether from the underlying treaty, as the U.S. recently did, in the wake of an adverse International Court of Justice (ICJ) ruling, with regard to the 1955 Treaty of

171. *Id.*
172. *Id.*
173. *Id.*
174. U.S. CONST. art. III.
175. *See generally* Christopher Jon Sprigman, *Congress's Article III Power and the Process of Constitutional Change*, 95 N.Y.U. L. REV. 1778 (2020).
176. As the U.S. did for the International Court of Justice. *See generally* Keith Highet, Note, *Litigation Implications of the US Withdrawal from the Nicaragua Case*, 79 AM. J. INT'L L. 992 (1985).

Amity with Iran.[177] International judges are meant to be independent of their national governments but often are not. On the ICJ, the judges are colloquially referred to by their national origin (e.g., "the British judge"), and empirical studies of ICJ voting records show they act accordingly. In short, even for the paradigmatic example of a trustee, there is substantial—though deliberately limited—*ex post* levers political actors possess.

None of this is true for ICANN. ICANN's CEO and board members were and are not subject to *ex ante* approval by the U.S. or other governments either, nor can they be removed or their decisions reversed *ex post*.[178] In these respects, ICANN is more independent than most courts, the core of the concept of trusteeship.

As a result, ceding authority to ICANN for Internet governance is more akin to a trustee relationship than a delegation. ICANN, which has long comprised many technical expert groups, has authority rooted in highly specialized knowledge—a characteristic emphasized by both principal-agent theory and trusteeship theory.[179] The multistakeholder model also has procedural legitimacy rooted in its encompassing governance process and inclusive approach. NGOs, firms, and other non-state actors are today a central feature in global governance not because they have risen in power vis-à-vis governments, but for the advantages they bring to governments in the act of governing.[180] These include legitimation (albeit contested) but also the very concrete informational and political resources they possess.

Seen in this light, ICANN shares some important features with conventional trustees. In short, the core question animating this Article—why a dominant state like the U.S. would cede governance authority permanently to an organization such as ICANN—requires attention not only to the logic of delegation, but also to the distinctive nature of the politics of multilateralism in the digital domain. Faced with extensive and rising international demands for multilateral control over a critically-important global resource, the U.S. faced two choices. It could continue to retain residual control over its agent, or it could cede full authority in key governance areas to that agent. The first strategy preserved national control but was brittle. Greater control by the ITU or some third actor or agent was not impossible—indeed it had already been attempted by the ITU—and the preservation of a global Internet required that there be only one source of naming and numbering. Because that threat was credible, the status quo—standard delegation—was, over the long term, unattractive to American decisionmakers.

The second option of ceding the IANA function irrevocably would not in fact block the multilateralization of Internet governance, but it would blunt much of the force of calls for multilateralization because the U.S. would no longer hold residual control over a key feature of Internet governance.

177. *US to End Treaty of Amity with Iran After ICJ Ruling*, BBC NEWS (Oct. 4, 2018), https://www.bbc.com/news/world-middle-east-45741270 [https://perma.cc/W42Y-JHQF].

178. *ICANN Bylaws*, *supra* note 21, at Art. 4.

179. *See generally* Hawkins et al., *supra* note 7; Alter, *supra* note 32, at 39.

180. *See generally States, NGOs, and International Environmental Institutions*, *supra* note 85; *see generally The Role of NGOs in Treaty-Making*, *supra* note 85.

ICANN's multistakeholder model entailed a major role for a wide array of governments as well as non-state actors, and while many were U.S. based, they were not under the direct control of the U.S. The rising normative appeal of multistakeholderism, moreover, made political attacks on ICANN's governance model less palatable to many governments. For the U.S., the fact that American firms and actors remained so critical to the operation of the Internet, and generally shared so many core values and preferences over Internet governance, meant that granting ICANN greater power did not necessarily diminish the realization of American preferences; indeed, it generally supported them. The basic preference structure remained intact even as the key actors shifted. This is the paradox at the heart of the ICANN case. Much as in Giuseppe Tomasi di Lampedusa's classic novel of 19th century Italian political change, *The Leopard*, "for things to remain as they are, things [had] to change."[181]

In sum, while theories of delegation in international relations provide plausible accounts of some aspects of the global governance of the Internet, none adequately explains American behavior in relinquishing control to ICANN. Ceding its residual power in an irrevocable way to an international organization is distinctive and perhaps even novel. The approach taken by the U.S. was one of preferences realized through the relinquishment of power to an entity designed to be relatively insulated from political pressure. The Obama Administration chose and supported not an obedient agent, but a more legitimate and independent trustee.

That the U.S. could do this at all reflected its dominance in the arena of Internet governance. In this regard, multistakeholder governance over the Internet has triumphed in large part because it reflects American power, not in spite of it.

B. Multistakeholderism and International Law: Implications from the ICANN Experience

Does the story of ICANN have broader significance for theories of international law and organization? Multistakeholder governance in international law remains rare, but it appears to be on the rise.[182] While the particularities of the ICANN case are unusual and perhaps unique, the general pattern of increasing use of multistakeholder models may not be. Is there a logic to the "choice for multistakeholderism?"[183] Consider, for instance, the creation of the Global Fund to Fight AIDS, Tuberculosis, and Malaria. The World Health Organization (WHO) has been the dominant actor in global health governance for decades.[184] But in the 1990s, there was concern, particularly among Western powers, that the WHO was becoming unduly

181. GIUSEPPE TOMASI DI LAMPEDUSA, THE LEOPARD 28 (Pantheon Books 2007) (1958).

182. Raymond & DeNardis, *supra* note 76.

183. *See, e.g.*, Helen V. Milner & Dustin Tingley, *The Choice for Multilateralism: Foreign Aid and American Foreign Policy*, 8 REV. INT'L ORGS. 313 (2013).

184. *About WHO*, WHO, https://www.who.int/about [https://perma.cc/K2G8-8SUL] (last visited Dec. 21, 2022).

politicized, state-centric, and bureaucratic.[185] The Global Fund was created after a G8 announcement in 2001 to provide an alternative for critical infectious diseases.[186]

From its inception, the Global Fund has had a multistakeholder structure, reflecting both the powerful role played by various NGOs but also the outsized influence of a then-new actor on the global health scene: the Bill and Melinda Gates Foundation.[187] But it also was emblematic of a new politics that not all were keen on. As Suerie Moon writes:

> For some, the rise of "multistakeholderism" was seen as a Trojan horse for industries and foundations not only to exert more control over global health initiatives, but also to counteract the numerical advantage that developing countries had in the WHO and other UN forums. From this perspective, the shift away from WHO at the turn of the millennium could be seen, not as a rejection of bureaucratic inefficiency, but as a shift to create new organizations where Northern governments and donors would have more sway.[188]

Multistakeholderism has normative appeal for many actors in international law precisely because it allows a wide range of actors into the circle of influence and decision making. But as with ICANN, the creation of the Global Fund underscored a growing concern on the part of some governments with traditional multilateral approaches to international law. One can plausibly explain the creation of these two governance bodies as arising from a belief that the policy preferences of powerful governments—in particular, the advanced industrial democracies that are also the home of many well-resourced firms and NGOs—might be best realized indirectly through greater incorporation of a wide variety of private sector actors, rather than directly through traditional state-centric international law models.

And as political power increasingly disperses in the world, the appeal of traditional multilateralism is likely to diminish for the U.S. In some settings, such as the United Nations Security Council, entrenched rules continue to favor traditional great powers.[189] But many international legal bodies operate on a one nation-one vote system and are subject to increasing demands for inclusive leadership.[190] As noted above, the greater inclusion of NGOs in international organizations is less a sign of governments ceding power than a sign that NGOs bring valuable resources to the table. But in the

185. Suerie Moon, *Global Health: A Centralized Network Searching (in Vain) for Hierarchy*, *in* GLOBAL GOVERNANCE IN A WORLD OF CHANGE 234, 238 (Michael N. Barnett et al. eds., 2021).

186. *History of the Global Fund*, GLOB. FUND, https://www.theglobalfund.org/en/about-the-global-fund/history-of-the-global-fund/ [https://perma.cc/TA8J-PX7L] (last visited Nov. 13, 2022).

187. *See generally* Moon, *supra* note 185.

188. *Id.* at 253.

189. *Compare* U.N. Charter arts. 39-51 (Chapter VII), *with* U.N. Charter arts. 9-22 (Chapter IV).

190. *See generally* Moon, *supra* 185.

vast majority of settings, NGO participation is limited to voice but not decisions. What distinguishes multistakeholderism, and perhaps makes it increasingly appealing to powerful Western governments who foresee greater power dispersion, is precisely that it goes much further.

In this sense we can trace a broad arc from the great power-centric approach of the 19th and early 20th centuries to the liberal multilateral order of the postwar era that was far more inclusive of weak governments, to a 21st century embrace of state as well as nonstate actors in international law. Some have interpreted this as a radical diminishment of state authority. As Miles Kahler and David Lake describe this view:

> The state's monopoly of familiar governance functions is ending as governance migrates down to newly empowered regions, provinces, and municipalities; up to supranational organizations; and laterally to such private actors as multinational firms and transnational [NGOs] that acquire previously "public" responsibilities.[191]

This view identifies some important developments but partly misstates (or may be misinterpreted with regard to) their significance and cause. It is not the weakness of governments, nor the power of nonstate actors, that solely explains these trends. It is more likely a combination of greater specialization in international cooperation combined with a political logic that recognizes—often—the utility of ceding greater power to others who share preferences over outcomes and procedures. This more indirect mode of governance is by no means new, but its significance for international law has not fully been appreciated.

V. CONCLUSION

The United States created the Internet. From its early Defense Department origins, through its National Science Foundation support, university framework, and technology firm dominance, the Internet and its key applications have been America's gift to the world. And by creating ICANN in 1998, the U.S. gave the rapidly-growing Internet both a formal structure for key elements of governance and more autonomy for regulatory processes. In the two decades that followed, the Internet became the most significant mode of communications in human history and the backbone of political, economic, and social activity for billions around the globe.

Why did the U.S. ultimately choose to relinquish an important aspect of authority and control over this unwieldy, but enormously valuable, global resource? The initial choice to delegate important regulatory functions to ICANN was a paradigmatic example of the gains from delegation in international law and organization. Less readily explained, however, was the decision to cede power permanently in 2016. Yet, diminishing its most visible

191. Miles Kahler & David Lake, *Globalization and Governance*, *in* GOVERNANCE IN A GLOBAL ECONOMY 1, 1 (Miles Kahler & David Lake eds., 2003).

role in the regulation of the Internet even further by ceding power to a trustee was, perhaps paradoxically, a rational strategy for the federal government. By the late 2000s, the threat of greater multilateral regulation of the Internet was clear and growing. By freeing ICANN and entrusting it with (limited) power, the U.S. blunted a more overt multilateral challenge to the basic model of an open Internet. Control over resources does not equal control over outcomes. Indeed, as the case of global governance of the Internet suggests, sometimes the opposite is true.

Monopolies of Misinformation: How Competitive Markets Can Improve Public Dialogue

John Bogert*

TABLE OF CONTENTS

* J.D., May 2023, The George Washington University Law School. B.A., Economics, May 2020, Franklin & Marshall College. Special thanks are due to Professor William Kovacic for his teachings and assistance, to my grandparents James and Kathleen Nicholson for making this work possible, and to my mother for her unwavering love and support.

I. INTRODUCTION

The Pacific Northwest tree octopus (Octopus Paxarbolis) is unique among cephalopods for its ability to survive on land, where it inhabits the tree canopies of the Olympic Peninsula's temperate rainforests.[1] It is also completely fictional and the subject of a notorious 1998 Internet hoax now "commonly used in Internet literacy classes" to teach students responsible Internet browsing.[2]

However, the lesson appears not to have stuck with students, and now misinformation plagues the Internet with consequences for the physical world. Many in the medical and political communities credit misinformation for seeding the present distrust in COVID-19 vaccines and U.S. elections,[3] and that distrust has contributed to vaccine hesitancy, the COVID-19 death count, the erosion of faith in democratic government, and the false justification of political violence.[4]

Given misinformation's ill effects, it is not surprising that Americans generally agree that misinformation should be curtailed in some manner or another.[5] Indeed, 88% of Americans believe that it has caused "some" or "a

---

1. Lyle Zapato, *Help Save the Endangered Pacific Northwest Tree Octopus from Extinction!*, ZAPATO PRODS. INTRADIMENSIONAL, https://zapatopi.net/treeoctopus/ [https://perma.cc/7AXF-AKW7] (last visited Nov. 20, 2021).

2. *Save The Pacific Northwest Tree Octopus*, LIBR. OF CONG., https://www.loc.gov/item/lcwaN0010826 [https://perma.cc/695M-4ELL] (last visited Nov. 20, 2021); *see also* Shem Unger & Mark Rollins, *Don't Believe Everything About Science Online: Revisiting the Fake Pacific Northwest Tree Octopus in an Introductory Biology College Course*, 32 SCI. EDUC. INT'L 159, 159-61 (2021) ("This study found that a large number of university students failed to determine this [hoax] as false.").

3. *See* Heather Hollingsworth, *Doctors Grow Frustrated over COVID-19 Denial, Misinformation*, ASSOCIATED PRESS (Oct. 4, 2021), https://apnews.com/article/coronavirus-pandemic-misinformation-health-433991ea434e12ccfdf97b5db415310d [https://perma.cc/56Q7-Q6BG] (reporting health care providers' exasperation with misinformation as a barrier to patients consenting to certain care); *see* Vera Bergengruen & Billy Perrigo, *Facebook Acted Too Late to Tackle Misinformation on 2020 Election, Report Finds*, TIME (Mar. 23, 2021, 6:00 AM), https://time.com/5949210/facebook-misinformation-2020-election-report/ [https://perma.cc/UMQ5-3VSF] ("The debate over accountability, content moderation, [and] online misinformation . . . is likely to take center stage . . . on Capitol Hill . . . .").

4. *See* Emma Pierson et al., *The Lives Lost to Undervaccination, in Charts*, N.Y. TIMES (Sept. 14, 2021), https://www.nytimes.com/interactive/2021/09/14/opinion/states-undervaccination-deaths.html [https://perma.cc/5A8W-4ZZR]; s*ee* Craig Silverman et al., *Facebook Hosted Surge of Misinformation and Insurrection Threats in Months Leading Up to Jan. 6 Attack, Records Show*, PROPUBLICA (Jan. 4, 2022, 8:00 AM), https://www.propublica.org/article/facebook-hosted-surge-of-misinformation-and-insurrection-threats-in-months-leading-up-to-jan-6-attack-records-show [https://perma.cc/HF2R-DPGU].

5. *See The American Public Views the Spread of Misinformation as a Major Problem*, ASSOCIATED PRESS & NORC (Oct. 8, 2021), https://apnorc.org/projects/the-american-public-views-the-spread-of-misinformation-as-a-major-problem/ [https://perma.cc/WV3Y-YWJ7]; *see* Amanda Seitz & Hannah Fingerhut, *Americans Agree Misinformation Is a Problem, Poll Shows*, ASSOCIATED PRESS (Oct. 8, 2021), https://apnews.com/article/coronavirus-pandemic-technology-business-health-misinformation-fbe9d09024d7b92e1600e411d5f931dd [https://perma.cc/4PEX-2BGD].

great deal" of confusion regarding "basic facts."[6] However, finding a solution has proven challenging.

So far, the debate over how to combat misinformation has stagnated around reforming controversial Section 230,[7] a provision of the Communications Decency Act that, among other things, limits the liability websites face for user-posted content on their platforms.[8] Section 230 reform efforts generally aim to alter websites' legal incentives to motivate action,[9] and although there have been many proposals,[10] thus far, none have evidently offered a solution for misinformation that has proven sufficiently politically popular, constitutionally viable, and regulatorily effective to become law.[11] For one, the politics of misinformation have become entwined with the divisive politics of how to respond to COVID-19 and claims of election fraud,[12] and secondly, the First Amendment bars a broad range of speech regulation with few exceptions.[13]

In contrast, a simultaneous antitrust reform movement is poised to alter the market incentives that websites and social media firms face when deciding how to handle misinformation on their platforms. The movement has already claimed misinformation as just another symptom of a larger monopoly problem that permits powerful firms to prioritize their own interests over consumer preferences[14]—specifically consumers' preference for trustworthy, accurate news[15]—and the support for antitrust change is growing.[16] Since the

6. MICHAEL BARTHEL ET AL., PEW RSCH. CTR., MANY AMERICANS BELIEVE FAKE NEWS IS SOWING CONFUSION 3 (2016), https://www.pewresearch.org/journalism/wp-content/uploads/sites/8/2016/12/PJ_2016.12.15_fake-news_FINAL.pdf [https://perma.cc/M872-7A2G].

7. Daren Bakst & Dustin Carmack, *Section 230 Reform: Left and Right Want It, for Very Different Reasons*, HERITAGE FOUND. (Apr. 12, 2021), https://www.heritage.org/technology/commentary/section-230-reform-left-and-right-want-it-very-different-reasons [https://perma.cc/GR5F-9452] ("[B]oth the left and the right agree that Section 230 needs to be reformed. But this is generally where the agreement ends . . . . Some want to reduce the chilling of speech . . . . And some want to use Section 230 reform . . . to chill speech still further.").

8. *See* 47 U.S.C. § 230(c)(2)(A), (c)(1).

9. Meghan Anand et. al., *All the Ways Congress Wants to Change Section 230*, SLATE (Mar. 23, 2021, 5:45 AM), https://slate.com/technology/2021/03/section-230-reform-legislative-tracker.html [https://perma.cc/K9M3-UVHG].

10. *Id.*

11. *See id.*

12. *See supra* notes 3-4 and accompanying text.

13. *See* discussion *infra* Section II.C.1.

14. Sean Illing, *Why "Fake News" Is an Antitrust Problem*, VOX (July 18, 2018, 9:00 AM), https://www.vox.com/technology/2017/9/22/16330008/eu-fines-google-amazon-monopoly-antitrust-regulation [https://perma.cc/7CFJ-CEFH].

15. *See* AM. PRESS INST., *Section 3: How People Decide What News to Trust on Digital Platforms and Social Media*, *in* A NEW UNDERSTANDING: WHAT MAKES PEOPLE TRUST AND RELY ON NEWS 14, 14-23 (2016) [hereinafter *How People Decide What News to Trust*], https://www.americanpressinstitute.org/wp-content/uploads/2016/04/What-Makes-People-Trust-and-Rely-on-News-Media-Insight-Project.pdf [https://perma.cc/C3AB-W6VF].

16. *See* discussion *infra* Section II.B.2.

early 2000s, tech giants like Meta, which owns Facebook;[17] Google, which owns YouTube;[18] and Amazon have amassed considerable influence, both economic and otherwise,[19] leaving many to ask whether U.S. antitrust laws need to catch up with the twenty-first century.[20]

One major area of antitrust law currently under scrutiny is Section 7 of the Clayton Antitrust Act and its case law,[21] which together provide the standards that agencies and courts use to decide whether a particular merger poses too great of a threat to consumers to permit its consummation.[22] Generally, this analysis involves weighing the post-merger level of market concentration,[23] often quantified into a Herfindahl–Hirschman Index ("HHI") value,[24] against any redeeming, procompetitive qualities of the merger to predict its probable effect on competition and therefore consumers.[25] In recent years, this approach's application has been criticized as overly deferential towards merging parties.[26]

Combined and compared side-by-side, the parallel reform movements behind Section 230 and Section 7 convene at the following conclusion: the unfettered spread of misinformation continues to pose a serious, present threat to public health and debate, but the remedy of Section 230 reform alone risks being too politically unpopular, too constitutionally vulnerable, or too regulatorily ineffective to await. Therefore, until these conditions change, Congress should prioritize antitrust reform and amend Section 7 by joint resolution to incorporate a bright-line HHI ceiling for the social media market to hinder market concentration, increase competition, and ultimately empower consumers to demand greater content scrutiny from their social media platforms.

To support this proposal, this Note first compares Section 230 and Section 7 in their respective regulatory, political, and constitutional contexts. Then, this Note argues that establishing an HHI ceiling for Section 7 merger

---

17. *See* Salvador Rodriguez, *Facebook Changes Company Name to Meta*, CNBC (Oct. 29, 2021, 8:56 AM), https://www.cnbc.com/2021/10/28/facebook-changes-company-name-to-meta.html [https://perma.cc/MJ5T-CY39].

18. *See Google Buys YouTube for $1.65 Billion*, NBC NEWS (Oct. 9, 2006, 11:54 AM), https://www.nbcnews.com/id/wbna15196982 [https://perma.cc/5TNK-2JZV].

19. *See* Sara Morrison & Shirin Ghaffary, *The Case Against Big Tech*, VOX (Dec. 8, 2021, 5:30 AM), https://www.vox.com/recode/22822916/big-tech-antitrust-monopoly-regulation [https://perma.cc/2U9S-LTP5].

20. *See* Steve Kovach, *Democrats and Republicans Disagree on How to Curb Big Tech's Power – Here's Where They Differ*, CNBC (Oct. 7, 2020, 12:50 PM), https://www.cnbc.com/2020/10/07/democrats-and-republicans-disagree-on-how-to-regulate-big-tech.html [https://perma.cc/G2U8-NKV5].

21. *See* STAFF OF H. SUBCOMM. ON ANTITRUST, COM., AND ADMIN. L. OF THE COMM. ON THE JUDICIARY, 116TH CONG., INVESTIGATION OF COMPETITION IN DIGITAL MARKETS 20-21 (Comm. Print 2020) [hereinafter INVESTIGATION OF COMPETITION IN DIGITAL MARKETS].

22. *See* discussion *infra* Section II.B.1.b.

23. *See infra* notes 104-10 and accompanying text.

24. *See infra* notes 105-06 and accompanying text.

25. *See infra* notes 111-14 and accompanying text.

26. *See* AURELIEN PORTUESE, INFO. TECH. & INNOVATION FOUND., REFORMING MERGER REVIEWS TO PRESERVE CREATIVE DESTRUCTION 2 (2021), https://www2.itif.org/2021-merger-reviews.pdf [https://perma.cc/ER2B-EX6D].

review is likely to both minimize misinformation's ill effects and provide a more reliable tool than Section 230 reform for combatting misinformation, at least until the political and constitutional context surrounding Section 230 shifts.

The background is divided into four parts. Section II.A explains how Section 230 protects social media firms from legal liability for misinformation and how the divisive politics of misinformation render changing Section 230 politically difficult. Section II.B discusses how Section 7 aligns social media firms' market incentives with consumers' preferences against misinformation and how antitrust politics are united towards increasing the regulation of social media firms. Section II.C highlights the stark disparity in constitutional scrutiny that reform options would endure to amend Section 230 under the demanding First Amendment and Section 7 under the permissive commerce clause. Section II.D briefly covers the typical business model of social media firms and how the social media market's economics renders it vulnerable to monopolization and suitable for antitrust regulation.

The analysis that follows is bifurcated and concludes by addressing rebuttals. Section III.A argues (1) that anti-misinformation Section 230 reform is unlikely to muster the political support required in Congress and (2) that even if it were to, Section 230 reform is likely to either be regulatorily counterproductive or constitutionally vulnerable. Section III.B then argues that Section 7 reform is not only constitutionally safe and politically popular but also capable of compelling social media firms to mitigate misinformation. At last, Section III.C concludes by addressing likely criticisms of the proposal within the context of a whole-of-government effort to mitigate misinformation wherever and whenever possible, within which the social media market's HHI ceiling exists as a humble but nonetheless valuable tool.

II. BACKGROUND

A. Section 230 and Misinformation Politics

1. Section 230's Law

Section 230 of the Communications Decency Act limits the liability of websites for their user-posted content and was passed in the early years of the Internet when courts differed on whether a website could be liable for such content.[27] Consider the tort of defamation, for example. Common law defamation possesses four elements:

27. Note, *Section 230 as First Amendment Rule*, 131 HARV. L. REV. 2027, 2029 (2018) (discussing the judicial history which led to "Congress enact[ing] [S]ection [230]").

> (a) a false and defamatory statement concerning another, (b) an unprivileged publication to a third party, (c) fault amounting at least to negligence on the part of the *publisher*; and (d) either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication.[28]

Because "publication" includes "intentionally and unreasonably fail[ing] to remove defamatory matter that [someone] knows to be . . . in his possession or under his control,"[29] whether a website could be held liable for defamatory content posted on its site by a third-party turned on whether the website was a "publisher,"[30] and this question divided courts.[31]

In *Cubby, Inc. v. CompuServe Inc.*, the Southern District of New York held an Internet service provider not liable for a third-party's defamatory post "because it had 'no more editorial control' than would 'a public library, book store, or newsstand' and therefore was a mere *distributor* that did not know or have reason to know of the content."[32] But in *Stratton Oakmont, Inc. v. Prodigy Servs.*, a New York state court held the owner of a website was "liable as a *publisher* of defamatory posts" because the owner possessed and "exercised 'editorial control' over offensive content" by electing to moderate such content.[33] Seeking to remedy this potentially perverse incentive for websites to turn a blind eye to their users' posts to avoid legal vulnerability as a publisher,[34] then-Congressmen Ron Wyden and Chris Cox proposed Section 230, framing it as a "'sword and shield' for Internet companies."[35] The sword empowered websites to moderate and censor without fear of liability, declaring that

> [n]o provider or user of an interactive computer service shall be held liable on account of . . . any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable . . . .[36]

The shield, on the other hand, protected websites from defamation liability by settling that "[n]o provider or user of an interactive computer service shall be

---

28. RESTATEMENT (SECOND) OF TORTS § 558 (AM. L. INST. 1977) (emphasis added).
29. RESTATEMENT (SECOND) OF TORTS § 577(2) (AM. L. INST. 1977).
30. Note, *supra* note 27, at 2029.
31. *See id.* (discussing the varying judicial application of publisher liability to websites).
32. *Id.* at 2028 (quoting Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 140-41 (S.D.N.Y. 1991)) (emphasis added).
33. *Id.* at 2029 (quoting Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710, at *4-5 (N.Y. Sup. Ct. May 24, 1995)) (emphasis added).
34. *See* Daisuke Wakabayashi, *Legal Shield for Social Media Is Targeted by Lawmakers*, N.Y. TIMES (Dec. 15, 2020), https://www.nytimes.com/2020/05/28/business/section-230-internet-speech.html [https://perma.cc/5MBU-8BBQ] ("[Wyden and Cox] were worried [publisher doctrine] would act as a disincentive for websites to take steps to block pornography and other obscene content.").
35. *Id.*
36. 47 U.S.C. § 230(c)(2)(A).

treated as the publisher or speaker of any information provided by another information content provider."[37]

Together, the sword and shield granted websites generous freedom in operating their platforms, and although it is impossible to know exactly what a world without Section 230 would have looked like, it remains undeniable that the Internet landscape we know today, dominated by giants such as Amazon, Apple, Facebook, and Google,[38] is a product of the protective legal environment Section 230 fostered.[39] However, Section 230's protection also ensured that websites were free to abide user-posted misinformation, and this consequence soon proved unpopular.[40]

2. Misinformation's Politics

Today, a bipartisan revolt has erupted against Section 230,[41] fueled by the view that social media firms no longer deserve the broad protections from liability that Section 230 provides them, and each party's grievance lies with either the sword or the shield.[42] "Conservatives claim that [the sword] gives tech companies a license to silence [conservative] speech," whereas "[l]iberals criticize [the shield] for giving platforms the freedom to profit from harmful speech and conduct."[43] This sword-and-shield framework helps illustrate the dynamic of the Section 230 debate, but it is also accurate to simply frame the debate as "a disagreement [over] the importance of allowing Americans to speak their minds."[44]

On the right, conservatives tend to disapprove of deplatforming individuals on account of their speech,[45] and some Republican state legislatures have gone so far as to "impos[e] fines on social media companies

37. 47 U.S.C. § 230(c)(1).

38. Chris Alcantara et al., *How Big Tech Got So Big: Hundreds of Acquisitions*, WASH. POST (Apr. 21, 2021), https://www.washingtonpost.com/technology/interactive/2021/amazon-apple-facebook-google-acquisitions/ [https://perma.cc/YLP7-QBW3] (describing the ubiquity of Amazon, Apple, Facebook, and Google in modern life).

39. *See Section 230 of the Communications Decency Act*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/cda230 [https://perma.cc/W75F-6MRN] (last visited Apr. 9, 2022) (explaining how Section 230 protections have allowed "user-generated websites" to "thrive," free from "potential liability for their users' actions").

40. *See* Marguerite Reardon, *Democrats and Republicans Agree That Section 230 Is Flawed*, CNET (June 21, 2020, 5:00 AM), https://www.cnet.com/news/democrats-and-republicans-agree-that-section-230-is-flawed/ [https://perma.cc/4TJC-M6Z7] ("Republicans and Democrats . . . have called for [Section 230] to be dismantled.").

41. *Id.*

42. *See* Danielle Keats Citron & Mary Anne Franks, *The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform*, 2020 U. CHI. LEGAL F. 45, 46-47 (2020).

43. *Id.*

44. Bakst & Carmack, *supra* note 7.

45. Colleen McClain & Monica Anderson, *Republicans, Democrats at Odds over Social Media Companies Banning Trump*, PEW RSCH. CTR. (Jan. 27, 2021), https://www.pewresearch.org/fact-tank/2021/01/27/republicans-democrats-at-odds-over-social-media-companies-banning-trump/ [https://perma.cc/55GZ-VYSH].

that . . . bar political candidates in th[at] state."[46] Notable examples include former President Trump's broad ban from multiple social media platforms following the January 6th insurrection and Representative Marjorie Taylor Greene's personal Twitter ban following her "repeated violations of [Twitter's] COVID-19 misinformation policy."[47]

On the left, liberals tend to support silencing or discrediting distributors of misinformation.[48] Misinformation—which is defined as "incorrect or misleading information," regardless of the speaker's mens rea[49]—has troubled liberals, who worry it weakens public confidence in the efficacy of public health measures and the validity of elections.[50] In fact, health care professionals have credited social media platforms, such as Facebook, with encouraging vaccine hesitancy by facilitating the spread of vaccine misinformation.[51] Facebook itself reported that misinformation is so rife on its platform that the United Nations Children's Fund ("UNICEF") and the World Health Organization "will not use [the] free ad [space]" Facebook

---

46. David McCabe, *Florida, in a First, Will Fine Social Media Companies That Bar Candidates*, N.Y. TIMES (May 24, 2021), https://www.nytimes.com/2021/05/24/technology/florida-twitter-facebook-ban-politicians.html [https://perma.cc/2E89-S6DS]; *see also Texas Passes Social Media 'De-Platforming' Law*, BBC NEWS (Sept. 10, 2021), https://www.bbc.com/news/technology-58516155 [https://perma.cc/ZF4Y-BT59].

47. Joe Hernandez, *Facebook Suspends Marjorie Taylor Greene's Account over COVID Misinformation*, NPR (Jan. 3, 2022, 6:55 PM), https://www.npr.org/2022/01/02/1069753102/twitter-bans-marjorie-taylor-greenes-personal-account-over-covid-misinformation [https://perma.cc/7R8Y-6QCF]; *see* Sarah Fischer & Ashley Gold, *All the Platforms That Have Banned or Restricted Trump So Far*, AXIOS (Jan. 11, 2021), https://www.axios.com/platforms-social-media-ban-restrict-trump-d9e44f3c-8366-4ba9-a8a1-7f3114f920f1.html [https://perma.cc/2TXR-ZLHL]; *see* Shannon Bond, *Facebook Ban on Donald Trump Will Hold, Social Network's Oversight Board Rules*, NPR (May 5, 2021, 11:36 AM), https://www.npr.org/2021/05/05/987679590/facebook-justified-in-banning-donald-trump-social-medias-oversight-board-rules [https://perma.cc/MXX6-BDYV].

48. *See* EMILY A. VOGELS ET AL., PEW RSCH. CTR., MOST AMERICANS THINK SOCIAL MEDIA SITES CENSOR POLITICAL VIEWPOINTS 4-6 (2020), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2020/08/PI_2020.08.19_social-media-politics_REPORT.pdf [https://perma.cc/LY3Y-KTJ7].

49. *Misinformation*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/misinformation [https://perma.cc/TZ6J-9DH6] (last visited Nov. 22, 2021); *see How to Address COVID-19 Vaccine Misinformation*, CDC, https://www.cdc.gov/vaccines/covid-19/health-departments/addressing-vaccine-misinformation.html [https://perma.cc/9Z93-LKRY] (last visited Nov. 22, 2021).

50. *See* Anna Edgerton, *Democrats Can't Force Facebook to Stem Covid Misinformation*, BLOOMBERG (July 20, 2021, 8:47 AM), https://www.bloomberg.com/news/articles/2021-07-20/democrats-can-t-make-facebook-help-win-the-covid-information-war [https://perma.cc/5LRQ-6PWL] ("Biden's struggle to control the coronavirus and vaccine misinformation online was evident in his broadside . . . that companies like Facebook . . . were 'killing people.'"); *see* Shirin Ghaffary, *Democratic Party Leaders Are "Banging Their Head Against the Wall" After Private Meetings with Facebook on Election Misinformation*, VOX (Oct 1, 2020, 4:20 PM), https://www.vox.com/recode/2020/10/1/21497453/facebook-democrats-2020-election-misinformation [https://perma.cc/83AK-4UB5] ("Democrats want to see Facebook more aggressively remove misinformation relating to the election.").

51. Hollingsworth, *supra* note 3.

provides "to promote pro-vaccine content, because they do not want to encourage the anti-vaccine commenters that swarm their [p]ages."[52]

Thus, because both political parties disagree over the source of Section 230's flaw, their ideas of how to remedy it are directly opposed, with one wishing to uncage speech and the other seeking to bind it. In contrast to the divisive politics and misinformative digital landscape Section 230 has generated, Section 7 has raised bipartisan political support for reform and actively combats the free flow of misinformation on social media.

B. Section 7 and the Antitrust Reform Movement

1. Section 7 Within the Broader Antitrust Law Context

To understand the relationship between Section 7 and misinformation, it is necessary to understand how Section 7 motivates firms to serve consumer preferences. Section 7 of the Clayton Antitrust Act is the statutory crux of antitrust-focused merger review,[53] the process whereby agencies and courts evaluate a merger, before or after its consummation, for antitrust concerns and decide whether to permit the merger to be consummated or not undone.[54] This Note focuses on antitrust-specific review ("merger review"), which is handled federally by the Department of Justice ("DOJ") and the Federal Trade Commission ("FTC"),[55] but many other bodies such as the FCC and the Committee on Foreign Investment in the United States ("CFIUS") may also review mergers to serve other interests, such as "the public interest, convenience, and necessity" or national security.[56]

Although conceptually straightforward, modern merger review proves to be a complex, ever-evolving task that requires parties to monitor market conditions,[57] case law,[58] and prevailing judicial attitudes to navigate its

52. Donie O'Sullivan et al., *Facebook Is Having a Tougher Time Managing Vaccine Misinformation Than It Is Letting On, Leaks Suggest*, CNN (Oct. 27, 2021, 10:56 AM), https://www.cnn.com/2021/10/26/tech/facebook-covid-vaccine-misinformation/index.html [https://perma.cc/L533-FLGZ].

53. *See* discussion *infra* Section II.B.1.b.

54. ANDREW GAVIL ET AL., ANTITRUST LAW IN PERSPECTIVE: CASES CONCEPTS AND PROBLEMS IN COMPETITION POLICY 671-74 (3d ed. 2017) (providing an introduction into merger review).

55. *Merger Review*, FTC, https://www.ftc.gov/news-events/topics/competition-enforcement/merger-review [https://perma.cc/Q5ME-5K35] (last visited Apr. 5, 2022).

56. *Overview of the FCC's Review of Significant Transactions*, FCC (July 10, 2014), https://www.fcc.gov/reports-research/guides/review-of-significant-transactions [https://perma.cc/X2LU-8EW8]; *The Committee on Foreign Investment in the United States (CFIUS)*, U.S. DEP'T OF TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius [https://perma.cc/MP2P-FPDA] (last visited Jan. 9, 2022).

57. *See infra* notes 107-10 and accompanying text.

58. GAVIL ET AL., *supra* note 54, at 672-74 (outlining the roles of different sections of the Sherman Antitrust Act, Clayton Antitrust Act, and Federal Trade Commission Act).

terrain.[59] To explain how Section 7 merger review empowers consumers, a brief overview of the goals and means of antitrust law is warranted.

a. Sherman Antitrust Act Foundation

U.S. antitrust law first arose to ensure markets prioritized consumer interests at a time when a small number of trusts came to dominate the U.S. economy.[60] The result was the 1890 Sherman Antitrust Act ("SAA"),[61] which prohibits "[e]very contract, combination . . . , or conspiracy, in restraint of trade," under Section One, and the conspired, attempted, or successful "monopoliz[ation]" of trade, under Section Two.[62] While fleshing-out these undefined offenses during the SAA's first decades, courts identified antitrust law's goals and enforcement tools.[63]

i. Section One and the Objective of Antitrust Law

Section One liability requires (1) concerted, (2) anticompetitive conduct,[64] and its case law settled antitrust law's goal of prioritizing consumer welfare.[65] Initially, the Supreme Court insisted on adhering to a plain reading of Section One's prohibition against *every* contract in restraint of trade,[66] but because "[e]very agreement concerning trade . . . [necessarily] restrains,"[67] the Court reversed course in 1911 in *Standard Oil Co. of N.J. v. United*

59. *Id.* at 68-78 (providing an overview of intellectual movements that inform antitrust law's goals and values).

60. John A. James, *Structural Change in American Manufacturing, 1850-1890*, 43 J. ECON. HIST. 433 (1983) ("At the time of the Civil War it was still essentially a county of small-scale enterprises, but with the emergence of large firms and concentrated national markets, that picture had changed radically by the end of the century.").

61. GAVIL ET AL., *supra* note 54, at 102.

62. 15 U.S.C. §§ 1-2 (emphases added).

63. *See* discussion *infra* Section II.B.1.a.i-ii.

64. S*ee, e.g.*, NCAA v. Alston, 141 S. Ct. 2141, 2167-68 (2021) (Kavanaugh, J., concurring) ("Price-fixing . . . is ordinarily a textbook antitrust problem because it extinguishes the free market in which individuals can otherwise obtain fair compensation for their work."); *see* 15 U.S.C. § 1.

65. *See infra* notes 70-72 and accompanying text; *see* Christine S. Wilson, Comm'r, FTC, Luncheon Keynote Address at George Mason Law Review 22nd Annual Antitrust Symposium: Antitrust at the Crossroads?, at 1 (Feb. 15, 2019), https://www.ftc.gov/system/files/documents/public_statements/1455663/welfare_standard_speech_-_cmr-wilson.pdf [https://perma.cc/AC5Z-E5BG] ("Under the consumer welfare standard, business conduct and mergers are evaluated to determine whether they harm consumers in any relevant market.").

66. United States v. Trans-Missouri Freight Ass'n, 166 U.S. 290, 312 (1897) ("The language of [Section One] includes every contract . . . in restraint of trade . . . . [A]s the very terms of the statute go, they apply to any contract of the nature described.").

67. Bd. of Trade of Chi. v. United States, 246 U.S. 231, 238 (1918) ("Every agreement concerning trade . . . restrains. To bind, to restrain, is of their very essence.").

States,[68] instead reading into "the language of Section [One]" "a reasonableness modification,"[69] known as the "rule of reason."[70]

This rule of reason asks "whether the restraint . . . promotes competition or . . . suppress[es] . . . competition," and this fact-intensive inquiry "ordinarily" requires investigating all the "facts peculiar to the business," such as the restraint's nature, probable or actual effect, history, and purpose.[71] By directing the rule of reason to serve competition, the Court had crowned "consumer welfare" as the sole, cognizable goal and beneficiary of antitrust law.[72] However, even armed with the consumer welfare standard, Section Two issues would expose to courts the limitations of relying on enforcement tools that wait until after an antitrust injury has been inflicted to intervene.[73]

ii. Section Two and the Limits of Ex Post Facto Intervention

Section Two liability requires (1) unilateral or concerted anticompetitive conduct and (2) "monopoly power,"[74] and its application exposed the dilemma caused by allowing monopolies to establish themselves before intervening.[75]

A fundamental assumption in mainstream economics is that firms seek to maximize their profits,[76] and because a firm's productive efficiency will generally increase with scale,[77] firms tend to have an incentive to grow their productive capacity and market share. Assuming sufficient price competition remains after the firm has grown, consumers will receive the newfound "surplus" from the increased productive efficiency in the form of lower prices, but once a firm grows beyond a certain size, perhaps a 90% market share, price competition is likely to be too weak to compel the monopolist to share its efficiency gains with consumers.[78] This dynamic is most readily

68. Standard Oil Co. of N.J. v. United States, 221 U.S. 1, 67 (1911) (distinguishing between the more literal construction of Section One from *Trans-Missouri Freight Ass'n.* from the "rule of reason" applied by the Court).

69. GAVIL ET AL., *supra* note 54, at 103.

70. *Id.*

71. *Bd. of Trade of Chi.*, 246 U.S. at 238.

72. *See* Wilson, *supra* note 65, at 1.

73. *See* discussion *infra* Section II.B.1.a.ii.

74. United States v. Microsoft Corp., 253 F.3d 34, 50 (D.C. Cir. 2001) ("[M]onopolization has two elements: '(1) the possession of monopoly power in the relevant market and (2) the willful acquisition or maintenance of that power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident.'" (quoting United States v. Grinnell Corp., 384 U.S. 563, 570-71 (1966))).

75. *See infra* notes 81-89 and accompanying text.

76. H.T. Koplin, *The Profit Maximization Assumption*, 15 OXFORD ECON. PAPERS 130, 130-31 (1963) (discussing the influence of the profit maximization assumption).

77. *Glossary of Statistical Terms: Economies of Scale*, OECD, https://stats.oecd.org/glossary/detail.asp?ID=3203 [https://perma.cc/38U4-4U7R] (last visited Jan. 8, 2022) ("Economies of scale refers to the phenomenon where the average costs per unit of output decrease with the increase in the scale or magnitude of the output being produced by a firm.").

78. *See* MAXWELL L. STEARNS ET AL., LAW AND ECONOMICS: PRIVATE AND PUBLIC 49-55 (2018).

understood in the context of price competition, but "[e]nhanced market power can also . . . manifest[] in non-price terms . . . that adversely affect customers, [such as] reduced product quality, reduced product variety, reduced service, or diminished innovation."[79] Regardless of the form of its manifestation, the inverse relationship between the *ability* from scale and the *incentive* from competition to cater to consumers' preferences informs Section Two doctrine.[80]

In 1945, the Second Circuit, acting in place of a disqualified Supreme Court,[81] faced a difficult decision in *United States v. Aluminum Co. of America.* The Department of Justice alleged, among other things, that the defendant, "Alcoa,"[82] the "single producer of 'virgin' [aluminum] ingots in the United States," was an unlawful monopoly because of its monopoly power alone.[83] On one hand, Alcoa had achieved a massive market share of "over ninety per cent,"[84] having crushed "at least one or two abortive attempts to enter the industry" by ensuring its supply always exceeded current demand.[85] On the other hand, actively restricting market supply had been affirmed to be anticompetitive behavior just five years prior in *United States v. Socony-Vacuum Oil Co.*,[86] and Alcoa had done the exact opposite by expanding its supply.[87]

Presented with these facts, the Second Circuit agonized that "Alcoa[] . . . was . . . a monopoly; indeed it ha[d] never been anything else," but "[t]he successful competitor, having been urged to compete, must not be turned upon [once] he wins."[88] Judge Hand himself unabashedly expressed his frustration at the legal and economic dilemma in an internal memo:

---

79. U.S. DEP'T OF JUST. & FED. TRADE COMM'N, HORIZONTAL MERGER GUIDELINES 2 (2010), https://www.ftc.gov/sites/default/files/attachments/mergers/100819hmg.pdf [https://perma.cc/5HMK-UCYE] [hereinafter HORIZONTAL MERGER GUIDELINES].

80. *See infra* notes 81-89 and accompanying text.

81. United States v. Aluminum Co. of America (*Alcoa*), 148 F.2d 416, 421 (2d Cir. 1945); *see also* 28 U.S.C. § 2109; *see generally* Lino A. Graglia, *Punished for Being Successful*, WALL ST. J. (Mar. 7, 1997, 12:26 AM), https://www.wsj.com/articles/SB857697229646440000 [https://perma.cc/KZ7G-K7XA] (explaining that the "the Supreme Court [was] unable to hear the government's appeal because [it] lack[ed] . . . a quorum" because "too many of the justices had worked on the case in their earlier careers").

82. *Alcoa*, 148 F.2d at 421.

83. *Id.* at 423.

84. *Id.*

85. *Id.* at 430-31.

86. United States v. Socony-Vacuum Oil Co., 310 U.S. 150, 220 (1940) ("The elimination of [crude oil overproduction] is no legal justification for [restricting market supply].").

87. *See Alcoa*, 148 F.2d at 430-31.

88. *Id.* at 430.

> [I]f we hold that [Alcoa] is not a monopoly, deliberately planned and maintained, everyone who does not get entangled . . . in the incredible nonsense that has emanated from the Supreme Court, will, quite rightly I think, write us down as asses. Wherever the line should be drawn, it must include a company such as this, if the [Sherman] Act is to be enforced.[89]

In the end despite the Circuit's concerns, it ruled against Alcoa,[90] arguing that "possession of unchallenged economic power deadens initiative" and "immunity from competition is a narcotic, and rivalry is a stimulant, to industrial progress."[91] Following this decision, it would seem as if the Second Circuit had adopted a no-fault monopolization standard for the whole U.S., but despite never being officially overturned, modern Section Two doctrine has rejected the no-fault standard, reaffirming the requirement of anticompetitive conduct.[92] As a result, possessing monopoly power is insufficient for a charge of monopolization; the defendant must also have "used [anticompetitive] acts to gain or sustain [it]."[93]

Today, Section Two anticompetitive conduct can be fulfilled by a variety of anticompetitive activities,[94] and "monopoly power" can be established where a firm has "the power to control prices or exclude competition."[95] However, by resolving the monopoly dilemma in favor of requiring anticompetitive conduct before permitting intervention, Section Two doctrine allows monopolies to still form so long as they grow lawfully or otherwise evade detection. Section 7 exists to limit the scope of this loophole.

b. Section 7's Law

By "arresting mergers . . . when the trend to[wards] [monopolization] . . . was still in its incipiency,"[96] Section 7 protects consumers by helping courts avoid difficult cases like *Aluminum Co. of America* from arising in the first

89. Marc Winerman & William Kovacic, *Learned Hand,* Alcoa*, and the Reluctant Application of the Sherman Act*, 79 ANTITRUST L.J. 295, 295-96, 296 n.2 (2013) (quoting an "undated pre-conference memo" physically on file at the Harvard Law School Library).

90. *Alcoa*, 148 F.2d at 448.

91. *Id.* at 427.

92. Otter Tail Power Co. v. United States, 410 U.S. 366, 377 (1973) ("Use of monopoly power 'to destroy threatened competition' is a violation . . . [Section] 2 of the Sherman Act.").

93. GAVIL ET AL., *supra* note 54, at 504.

94. *E.g., Microsoft Corp.*, 253 F.3d at 58, 64, 66, 85 (holding that Microsoft violated Section Two by "engaging in a variety of exclusionary acts . . . to maintain its monopoly," including "irremovably" "binding [Internet Explorer] to Windows"); *see also* JTC Petroleum Co. v. Piasa Motor Fuels, Inc., 190 F.3d 775, 779-80 (7th Cir. 1999) (permitting a Section Two claim to continue based on facts violative of Section One).

95. United States v. E.I. du Pont de Nemours & Co., 351 U.S. 377, 391 (1956).

96. Brown Shoe Co. v. United States, 370 U.S. 294, 317 (1962).

place.[97] Enacted in 1914, Section 7 of the Clayton Antitrust Act ("CAA") enjoins mergers "where . . . the effect of such acquisition[s] . . . *may* be substantially to lessen competition, or to tend to create a monopoly,"[98] and as the statutory language suggests, its legal standards are imprecise.[99] As a former general counsel to the FTC explained, "[i]n US merger policy, . . . goals have not always been constant, or consistent with each other, and our enforcement tools have not always been perfectly adapted to their tasks."[100] Therefore, the best way to understand Section 7's standards are as functions of evolving judicial attitudes towards the virtue of market intervention when armed with imperfect information but nonetheless asked to predict the future.

i. Merger Review Analytical Framework

Merger review operates on the "theory . . . that high market concentration can facilitate collusive behavior," the subject of Section One, and even grant "[monopoly] power," the subject of Section Two, which in either case enables firms to betray consumers.[101] The goal of Section 7 is to protect consumer welfare by preemptively depriving firms of the ability to engage in anticompetitive conduct at all.

Mergers come in three varieties: horizontal, vertical, [and] conglomerate.[102] "[H]orizontal mergers . . . involve sellers of substitutes, . . . vertical mergers . . . involve firms['] . . . suppliers [and] customers," and "[c]onglomerate mergers involve firms that sell neither substitutes nor complements."[103] For horizontal mergers, courts consider the post-merger market concentration and its distance from the pre-merger concentration.[104] Although courts could rely on a simple count of competitors or their market shares,[105] typically the DOJ and FTC will provide an HHI measurement, "calculated by summing the squares of the individual firms' market

97. *See* Debra A. Valentine, Assistant Dir. for Int'l Antitrust, Fed. Trade Comm'n, Prepared Remarks Before INDECOPI Conference: The Evolution of U.S. Merger Law (Aug. 13, 1996), https://www.ftc.gov/public-statements/1996/08/evolution-us-merger-law [https://perma.cc/632A-R285] ("[T]here is no doubt that Congress was concerned about the monopoly power of the great industrial trusts – it wanted to protect consumers and smaller firms from unfair use of that power.").

98. 15 U.S.C. § 18 (emphasis added).

99. *See* GAVIL ET AL., *supra* note 54, at 697-700 (detailing the various, conflicting authorities that attorneys must consider).

100. Valentine, *supra* note 97.

101. *Id.*

102. *See* GAVIL ET AL., *supra* note 54, at 671.

103. *Id.*; *see generally* Adam Hayes, *Cross Price Elasticity: Definition, Formula for Calculation, and Example*, INVESTOPEDIA, https://www.investopedia.com/terms/c/cross-elasticity-demand.asp [https://perma.cc/5BX7-HV4V] (last updated July 31, 2022) (explaining that substitutes are goods or services consumers may view as alternatives, such as Pepsi and Coke sodas, whereas complements are goods or services consumers may view as most useful together, such as peanut butter and jelly).

104. F.T.C. v. Penn State Hershey Med. Ctr., 838 F.3d 327, 346-47 (3d Cir. 2016).

105. GAVIL ET AL., *supra* note 54, at 766.

shares."[106] This first requires courts to consider the merger in the context of the relevant geographic market,[107] the relevant product market,[108] and the number and character of current and future possible market participants.[109] For example, in a defined market where two firms each have a fifty percent market share, the HHI would be 5,000, and the FTC and DOJ would designate that market as "Highly Concentrated" because its HHI value measured "above 2500."[110]

Next, courts will consider any mitigating factors that may overcome any anticompetitive concerns suggested by the market concentration, such as the presence of monopsonistic buyers,[111] low barriers to market entry for potential competitors,[112] and new productive efficiencies.[113] Finally, furnished with the anticompetitive and procompetitive considerations, courts weigh them to predict the merger's net-competitive effect for consumers.[114] Given the predictive nature of this final weighing, the analysis delegates a large degree of discretion to a judge's judicial attitude towards market intervention to tip the scales.[115]

ii. Judicial Attitudes Evolve

Judicial attitudes towards consumers' need for protection have varied over time and in response to those times. In 1962, the Supreme Court dictated in *Brown Shoe Co. v. United States* that "Congress used the words '*may* be substantially to lessen competition' . . . , to indicate that [Section 7's] concern was with *probabilities*, not certainties"[116] and that because Congress "appreciated that occasional higher costs and prices might result from the maintenance of fragmented industries and markets," newfound, post-merger

106. HORIZONTAL MERGER GUIDELINES, *supra* note 79, at 18.

107. United States v. Philadelphia Nat'l Bank, 374 U.S. 321, 334 (1963).

108. United States v. E.I. du Pont de Nemours & Co., 351 U.S. 377, 380-81 (1956) ("[W]hether the defendants control the price and competition in the market for such part of trade . . . depends upon . . . whether there is a cross-elasticity of demand between [the defendants' product and its substitutes].").

109. United States v. Waste Mgmt., Inc., 743 F.2d 976, 983 (2d Cir. 1984) ("[E]ntry into the relevant product and geographic market by new firms . . . in the Fort Worth area is so easy that any anti-competitive impact of the merger . . . would be eliminated . . . .").

110. HORIZONTAL MERGER GUIDELINES, *supra* note 79, at 19.

111. United States v. Baker Hughes Inc., 908 F.2d 981, 981-92 (D.C. Cir. 1990) (permitting a merger in the context of a powerful and limited number of buyers); *see also* HORIZONTAL MERGER GUIDELINES, *supra* note 79, at 27.

112. *Waste Mgmt., Inc.*, 743 F.2d at 983.

113. F.T.C. v. Procter & Gamble Co., 386 U.S. 568, 580 (1967) ("*Possible* economies cannot be used as a defense to illegality. Congress was aware that some mergers which lessen competition may also result in economies, but it struck the balance in favor of protecting competition.") (emphasis added).

114. *See* F.T.C. v. H.J. Heinz Co., 246 F.3d 708, 726-27 (D.C. Cir. 2001).

115. *See* discussion *infra* Section II.B.1.b.ii; *see also H.J. Heinz Co.*, 246 F.3d at 727 n.26 ("The most difficult mergers to assess may be those that . . . create[e] market power that increases the risk of oligopolistic pricing while at the same time creating efficiencies that reduce production or marketing costs." (quoting LAWRENCE A. SULLIVAN & WARREN S. GRIMES, THE LAW OF ANTITRUST: AN INTEGRATED HANDBOOK 511 (1st ed. 2000))).

116. Brown Shoe Co. v. United States, 370 U.S. 294, 323 (1962) (emphases added).

productive efficiencies were a non-cognizable mitigating factor.[117] Indeed in 1967, the Court reaffirmed that "[p]ossible economies [of scale] cannot be used as a defense,"[118] and upon this basis, the Court went on to enjoin mergers with post-merger market shares as low as five percent.[119]

However, the last time the Supreme Court decided a substantive Section 7 case was in 1974,[120] and since then the lower Circuits have mutinied and departed from its caselaw.[121] In the context of stagflation and increased foreign competition of the 1970s,[122] Circuits sought greater certainty of anticompetitive effects before enjoining mergers.[123] Procedurally, the plausibility standards adopted in *Matsushita Electric Industrial Co. v. Zenith Radio Corp.* and *Bell Atlantic Corp. v. Twombly* were procedural manifestations of courts' newfound hesitancy to intervene, and Circuits may have interpreted the Supreme Court's procedural holdings as tacit permission to diverge from its substantive holdings as well.[124] Since then, the FTC and DOJ have likewise updated their jointly published *Merger Guidelines*[125]—which provide notice of how they will analyze mergers[126]—to recognize productive efficiencies as a cognizable mitigating factor.[127] But today, attitudes are reversing once again.[128]

---

117. *Id.* at 344.

118. F.T.C. v. Procter & Gamble Co., 386 U.S. 568, 580 (1967).

119. United States v. Pabst Brewing Co., 384 U.S. 546, 550, 553 (1966).

120. GAVIL ET AL., *supra* note 54, at 697 ("[T]he trail of Supreme Court decisions interpreting the amended Section [7] begins with *Brown Shoe* in 1962 and effectively ends with *[United States v. General Dynamics, 415 U.S. 486]* in 1974 . . . . ").

121. *See infra* notes 122-24 and accompanying text.

122. Int'l Fin. Discussion Paper 799 The Great Inflation of the 1970s, at 2, 18-19 (Apr. 2004), https://www.federalreserve.gov/pubs/ifdp/2004/799/ifdp799.pdf [https://perma.cc/EW79-BAKV]; JOHN ZYSMAN & LAURA TYSON, AMERICAN INDUSTRY IN INTERNATIONAL COMPETITION: GOVERNMENT POLICIES AND CORPORATE STRATEGIES 15, 18 (1983) (discussing the "intense foreign competition" the United States began to face in the era following the Second World War).

123. *See* GAVIL ET AL., *supra* note 54, at 71-73, 440-41.

124. Matsushita Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 587 (1986) ("[I]f the factual context renders respondents' claim implausible—if the claim is one that simply makes no economic sense—respondents must [present] more persuasive evidence . . . than would otherwise be necessary."); Bell Atl. Corp. v. Twombly, 550 U.S. 544, 556 (2007) ("Asking for plausible grounds to infer an agreement . . . simply calls for enough fact to raise a reasonable expectation that discovery will reveal evidence of illegal agreement.").

125. *Mergers*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/mergers [https://perma.cc/G5CM-DDWE] (last visited Jan. 29, 2022).

126. GAVIL ET AL., *supra* note 54, at 719 ("The Merger Guidelines . . . describe how the Justice Department and Federal Trade Commission will exercise their prosecutorial discretion . . . , not . . . the applicable legal standard that should or would be applied by a court."); HORIZONTAL MERGER GUIDELINES, *supra* note 79, at 1 ("These Guidelines describe the principal analytical techniques . . . on which the Agencies usually rely . . . .").

127. HORIZONTAL MERGER GUIDELINES, *supra* note 79, at 29-31.

128. *See* discussion *infra* Section II.B.2.

2. The Antitrust Reform Movement

Today, a sense that too much faith has been placed in efficiency's ability to counterbalance increased market concentration has arisen, and a bipartisan movement has coalesced to respond.[129] Technology markets have become increasingly concentrated in the hands of a few, large corporations,[130] and ongoing litigation alleges that at least one of these giants unlawfully guarded their newfound monopoly power.[131] In the ongoing case of *FTC v. Facebook, Inc.*, the FTC seeks Facebook's dissolution to answer for its alleged monopolization strategy of "maintain[ing] its dominant position by acquiring companies that could emerge as or aid competitive threats," such as Instagram and WhatsApp,[132] a policy its CEO, Mark Zuckerberg, summarized in 2008 as "it is better to buy than compete."[133] Following *Citizens United v. FEC*, such firms' ability to translate their economic power into political influence through campaign contributions came under the protection of the First Amendment,[134] permitting Facebook alone to spend almost twenty million dollars on lobbying in 2020.[135]

In response, the FTC withdrew its support of the *Vertical Merger Guidelines* on the basis that it "contravened the Clayton Act's [nonexistent] language with [regard] to efficiencies,"[136] and the DOJ followed suit.[137] Both agencies have even "launched a joint public inquiry" to "seek[] comments . . . to inform potential revisions to the [Horizontal] guidelines" as well.[138]

In Congress, Democrats and Republicans now share "broad agreement that Big Tech wields too much power in the market and that government needs

---

129. *See* discussion *infra* Section II.B.2.

130. *See* Jasper Jolly, *Is Big Tech Now Just Too Big to Stomach?*, THE GUARDIAN (Feb. 6, 2021, 3:00 AM), https://www.theguardian.com/business/2021/feb/06/is-big-tech-now-just-too-big-to-stomach [https://perma.cc/76W9-3KBR].

131. First Amended Complaint at 1-2, F.T.C. v. Facebook, Inc., 581 F. Supp. 3d 34 (D.D.C. 2022) (No. 1:20-cv-03590-JEB).

132. *Id.*

133. *Id.*

134. *See* Citizens United v. FEC, 558 U.S. 310, 353 (2010) ("There is simply no support for the view that the First Amendment . . . permit[s] the suppression of political speech by media corporations."); *see* JANE CHUNG, PUB. CITIZEN, BIG TECH, BIG CASH: WASHINGTON'S NEW POWER PLAYERS 7-13 (2021), https://www.citizen.org/wp-content/uploads/Big-Tech-Big-Cash-Washingtons-New-Power-Players.pdf [https://perma.cc/X47W-TT8P].

135. *See* CHUNG, *supra* note 134, at 8.

136. Press Release, Fed. Trade Comm'n, Federal Trade Commission Withdraws Vertical Merger Guidelines and Commentary (Sept. 15, 2021), https://www.ftc.gov/news-events/press-releases/2021/09/federal-trade-commission-withdraws-vertical-merger-guidelines [https://perma.cc/45YF-MLNF].

137. Jonathan Kanter, Assistant Att'y Gen., U.S. Dep't of Just. Antitrust Div., Remarks at FTC Press Conference Announcing Call for Public Comment: Modern Competition Challenges Require Modern Merger Guidelines, at 1-5 (Jan. 18, 2022), https://www.justice.gov/opa/speech/file/1463546/download [https://perma.cc/CS9B-MNHE].

138. Press Release, Fed. Trade Comm'n, Federal Trade Commission and Justice Department Seek to Strengthen Enforcement Against Illegal Mergers (Jan. 18, 2022), https://www.ftc.gov/news-events/press-releases/2022/01/ftc-and-justice-department-seek-to-strengthen-enforcement-against-illegal-mergers [https://perma.cc/R9S9-6D9P].

to put more restrictions in place."[139] On the right, conservatives again claim that "social media platforms like [Meta's] Facebook and Google's YouTube [unfairly] discriminate against conservative viewpoints."[140] On the left, liberals criticize social media firms as notable bad actors within a broader, economy-wide monopoly problem.[141]

Nonetheless, the left and right have found considerable common ground as to goals and solutions. In 2020, the House Judiciary Subcommittee on Antitrust published a bipartisan report that claimed Apple, Google, Amazon, and Meta possessed monopoly power in their respective markets and that at least Amazon and Facebook have engaged in exclusive dealing and predatory mergers to maintain it.[142] The report also offered remedial proposals such as establishing a "[p]resumptive prohibition against future mergers and acquisitions by the dominant platforms," "[s]trengthening Section [7] of the Clayton Act [by] restoring presumptions and bright-line rules," and "overriding problematic precedents in the case law."[143]

In the Senate, Democratic Senator Amy Klobuchar has teamed up with Senate Republicans Chuck Grassley and Tom Cotton to sponsor a number of antitrust bills,[144] which would prohibit dominant firms from using their monopoly power to "[b]ias[] search results in favor of [themselves],"[145] "shift the burden of proof to [the party] that wishes to buy or merge with another to show [the merger is] not anticompetitive,"[146] and otherwise complement other House proposals.[147] Therefore, politically, both parties appear willing to

---

139. Kovach, *supra* note 20.

140. *Id.*

141. *See* Press Release, Amy Klobuchar, Senator, Senator Klobuchar Introduces Sweeping Bill to Promote Competition and Improve Antitrust Enforcement (Feb. 4, 2021) [hereinafter Senator Klobuchar Introduces Sweeping Bill], https://www.klobuchar.senate.gov/public/index.cfm/2021/2/senator-klobuchar-introduces-sweeping-bill-to-promote-competition-and-improve-antitrust-enforcement [https://perma.cc/CZ3A-B8X8].

142. Kovach, *supra* note 20.

143. INVESTIGATION OF COMPETITION IN DIGITAL MARKETS, *supra* note 21, at 20-21.

144. *See* Senator Klobuchar Introduces Sweeping Bill, *supra* note 141; *see* Ashley Gold, *New Klobuchar, Cotton Bill Could Block Big Tech Mergers*, AXIOS (Nov. 5, 2021), https://www.axios.com/klobuchar-cotton-big-tech-antitrust-bill-535d9df6-5b39-4e75-b6d8-13f30c21f3cf.html [https://perma.cc/S2WB-4AWW]; *see* Press Release, Amy Klobuchar, Senator, Klobuchar, Grassley, Colleagues to Introduce Bipartisan Legislation to Rein in Big Tech (Oct. 14, 2021) [hereinafter Klobuchar, Grassley, Colleagues to Introduce Bipartisan Legislation], https://www.klobuchar.senate.gov/public/index.cfm/2021/10/klobuchar-grassley-colleagues-to-introduce-bipartisan-legislation-to-rein-in-big-tech [https://perma.cc/H23V-7MFV]; *see* Ryan Tracy & John D. McKinnon, *Antitrust Tech Bills Gain Bipartisan Momentum in Senate*, WALL ST. J. (Nov. 25, 2021, 5:30 AM), https://www.wsj.com/articles/antitrust-tech-bills-gain-bipartisan-momentum-in-senate-11637836202 [https://perma.cc/H2QT-577X].

145. Klobuchar, Grassley, Colleagues to Introduce Bipartisan Legislation, *supra* note 144.

146. Gold, *supra* note 144.

147. Lauren Feiner, *Lawmakers Unveil Major Bipartisan Antitrust Reforms That Could Reshape Amazon, Apple, Facebook and Google*, CNBC (Dec. 13 2021, 1:35 PM), https://www.cnbc.com/2021/06/11/amazon-apple-facebook-and-google-targeted-in-bipartisan-antitrust-reform-bills.html [https://perma.cc/JV27-XXS5].

regulate social media firms if it means eroding their economic or political influence.[148] The question is how to do so without offending the Constitution.

C. Constitutionality of Regulating Markets and Speech

In addition to determining whether Section 230 and Section 7 reform will improve upon the status quo and whether it is politically popular, it is necessary to assess whether the Constitution will permit it.

1. Speech Regulation and the First Amendment

As a general rule, the First Amendment bars speech regulation by prohibiting any "law . . . abridging the freedom of speech, or of the press,"[149] although various exceptions exist,[150] such as for defamation,[151] some compelled speech,[152] some commercial speech,[153] and other categories less relevant to this Note.[154]

To avail itself of defamation, discussed in greater detail above,[155] Congress need only revoke Section 230 to resubject websites to potential liability as publishers.[156] But even so, as a constitutional matter, "public official[s]" cannot "recover[] damages for . . . defamat[ion] . . . unless . . . the statement was made with 'actual malice'—that is, . . . knowledge that it was false or with reckless disregard [for the truth],"[157] and in "matter[s] of public concern, . . . even a private figure must show actual malice in order to recover presumed . . . or punitive damages."[158]

To instead actively require websites to remove misinformation or at least flag it for readers, Congress would have to satisfy the more demanding constitutional requirements for compelling speech or controlling commercial speech.[159]

For instance, in *National Institute of Family and Life Advocates. v. Becerra*, the Supreme Court held that compelling unlicensed crisis pregnancy centers to "provide a government-drafted notice, [that] stat[ed] that '[the]

148. *See* discussion *supra* Section II.B.2.

149. U.S. CONST. amend. I.

150. KATHLEEN ANN RUANE, CONG. RSCH. SERV., 95-815, FREEDOM OF SPEECH AND PRESS: EXCEPTIONS TO THE FIRST AMENDMENT 1-35 (2014) (providing a broad overview of the basics of First Amendment doctrine).

151. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 301-02 (1964) ("The imposition of liability for private defamation does not abridge the freedom of public speech or any other freedom protected by the First Amendment.") (Goldberg J., concurring).

152. *See infra* notes 160-62 and accompanying text.

153. *See infra* notes 163-65 and accompanying text.

154. *See* RUANE, *supra* note 150, at 1-35.

155. *See supra* notes 28-33 and accompanying text.

156. *See supra* notes 34-37 and accompanying text.

157. *Sullivan*, 376 U.S. at 279-80.

158. RUANE, *supra* note 150, at 21 (citing Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974)); *see* Gertz v. Robert Welch, Inc., 418 U.S. 323, 323-24 (1974).

159. *See infra* notes 160-65 and accompanying text.

facility [wa]s not licensed as a medical facility by the State of California,'"[160] likely violated the First Amendment because it "alter[ed] the content of [their] speech,"[161] and crucially, "regulations [that] 'target speech based on its . . . content . . . are presumptively unconstitutional and . . . justif[iable] only [when] *narrowly tailored* to serve *compelling state interests*.'"[162]

Alternatively, Congress could argue that mandating the censorship or flagging of misinformation is merely the regulation of *commercial* speech, which needs only (1) "concern lawful activity and not be misleading," (2) implement a "substantial" "government interest," (3) "directly advance[] the government interest," and (4) be no "more extensive than . . . necessary . . . ."[163] But a platform's decision regarding how to treat a user's post would strain to be construed as commercial speech, "speech which does 'no more than propose a commercial transaction.'"[164] Consequently, constitutional policy seems to be placing its faith in "preserv[ing] an uninhibited marketplace of ideas in which truth will [hopefully] ultimately prevail."[165]

2. Market Regulation and the Commerce Clause

In contrast to speech regulation, market regulation enjoys relatively permissive constitutional standards under the commerce clause, which only requires that Congress have a "rational basis" for believing the economic activity regulated, when "taken in the aggregate, substantially affect[s] interstate commerce."[166] Therefore, regulation that is framed as speech regulation faces far more constitutional scrutiny than regulation framed as market regulation, and importantly, such market regulation is regulatorily common and justified on the basis of rectifying market failures, such as network effects.[167]

D. Social Media Market's Network Effect

Because this Note considers how competition impacts social media firms as conductors of misinformation, it is worth taking a moment to discuss the nature of the social media market as a platform market. Platform markets are characterized by the presence of "platform" firms that facilitate transactions between two parties by bringing them together in exchange for a

160. Nat'l Inst. of Fam. & Life Advocs. v. Becerra (*NIFLA*), 138 S. Ct. 2361, 2370 (2018) (quoting CAL. HEALTH & SAFETY CODE § 123472(b)(1) (West 2018)).

161. *Id.* at 2365 (quoting Riley v. Nat'l Fed'n of the Blind of N.C., Inc., 487 U.S. 781, 795 (1988)) (second alteration in original).

162. *Id.* at 2371 (quoting Reed v. Town of Gilbert, 576 U.S. 155, 163 (2015)) (emphases added).

163. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 566 (1980).

164. Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 64-66 (1983) (quoting Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 762 (1973)).

165. *NIFLA*, 138 S. Ct. at 2366 (quoting McCullen v. Coakley, 573 U.S. 464, 476 (2014)).

166. Gonzales v. Raich, 545 U.S. 1, 2 (2005) (citing United States v. Lopez, 514 U.S. 549, 557 (1995)).

167. *See* STEPHEN BREYER, REGULATION AND ITS REFORM 15-35 (1982).

fee from one or both parties.[168] The more parties a platform can gather on one side, the greater the value the platform has for the other side.[169] Take credit cards for example. Merchants naturally prefer to deal with a credit card company only when many of their customers will use that card, and likewise, customers naturally prefer to hold a credit card only when the stores they frequent accept that card.[170]

This relationship between the popularity and value of a platform is known as the "network effect," and it can help a monopolist entrench its monopoly power by giving consumers another reason to avoid smaller platforms.[171] Additionally, once a network has entrenched itself, Sherman Antitrust Act action provides a poorer remedy because both sides of the platforms are consumers, so the complex, if not contradictory, interests of "both sides of the platform" must be considered[172] before assessing "as a whole" "[]competitive effects."[173] If not by legal intervention, the only way to overcome the network effect and dislodge the monopolist is for a rival platform to achieve a discount, quality, or innovation "leap[]" that finally motivates consumers to migrate to its platform instead.[174]

Social media firms qualify as platforms because they typically unite non-paying users and paying advertisers; users seek the content they enjoy, and advertisers seek the users most likely to act upon their advertisements.[175] For example, Facebook's service as a platform is to observe its users' browsing habits, categorize their interests, and sell to advertisers the service of connecting them to the appropriate users.[176] When users seek to connect with friends or family, it remains far simpler to endure one platform than

168. GAVIL ET AL., *supra* note 54, at 622-25.

169. *Id.*

170. *See* United States v. Visa U.S.A., Inc., 344 F.3d 229, 234-36 (2d Cir. 2003) (describing the relationship between cardholders, merchants, and banks within the "General Purpose Payment Card Industry"); GAVIL ET AL., *supra* note 54, at 622 ("[M]erchants are more likely to accept a payment system's card the greater its number of cardholders, and cardholders are more likely to obtain a card the greater the number of merchants that accept it.").

171. *See* GAVIL ET AL., *supra* note 54, at 622 ("'Network effects' arise when the value of a product to a buyer depends on the number of other users. Communication systems are an example: a telephone is more valuable the more [people] you can call.").

172. Ohio v. Am. Express Co., 138 S. Ct. 2274, 2286 (2018).

173. *Id.* at 2287.

174. GAVIL ET AL., *supra* note 54, at 1100 ("To dislodge an industry leader in a market with strong network effects . . . the entrant may need to develop a dramatically improved product that 'leapfrogs' the market leader's technology.").

175. *See Social Media Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/social-media/ [https://perma.cc/4U89-8399]; *see, e.g.*, Greg McFarlane, *How Facebook (Meta), Twitter, Social Media Make Money from You*, INVESTOPEDIA, https://www.investopedia.com/stock-analysis/032114/how-facebook-twitter-social-media-make-money-you-twtr-lnkd-fb-goog.aspx#:~:text=The%20primary%20way%20social%20media,before%20social%20media%20companies%20existed [https://perma.cc/3ZWJ-JYQ4] (last updated Nov. 04, 2021).

176. Mark Zuckerberg, *Understanding Facebook's Business Model*, META (Jan. 24, 2019), https://about.fb.com/news/2019/01/understanding-facebooks-business-model/ [https://perma.cc/LF6T-TUY5].

convince their entire social circle to migrate to another.[177] Thus, the social media market as a platform market is especially vulnerable to monopolization and a strong candidate for market correction.

Now, having unpacked some of the legal and economic causes for misinformation's unfettered spread on social media and having considered the political and constitutional hurdles to statutory reform, the final step is to ask: assuming the political and constitutional background will persist unchanged for the foreseeable future, what can be done right now to mitigate misinformation?

III. ANALYSIS

A. Difficulty of Section 230 Reform

1. Proponents of Section 230 Reform Pursue Politically Irreconcilable Goals

The first hurdle for Section 230 reform is political feasibility. Although both parties share a general discontent with Section 230, Republicans and Democrats seek mutually exclusive ends; the left wishes to regulate speech by requiring websites to moderate misinformation, and the right wants to deregulate speech by prohibiting websites from moderating speech.[178] Therefore, because their goals exist in opposite directions from the status quo, future changes to Section 230 are unlikely to include provisions that might address platforms' legal permission to abide misinformation on their websites.

2. Amending Section 230 Risks Constitutional Criticism or Ensures Regulatory Regression

The second hurdle for anti-misinformation Section 230 reform is ensuring the change from the status quo both works as a regulatory tool and survives constitutional scrutiny. The simplest way to remove websites' liability shield is to revoke Section 230 entirely. Websites would once again be vulnerable to defamation liability, which is constitutionally sound,[179] and the Internet would revert to the pre-Section 230 status quo.[180] But platforms would regain the perverse incentive to avoid moderating their platform's third-party content,[181] or simply opt to disallow user-posted content entirely.

177. *See* Lydia Emmanouilidou & Brandi Fullwood, *We Asked Listeners Why They Can't Quit Facebook. Here's What You Said*, WORLD (Feb. 4, 2019, 2:00 PM), https://theworld.org/stories/2019-02-04/we-asked-listeners-why-they-cant-quit-facebook-heres-what-you-said [https://perma.cc/4Y3Q-NKHS] (reporting reasons why users of Facebook chose not to leave the platform).

178. *See* discussion *supra* Section II.A.2.

179. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 301-02 (1964).

180. *See* discussion *supra* Section II.A.1.

181. *See* discussion *supra* Section II.A.1.

This result would not only be counterproductive but also deprive users the benefits of access to social media.[182]

Given liberals' desire to actively minimize misinformation,[183] and conservatives' desire to embolden speech,[184] reform could also include changes beyond mere revocation. For instance, Congress could pass a statute that simply imposes a duty on websites to ensure its content does not include misinformation. This change would directly address the misinformation problem, but it could very well violate the First Amendment and the "marketplace of ideas" ideal it endorses.[185] Specifically, any statute that compels social media platforms to permit, disclaim, or remove misinformative posts risks being challenged as content-altering, compelled speech of the platform, just as the mandated disclosure was in *National Institute of Family and Life Advocates. v. Becerra*.[186]

Thus, successfully reforming Section 230 to tackle misinformation as speech is a tall order. The task raises the political support of the left but evokes deep suspicion from the right and,[187] depending on Congress' legislative approach, either restores the pre-Section 230 risk of legal liability for platforms' censorship of misinformation or risks invalidation of the statute under the First Amendment.[188] If, however, misinformation is tackled as a symptom of a market failure in need of correction under Section 7, the political, regulatory, and constitutional hurdles shrink considerably.[189]

B. Viability of Section 7 Reform

1. Amending Section 7 Enjoys Constitutional Permission and Bipartisan Appeal

In contrast to Section 230 reform, amending Section 7 to include a bright-line Herfindahl-Hirschman Index ceiling for the social media market would enjoy the permissive constitutional scrutiny of the commerce clause and the warmer reception of both political parties, given their desire to erode the economic or political influence of large social media firms.[190]

182. *See, e.g.*, *Is Social Media Good for Society?*, PROCON.ORG, https://socialnetworking.procon.org/ [https://perma.cc/UXG4-RTXU] (last updated Nov. 18, 2022).

183. *See supra* notes 43, 48-50 and accompanying text.

184. *See supra* notes 43, 45-47 and accompanying text.

185. Nat'l Inst. of Fam. & Life Advocs. v. Becerra, 138 S. Ct. 2361, 2366 (2018) (quoting McCullen v. Coakley, 573 U.S. 464, 476 (2014)).

186. *See supra* notes 160-62 and accompanying text.

187. *See* discussion *supra* Section II.A.2.

188. *See* discussion *supra* Sections II.A.1, II.C.1.

189. *See* discussion *infra* Section II.D.

190. *See* discussion *supra* Section II.B.2.

Constitutionally, the Clayton Antitrust Act already avows authority from the commerce clause,[191] and a market-specific HHI ceiling would likewise satisfy its requirements. Congress would be readily able to argue, if challenged, that it had a "rational basis" for believing that the merging of social media firms, when "taken in the aggregate, substantially affect[s] interstate commerce,"[192] insofar as those firms may have a nationwide presence and facilitate online advertising.[193]

Politically, both parties share an interest in weakening the power of social media firms, economically or otherwise,[194] and preventing further concentration or reconcentration is one such method of diminishing their individual influence over online speech.[195] Of course, both parties might disagree over the precise value at which to set the HHI ceiling, but they could at least agree that some minimum is appropriate. As such, the parties' goals are at least in the same direction from the status quo, even if not equal in distance.

This unidimensional dynamic is to be expected because economic regulation commonly bears witness to it.[196] Economic regulation tends to garner broad support at some minimum level because it is "extremely difficult to insure against" the "vagaries of the business cycle,"[197] and capitalism is more palatable when "citizens participate together in risk-reducing arrangements."[198] Economic regulation tackles all sorts of market failures, such as externalities, inadequate information, and, yes, monopolies and cartels.[199] In each case, "[t]he justification for intervention arises out of an alleged inability of the marketplace to deal with particular structural problems."[200] In the case of misinformation and social media platforms, if left unchecked, monopolies in social media will inevitably arise at one point or another and fail to provide consumers the level of content moderation they desire.

---

191. Clayton Antitrust Act of 1914, Pub. L. No. 63-212, § 1(a), 38 Stat. 730, 730 (1914) (codified at 15 U.S.C. § 12(a)) (taking care to define "'[c]ommerce' as . . . trade or commerce among the several States and with foreign nations . . . .").

192. Gonzales v. Raich, 545 U.S. 1, 2 (2005) (citing United States v. Lopez, 514 U.S. 549, 557 (1995)).

193. *See, e.g.*, *Social Media Fact Sheet*, *supra* note 175; *see e.g.*, McFarlane, *supra* note 175.

194. *See* discussion *supra* Section II.B.2.

195. *See* discussion *infra* Section VI.B. III.B.2.

196. *See infra* notes 197-200 and accompanying text.

197. Theodore R. Marmor & Jerry L. Mashaw, *The Case for Social Insurance*, *in* THE NEW MAJORITY: TOWARD A POPULAR PROGRESSIVE POLITICS 78, 78 (Stanley B. Greenberg & Theda Skocpol, eds., 1997).

198. *Id.* at 78-79.

199. BREYER, *supra* note 167, at 15-35.

200. *Id.* at 15.

2. Strengthening Section 7 Mitigates the Harms of Misinformation

The most important question is whether establishing an HHI ceiling in the social media market will in fact mitigate misinformation's negative effects. Although there are limits to Section 7's ability to control social media firms' misinformation policies by influencing their market incentives, amending Section 7 can still make a worthwhile contribution.

An HHI ceiling can mitigate misinformation because consumers of news prefer sources they trust and respect.[201] Without a competitive market, social media firms have little incentive to provide the moderation necessary to receive the public's trust and respect. Televised news is analogous. Presented with a choice, consumers turn to the channel they trust and respect,[202] but if a consumer is unable to verify the validity of news and cannot access another source, for example when at a diner or airport that only airs one news station, then the viewer may simply have to rely on the news-source she can access.

Although the incentive for social media firms to respond to consumer preferences is currently weaker than it would be in a more competitive market, it is still visible. The practice of deplatforming is one example. When a personality's use of a platform becomes overly offensive to the sensibilities of a majority of users, platforms sometimes deplatform the personality to disassociate themselves and satisfy their broader user base.[203] In a similar vein, Twitter's practice of adding warnings to misinformative posts displays the same purpose.[204] Younger readers may even be familiar with YouTube's "Adpocalypse,"[205] where upon "learning [that] their ads [were] appearing on YouTube next to videos espousing racist and anti-Semitic views," companies such as "Wal-Mart, PepsiCo, Starbucks, [and] General Motors" pulled many of their ads from the platform.[206] In response, YouTube enacted broad measures to ensure hate speech received no revenue from YouTube.[207] The

201. *How People Decide What News to Trust*, *supra* note 15, at 14-27.

202. *See* Amy Mitchell et al., *Loyalty and Source Attention*, *in* PEW RSCH. CTR., THE MODERN CONSUMER: NEWS ATTITUDES AND PRACTICES IN THE DIGITAL ERA 8-10, 12-14 (2016), https://www.pewresearch.org/journalism/wp-content/uploads/sites/8/2016/07/PJ_2016.07.07_Modern-News-Consumer_FINAL.pdf [https://perma.cc/VZ49-QSV7].

203. *See* Hernandez, *supra* note 47; *see* Fischer & Gold, *supra* note 47; *see* Bond, *supra* note 47.

204. *See COVID-19 Misleading Information Policy*, TWITTER, https://help.twitter.com/en/rules-and-policies/medical-misinformation-policy [https://perma.cc/P3E3-RPKD] (last visited Apr. 8, 2022).

205. Rachel Dunphy, *Can YouTube Survive the Adpocalypse?*, N.Y. MAG. (Dec. 28, 2017), https://nymag.com/intelligencer/2017/12/can-youtube-survive-the-adpocalypse.html [https://perma.cc/QR5Q-R4CH].

206. Ian Sherr, *Wal-Mart, PepsiCo and Dish Pull YouTube Ads over Hateful Videos*, CNET (Mar. 24, 2017, 8:57 PM), https://www.cnet.com/news/wal-mart-pepsi-and-dish-pull-youtube-ads-over-hateful-videos-google-alphabet-antisemitism/ [https://perma.cc/N4L6-7HUA].

207. *See* Dunphy, *supra* note 205.

goal of the HHI ceiling is to strengthen that market incentive to cater to consumers' preferences regarding misinformation.

By forbidding future increases in market concentration or reconcentration through stringent Section 7 merger review, new competitors will be given the breathing space needed to develop and compete, including over the quality of the news sharing they facilitate. Without the ability to maintain their monopoly power by mergers, monopolies will inevitably fall because in anticompetitive markets, antitrust enforcers can seek divestiture remedies, as it does against Facebook today and did against Microsoft in 2001.[208] In competitive markets, monopolies still suffer from "deaden[ed] initiative,"[209] and they eventually rise and fall in the dynamic environment of competition.[210]

Once freed from the "unchallenged economic power" that "deadens initiative" and delays "industrial progress,"[211] the social media market may even develop and discover more effective tools for identifying and neutralizing misinformation on their platforms. The FTC and DOJ assert that "[c]ompetition . . . spurs firms to innovate,"[212] and in its absence, we cannot know what anti-misinformation policies or tools consumers have been denied, from yet discovered or developed sorting algorithms to artificial intelligence.[213]

C. Section 7 Reform's Role Within Whole-of-Government Action

Implementing an HHI ceiling should be viewed as one aspect of a whole-of-government action plan. Although an HHI ceiling would improve upon the present, it has certain limitations, which, while not outweighing its benefits, do highlight the opportunity for fruitful, non-mutually exclusive supplementation.

First, an HHI ceiling would not constitute a panacea for misinformation. For one, social media is not the sole source of misinformation. Radio and podcasts have been labeled the "Wild West of the airwaves" for providing speakers who have already been excluded from other

208. First Amended Complaint at 1-2, F.T.C. v. Facebook, Inc., 581 F. Supp. 3d 34 (D.D.C. 2022) (No. 1:20-cv-03590-JEB); *see* United States v. Microsoft Corp., 253 F.3d 34, 105-07 (D.C. Cir. 2001) (reversing and remanding the question of divestiture as a remedy for Microsoft's violation of Section Two).

209. United States v. Aluminum Co. of America (*Alcoa*), 148 F.2d 416, 427 (2d Cir. 1945).

210. Rick Newman, *10 Great Companies That Lost Their Edge*, U.S. NEWS & WORLD REP. (Aug. 19, 2010, 10:39 AM), https://money.usnews.com/money/blogs/flowchart/2010/08/19/10-great-companies-that-lost-their-edge [https://perma.cc/G43R-8SMU] (listing popular businesses that lost economic relevance over time).

211. *Alcoa*, 148 F.2d at 427.

212. HORIZONTAL MERGER GUIDELINES, *supra* note 79, at 23.

213. *See* Katarina Kertysova, *Artificial Intelligence and Disinformation*, 29 SEC. & HUM. RTS. 55, 55-60 (2018) (discussing possible use of artificial intelligence to combat misinformation).

more scrutable platforms a voice.[214] Nor are mainstream news outlets and politicians immune from spreading misinformation either. News networks have televised misleading information on occasion,[215] and politicians have wielded the credibility of their offices to tout less than truthful claims.[216] And if the competitive social media market were to come to resemble traditional news networks, then much like with traditional news, the consumer and the provider will be free to consume and circulate misinformation in accordance with their preferences, and in all likelihood a significant number will.

Nonetheless, such a world is preferable to the present and preferable to waiting for misinformation-focused Section 230 reform. Yes, misinformation will continue to exist and circulate; the faith the First Amendment places in Americans to freely navigate a marketplace of ideas ensures that reality. But at least consumers of news through social media will have more choice in how and from whom they consume their news, and at least social media firms will have a greater incentive to provide moderated content. Even for the firms and consumers that prefer zero moderation, their level of content-scrutiny will be known and comparable for others to see.

Second, to the extent that social media platforms' economies of scale have created productive efficiencies that may have flowed to consumers, an HHI ceiling will sever one avenue to these efficiencies, meaning that consumers may be denied possible innovations only realizable with scale. However, the judgement call as to whether consumers would be better served by scale or competition is one which the U.S. already makes via the prosecutorial discretion of the FTC and DOJ. The HHI ceiling merely gives these bodies a tool to readily enjoin statutorily indefensible mergers without expending time, money, and expertise litigating a prediction of the future. To the extent consumers do lose out on shared productive efficiency gains, that cost is still the price that affords consumers a more democratic market that is rich with competition. Moreover, doubting monopolists' willingness to share efficiency gains with consumers is not only a non-radical return to standing Supreme Court caselaw, but also loyal to Congress' original choice to favor "fragmented . . . markets" over "occasional[ly] higher . . . prices."[217]

---

214. Tiffany Hsu & Marc Tracy, *On Podcasts and Radio, Misleading Covid-19 Talk Goes Unchecked*, N.Y. TIMES (Nov. 12, 2021), https://www.nytimes.com/2021/11/12/business/media/coronavirus-misinformation-radio-podcasts.html [https://perma.cc/QTR4-3WLG].

215. *See* Michael Grynbaum & Sydney Ember, *CNN Corrects a Trump Story, Fueling Claims of 'Fake News'*, N.Y. TIMES (Dec. 8, 2017), https://www.nytimes.com/2017/12/08/business/media/cnn-correction-donald-trump-jr.html [https://perma.cc/3XDD-TT5C]; *see also* Oliver Darcy, *Analysis: TV Providers Should Not Escape Scrutiny for Distributing Disinformation*, CNN (Jan. 8, 2021, 7:19 AM), https://www.cnn.com/2021/01/08/media/tv-providers-disinfo-reliable-sources/index.html [https://perma.cc/HL5Y-JS7D].

216. Philip Bump, *A Year of Election Misinformation from Trump, Visualized*, WASH. POST (Feb. 11, 2021, 6:04 PM), https://www.washingtonpost.com/politics/2021/02/11/year-election-misinformation-trump-visualized/ [https://perma.cc/NS8K-ANK6].

217. Brown Shoe Co. v. United States, 370 U.S. 294, 344 (1962) (asserting that Congress "appreciated that occasional higher costs and prices might result from the maintenance of fragmented industries and markets").

Third, an HHI ceiling—even one relying on competitive markets and antitrust enforcers to push current monopolies back beneath its ceiling—provides an underinclusive and slow tool to undo current, and prevent future, monopolies. After all, because Section Two doctrine rejected the no-fault standard and kept the requirement of anticompetitive conduct, new monopolies can still grow by their individual merits without mergers,[218] and current monopolies will likely still take time to be dissolved or shrink in response to enforcement and fair competition. However, the faith in competition to rectify present misallocations and inefficiencies is the heart of U.S. antitrust law, and a long-term improvement in the competitiveness of markets should not be ignored for its lack of instant gratification.

Therefore, misinformation will persist, but at least it will persist in fewer places, among fewer communities, and within more conspicuous forms and fora. From there, it is up to the people themselves to sort fact from fiction, but at least they will be better equipped for that task.

IV. CONCLUSION

As should be clear by now, a tremendous amount of trouble could have been avoided if U.S. students simply remembered to question every tree octopus they saw. But they did not, and why they did not is outside the scope of this Note. For now, it suffices to say that when faced with the blight of misinformation upon the U.S. forum for public debate and the danger it poses to democracy and public health, every worthwhile step should be taken to disarm, displace, and debunk it. Establishing an HHI ceiling by joint resolution is one such step.

Even if we would rather pin our frustrations on the power Section 230 has granted to some of the largest conductors of misinformation, trying to abolish or replace Section 230 is unlikely to remedy the situation, at least for now. The task is constitutionally vulnerable, politically fraught, and regulatorily risky. Instead, directing our frustrations towards addressing social media's monopoly problem constitutes a productive, even if relatively unsatisfying, improvement in raising the quality of public debate. Establishing an HHI ceiling for the social media market by statute, despite its reliance on market forces and the marketplace of ideas, remains a worthwhile, constitutionally firm, politically savvy, and regulatorily safe step in the right direction to cleansing our forests of tree octopuses.

218. *See* discussion *supra* Section II.B.1.a.ii.

A Digital Checkup on HIPAA: Modernizing Healthcare Privacy Standards for Telehealth Services

Julia Wells*

TABLE OF CONTENTS

* J.D., May 2023, The George Washington University Law School; B.A., Religion & Philosophy, Colgate University. I would like to thank Sarah Morris, Journal Adjunct, and Andrew Seneviratne, Notes Editor, for their support and guidance. I would also like to thank my family for their support during the writing process.

I. INTRODUCTION

Imagine consulting with your doctor or medical team through videoconferencing platforms or over messaging apps, but those platforms and apps are not encrypted or otherwise secure. Further, imagine that the device your doctor used to communicate with you is stolen, allowing the thief to view your personal health information. This is not an imaginary problem. In 2013, four unencrypted laptops belonging to Advocate Health Care that contained personal health information were stolen, and another unencrypted laptop with the personal information of over 2,000 patients was stolen from an employee's car.[1] The theft of unencrypted devices is not the only risk to patient privacy, however. Risks to patient privacy include ransomware attacks, health care providers sending private health information to the wrong person, and sending and storing unencrypted health information, including videos.[2]

Prior to the coronavirus pandemic, the use of telehealth services was uncommon.[3] Due to the pandemic, the use of telehealth services has increased, allowing people to receive routine checkups and medical care without risking their health by entering a hospital or doctor's office.[4] Although these telehealth services have provided much needed medical care during the pandemic, they have raised numerous patient privacy concerns. Because the pandemic made telehealth services a necessity to prevent in-person contact, several health care providers had to implement telehealth services quickly. Many of these services have likely not undergone the normal security checks and may not comply with the Health Insurance Portability and Accountability Act ("HIPAA").

During the pandemic, the Department of Health and Human Services ("HHS") announced that it would not penalize covered health care providers using video chatting platforms that may not be HIPAA compliant for telehealth services "in connection with the good faith provision of telehealth during the [pandemic]."[5] This regulatory discretion in enforcement implicates patients' data privacy. Because telehealth services will likely remain popular

---

1. Lisa Schencker, *Advocate to Pay $5.5 Million over Data Breach: Record HIPAA Settlement*, CHI. TRIB. (Aug. 5, 2016, 7:20 AM), https://www.chicagotribune.com/business/ct-advocate-settlement-privacy-0805-biz-20160804-story.html [https://perma.cc/PXF6-WBUT].

2. *See What Are Some Common HIPAA Violations?*, COMPLIANCY GRP., https://compliancy-group.com/common-hipaa-violations/ [https://perma.cc/MY59-5D7C] (last visited Mar. 3, 2022).

3. *See* Gabriela Weigel et al., *Opportunities and Barriers for Telemedicine in the U.S. During the COVID-19 Emergency and Beyond*, KAISER FAM. FOUND. (May 11, 2020), https://www.kff.org/womens-health-policy/issue-brief/opportunities-and-barriers-for-telemedicine-in-the-u-s-during-the-covid-19-emergency-and-beyond/ [https://perma.cc/BV2H-VYH3].

4. *Id.*

5. *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency*, U.S. DEP'T HEALTH & HUM. SERVS. [hereinafter *Notification of Enforcement Discretion*], https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html [https://perma.cc/NF45-S27B] (last updated Jan. 20, 2021).

after the pandemic, Congress should reform HIPAA so that it maintains flexibility regarding telehealth platforms while protecting patients' personal information. HIPAA should be reformed to include more detailed provisions concerning best practices for maintaining data privacy, such as two-factor authentication and firewalls, and include technical requirements for devices used to connect with patients, such as encryption.

Part A of the Background section of this Note provides an overview of telehealth services and the agencies involved in regulating and providing access to those services. Additionally, Part A describes the expansion of telehealth services in the United States. Part B of the Background presents a brief overview of HIPAA, its limitations, as well as an overview of HHS' Notification of Relaxed Enforcement. Moreover, Part B describes the roles agencies, particularly the FCC, play in overseeing and implementing telehealth services. Part A of the Analysis demonstrates the feasibility of Congress addressing matters relating to healthcare despite intense congressional polarization. Part B of the Analysis argues that the FCC should be given a larger role in regulating telehealth services, and Part C proposes reforms that should be made to HIPAA to increase flexibility while providing greater protection to patients' private information. Finally, Part D addresses potential limitations of the proposal and provides possible solutions to those limitations.

II. BACKGROUND

A. Overview of Telehealth Services

1. Definition and Expansion of "Telehealth Services"

Telehealth services is "the use of electronic information and telecommunications technologies to support and promote long-distance clinical health care, patient and professional health-related education, and public health and health administration."[6] These services can be provided through audio, text, and video.[7] They are designed to overcome geographic barriers in connecting with patients for clinical services through information and communication technologies (e.g., computers, cell phones, etc.).[8]

Prior to the coronavirus pandemic, the use of telehealth services was uncommon. Based on a sample of health benefit claims in 2018, only 2.4% of patients enrolled in large employer health plans that included outpatient

6. *What Is Telehealth?*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/3015/what-is-telehealth/index.html [https://perma.cc/BAP6-RXNN] (last updated Mar. 27, 2020).

7. *Id.*

8. NICOL TURNER LEE ET AL., BROOKINGS INST. & JOHN LOCKE FOUND., REMOVING REGULATORY BARRIERS TO TELEHEALTH BEFORE AND AFTER COVID-19 5 (2020), https://www.brookings.edu/wp-content/uploads/2020/05/Removing-barriers-to-telehealth-before-and-after-COVID-19_PDF.pdf [https://perma.cc/W6XY-FJ94].

services had used a telehealth service.[9] By May of 2020, a poll had found that at least 23% of adults had utilized telehealth services, and that number has exponentially grown.[10] A global study from July 2021 found that, out of 5,000 responses, almost half had engaged in telehealth services.[11] Over 80% of the group that had used telehealth services used those services during the pandemic in order to minimize in-person interactions.[12] Furthermore, 63% of respondents stated that they plan to continue using telehealth services post-pandemic, and 77% stated that they "enjoyed using telehealth."[13] In addition to the increasing usage of telehealth services, investments in those services have increased.[14] In August 2021, the Biden-Harris Administration declared "a $19 million investment to expand telehealth and improve access in rural communities."[15] Furthermore, a study found that 76% of employers expanded their telehealth services during the pandemic and that they plan to continue providing telehealth options post-pandemic.[16] Given its increased usage and investment, as well as the convenience telehealth services provide both patients and doctors, telehealth services will likely remain popular after the pandemic. The continued use of telehealth services makes agency regulation extremely important.

2. Agency Regulation and Oversight of Telehealth Services

A variety of government agencies, including HHS and the FCC, are involved in regulating and providing greater access to telehealth services. The FCC has long been involved in telecommunications, including telehealth and telemedicine. In the Telecommunications Act of 1996, Congress ordered the FCC to "encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans."[17] In 2006, the

---

9. *See* Gabriela Weigel et al., *Opportunities and Barriers for Telemedicine in the U.S. During the COVID-19 Emergency and Beyond*, KAISER FAM. FOUND. (May 11, 2020), https://www.kff.org/womens-health-policy/issue-brief/opportunities-and-barriers-for-telemedicine-in-the-u-s-during-the-covid-19-emergency-and-beyond/ [https://perma.cc/BV2H-VYH3].

10. *Id.*

11. *New Survey Reveals Appeal of Telehealth Services; 63% Plan to Increase Use Post-Pandemic*, BUS. WIRE (Oct. 13, 2021, 9:00 AM), https://www.businesswire.com/news/home/20211013005160/en/New-Survey-Reveals-Appeal-of-Telehealth-Services-63-Plan-to-Increase-Use-Post-Pandemic [https://perma.cc/T5LZ-AN8G].

12. *Id.*

13. *Id.*

14. David Jagielski, *Why It Isn't Too Late to Invest in Telehealth*, MOTLEY FOOL (Sept. 8, 2021, 6:13 AM), https://www.fool.com/investing/2021/09/08/why-it-isnt-too-late-to-invest-in-telehealth/ [https://perma.cc/DK6C-CTLE].

15. *Id.*

16. *Id.*

17. Telecommunications Act of 1996, Pub. L. No. 104-104, § 706, 110 Stat. 56, 152 (1996); *FCC Health IT Actions and Activities Timeline*, FCC, https://www.fcc.gov/general/fcc-health-it-actions-and-activities-timeline [https://perma.cc/X578-RSUQ] (last visited Jan. 28, 2022).

FCC created the Rural Health Care Pilot Program aimed at introducing telemedicine and telehealth services to rural areas.[18] Moreover, in 2014, the FCC formed the Connect2Health FCC Task Force, which is concerned with "the critical intersection of broadband, advanced technology, and health with the primary goal of ensuring that advanced health care solutions are readily accessible to all Americans."[19] Additionally, the FCC worked with the Food and Drug Administration and the Office of the National Coordinator for Health Information Technology to propose "recommendations on appropriate, risk-based regulatory framework pertaining to health information technology . . . that promotes innovation, protects patient safety, and avoids regulatory duplication."[20]

During the pandemic, Congress furthered the FCC's role in telehealth by passing the Coronavirus Aid, Relief, and Economic Security Act ("CARES Act").[21] The CARES Act allocated $200 million to the FCC for the expansion of telehealth services across the U.S.[22] The FCC was authorized to use these funds "to prevent, prepare for, and respond to coronavirus, domestically or internationally, including to support efforts of health care providers to address coronavirus by providing telecommunications services, information services, and devices necessary to enable the provision of telehealth services during an emergency period."[23] With this increased funding, the FCC has focused on providing telehealth services to people in remote areas.[24] It uses these funds to enable eligible nonprofit and public health care providers to buy telecommunications services and devices necessary to use those services.[25]

In addition to allocating funds to the FCC to expand telehealth services, the CARES Act encourages the expansion of telemedicine in general.[26] For example, Section 3212 adds $29 million in annual funding for 2021 through 2025 to develop "'evidence-based projects that utilize telehealth technologies through telehealth networks.'"[27] Moreover, Section 3707 instructs the Secretary of HHS to "encourage the use of telecommunications systems" in home health services during the emergency period.[28] Other provisions in the

18. *FCC Health IT Actions and Activities Timeline*, *supra* note 17.

19. *Id.*

20. *Id.*

21. Coronavirus Aid, Relief, and Economic Security Act, Pub. L. No. 116-136, 134 Stat. 281 (2020).

22. Coronavirus Aid, Relief, and Economic Security Act § 15002; *Connecting Americans to Healthcare*, FCC, https://www.fcc.gov/connecting-americans-health-care [https://perma.cc/D2XD-9DAS] (last visited Nov. 19, 2021).

23. Coronavirus Aid, Relief, and Economic Security Act § 15002.

24. *Connecting Americans to Healthcare*, *supra* note 22.

25. *CARES Act: AMA COVID-19 Pandemic Telehealth Fact Sheet*, AM. MED. ASS'N [hereinafter *Pandemic Telehealth Fact Sheet*], https://www.ama-assn.org/delivering-care/public-health/cares-act-ama-covid-19-pandemic-telehealth-fact-sheet [https://perma.cc/XT7Z-HGB4] (last updated Apr. 27, 2020).

26. Andrew D. Lipman & Tamar E. Finn, *CARES Act Includes Provisions Regarding Telecommunications, Telehealth*, MORGAN LEWIS (Apr. 1, 2020), https://www.morganlewis.com/pubs/2020/04/cares-act-includes-provisions-regarding-telecommunications-telehealth-cv19-lf [https://perma.cc/63BX-2VPJ].

27. Coronavirus Aid, Relief, and Economic Security Act § 3212.

28. Coronavirus Aid, Relief, and Economic Security Act § 3707.

CARES Act provide for reimbursement of particular telehealth services for seniors on Social Security and encourage the Secretary of Veterans Affairs to enter into contracts to expand telehealth services for veterans.[29] Although the expansion of the FCC's regulation of telehealth services has so far been limited to during the pandemic, the continued rise in telehealth services indicates that continued regulation will be necessary post-pandemic. Given the variety of provisions in the CARES Act that aim to expand telehealth services, it is likely that telehealth services will continue to be a priority for the foreseeable future. And, given the growing importance of telehealth services, it is important to understand the patient privacy regulations that were in place prior to COVID-19.

B. Health Insurance Portability and Accountability Act of 1996

Part 1 of this section describes the critical provisions of HIPAA impacting telehealth services and the rules, including the Privacy Rule and the Security Rule, that health care providers and business associates must follow. Additionally, Part 1, Subsection c explains how the Health Information Technology for Economic and Clinical Health (HITECH) Act amended HIPAA. Part 2 discusses the potential issues with HIPAA outside the public health emergency context. Part 3 explains the Department of Health and Human Services' notification of relaxed enforcement of HIPAA and describes the potential issues with such relaxed enforcement of HIPAA.

1. Overview of HIPAA

Under the HIPAA of 1996, health information is protected.[30] Protected health information ("PHI") includes information that can be used to identify an individual and is related to "the individual's past, present or future physical or mental health or condition," "the provision of health care to the individual," "or the past, present, or future payment for the provision of health care to the individual."[31] The protection of health information is governed by the HIPAA Privacy Rule, a primary objective of which is ensuring "that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being."[32]

29. Coronavirus Aid, Relief, and Economic Security Act §§ 3704, 20004; *see* Lipman & Finn, *supra* note 26.

30. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

31. Health Insurance Portability and Accountability Act § 1171; U.S. DEP'T HEALTH & HUM. SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 4 (2003) [hereinafter SUMMARY OF HIPAA PRIVACY RULE], https://www.hhs.gov/sites/default/files/privacysummary.pdf [https://perma.cc/5GQJ-WGFH].

32. SUMMARY OF HIPAA PRIVACY RULE, *supra* note 31, at 1.

a. The Privacy Rule

The Privacy Rule applies to health plans, health care providers who electronically convey health information regarding certain transactions, and health care clearinghouses, such as billing services.[33] The Privacy Rule requires covered entities to enter into a Business Associate Agreement ("BAA") with any business associates performing work on behalf of, or providing services to, covered entities.[34] Business associates are people or other organizations that perform a variety of services including claims processing, billing, and data analysis.[35] Services that business associates provide include legal, consulting, management, accreditation, and financial.[36] Covered entities are required to "impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates" in the BAA.[37] BAAs cannot be used to authorize business associates to use or disclose PHI in violation of the Privacy Rule.[38] Additionally, BAAs must "[r]equire the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract."[39] Finally, if the covered entity discovers the business associate violated the agreement, the entity must "take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the . . . arrangement."[40] The requirement to enter into a BAA only applies if the relationship between the covered entity and the business associate involves creating or sharing PHI.[41]

b. The Security Rule

HIPAA also includes a Security Rule, the purpose of which is to "protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care."[42] The Security Rule of HIPAA protects a subgroup of the information protected by the Privacy Rule.[43] This subgroup is "all individually identifiable health information a covered entity creates, receives,

---

33. *Id.* at 2.

34. U.S. DEP'T HEALTH & HUM. SERVS., BUSINESS ASSOCIATES 1 (2003), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.pdf [https://perma.cc/3AMX-NSLR].

35. *Id.* at 3.

36. *Id.*

37. *Id.*

38. *Id.*

39. BUSINESS ASSOCIATES, *supra* note 34, at 3.

40. *Id.*

41. 45 C.F.R. § 160.103(1)(i)-(ii) (2022); SUMMARY OF HIPAA PRIVACY RULE, *supra* note 31, at 3.

42. *Summary of the HIPAA Security Rule*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html#:~:text=The%20Security%20Rule%20protects%20a,%E2%80%9D%20(e%2DPHI) [https://perma.cc/5HVQ-DV3Q] (last updated July 26, 2013).

43. *Id.*

maintains or transmits in electronic form," otherwise known as e-PHI.[44] In other words, the Security Rule protects PHI only when it is transmitted electronically.[45] The Security Rule applies to the same entities as the Privacy Rule, as well as business associates who transmit health information electronically.[46]

Under the Rule, covered entities must "maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI."[47] Covered entities are required to ensure that e-PHI is not disclosed or made available to those who are unauthorized.[48] Additionally, e-PHI must not be "altered or destroyed in an unauthorized manner" and must be "accessible and usable on demand by an authorized person."[49] Moreover, covered entities are required to "[i]dentify and protect against reasonably anticipated threats to the security or integrity of the information" and "[p]rotect against reasonably anticipated, impermissible uses or disclosures."[50] Finally, covered entities must ensure that all employees comply with the Security Rule.[51]

c. Key Technical Considerations

The Security Rule does not require that each covered entity must adopt a specific security measure; rather, covered entities have discretion in deciding which security measures to assume.[52] The Rule, however, does list factors that a covered entity must consider in its decision. Such factors include the entity's "size, complexity, and capabilities," the entity's "technical, hardware, and software infrastructure," the "costs of security measures, and" "the likelihood and possible impact of potential risks to e-PHI."[53] Covered entities must perform regular risk analyses to ensure that all e-PHI remain protected.[54] A risk analysis entails assessing "the likelihood and impact of potential risks to e-PHI," implementing security measures to address those potential risks, recording the security measures adopted and the rationale for that adoption, and maintaining "appropriate security protections."[55]

---

44. *Id.*
45. *Summary of the HIPAA Security Rule*, *supra* note 42; *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CDC, https://www.cdc.gov/phlp/publications/topic/hipaa.html [https://perma.cc/JD7A-S7LX] (last updated Sept. 14, 2018).
46. *See Summary of the HIPAA Security Rule*, *supra* note 42.
47. *Id.*
48. *Id.*
49. *Id.*
50. *Id.*
51. *Id.*
52. *Summary of the HIPAA Security Rule*, *supra* note 42.
53. *Summary of the HIPAA Security Rule*, *supra* note 42; *HIPAA Security Rule & Risk Analysis*, AM. MED. ASS'N, https://www.ama-assn.org/practice-management/hipaa/hipaa-security-rule-risk-analysis [https://perma.cc/QJ7M-M9DT] (last visited Apr. 11, 2022).
54. *Summary of the HIPAA Security Rule*, *supra* note 42.
55. *Id.*

Because covered entities are not required to adopt any specific security measures, the Security Rule does not require encryption of PHI.[56] Encryption converts "an original message of regular text into encoded text" using an algorithm.[57] Once the recipient receives the encrypted information, the recipient can restore the plain text of the information only by using a key, which is "a group of random characters in a particular order."[58] By encrypting information, a party can reduce the likelihood that someone other than the intended recipient would be able to translate the information into plain text.[59]

There are two main types of encryption: symmetric and asymmetric.[60] For symmetric encryption, "the sender uses the same secret key to decrypt the text as the recipient uses to decrypt the text."[61] Asymmetric encryption, on the other hand, requires two different keys.[62] The sender encrypts the message using a public key, and the recipient uses a private key to decrypt the message.[63] Although the public key can be made known to and identified by anyone, only the person decrypting the message can know the private key.[64] With end-to-end encryption, a form of asymmetric encryption, only those with the decryption keys can see the encrypted information.[65] End-to-end encryption thus "prevents unintended users, including third parties, from reading or modifying data when only the intended readers should have this access and ability."[66] When using any form of encryption, entities must ensure the security of encryption keys.[67] Entities may store keys on secure repositories, such as a local hard drive or a USB, but access to those keys should be limited and methods of verifying those who access the key, such as passwords, should be used.[68] Although encryption requires entities to ensure security of encryption keys regularly, which may be difficult for some entities, encryption is a useful tool in securing private information.[69]

---

56. *Is the Use of Encryption Mandatory in the Security Rule?*, U.S. DEP'T HEALTH & HUM. SERVS. [hereinafter *Is the Use of Encryption Mandatory?*], https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html [https://perma.cc/64YH-UJVL] (last updated July 26, 2013).

57. *What Is Encryption?*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/2021/what-is-encryption/index.html [https://perma.cc/LBD2-R469] (last updated July 26, 2013); *see* Nina Patel, Note, *Your Personal Health Information May Have Been Compromised: Using Encryption to Prevent Data Breaches on End-User Devices*, 48 HOFSTRA L. REV. 563, 578 (2019).

58. Patel, *supra* note 57, at 578; *What Is a Cryptographic Key? Keys and SSL Encryption*, CLOUDFLARE, https://www.cloudflare.com/learning/ssl/what-is-a-cryptographic-key/#:~:text=Combined%20with%20an%20encryption%20algorithm,KZ0KVey8l1c%3D%22%20as%20the%20ciphertext [https://perma.cc/V5QG-TN2N] (last visited Mar. 4, 2022).

59. *What Is Encryption?*, *supra* note 57.

60. Patel, *supra* note 57, at 580.

61. *Id.*

62. *Id.*

63. *Id.*

64. *Id.* at 580-81.

65. *What Is End-to-End Encryption?*, IBM, https://www.ibm.com/topics/end-to-end-encryption [https://perma.cc/UY58-TYTS] (last visited Mar. 3, 2022).

66. *Id.*

67. Patel, *supra* note 57, at 580-81.

68. *Id.* at 581.

69. *See id.* at 564-65, 580-81.

Rather than requiring encryption, the Security Rule makes encryption an "addressable implementation specification."[70] The "addressable" designation "permits covered entities to determine whether the addressable implementation specification is reasonable and appropriate for that covered entity."[71] Thus, a covered entity is only required to implement encryption "if, after a risk assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its risk management of the confidentiality, integrity and availability of e-PHI."[72] If an entity determines that encryption is not reasonable and appropriate, the entity must note that decision and, if reasonable and appropriate, "implement an equivalent alternative measure."[73] An entity may not need to adopt either the implementation specification or the alternative if the Security Rule can be met otherwise, but the entity must record its rationale for doing so.[74]

Similar to encryption, other security measures are also addressable and, thus, are not required at the outset. One such security measure is a firewall. A firewall is a computer software or hardware that protects one's network "by filtering traffic and blocking outsiders from gaining unauthorized access to the private data" on the computer.[75] Firewalls can also prevent malicious software from infecting a computer.[76] Another such security measure is two-factor authentication. Two-factor authentication is a two-step log-in process that verifies the user's identity and prevents unauthorized individuals from accessing the user's information.[77] When HIPAA was first enacted, covered entities were required to consider and implement these technical considerations if it were "'reasonable and appropriate'" for the entity to do so, but compliance with HIPAA remained low until the passage of the HITECH Amendment.[78]

---

70. *Is the Use of Encryption Mandatory?*, *supra* note 56.

71. *Summary of the HIPAA Security Rule*, *supra* note 42.

72. *Is the Use of Encryption Mandatory?*, *supra* note 56; *see, e.g.*, Press Release, U.S. Dep't Health & Hum. Servs., Lifespan Pays $1,040,000 to OCR to Settle Unencrypted Stolen Laptop Breach (July 27, 2020), https://public3.pagefreezer.com/content/HHS.gov/31-12-2020T08:51/https://www.hhs.gov/about/news/2020/07/27/lifespan-pays-1040000-ocr-settle-unencrypted-stolen-laptop-breach.html [https://perma.cc/NR2U-5ES4] (stating that Lifespan Health System Affiliated Covered Entity settled with HHS after OCR "determined that there was systemic noncompliance with the HIPAA Rules including a failure to encrypt ePHI on laptops after Lifespan ACE determined it was reasonable and appropriate to do so").

73. *Is the Use of Encryption Mandatory?*, *supra* note 56.

74. *Id.*

75. Alison Grace Johansen, *What Is a Firewall? Firewalls Explained and Why You Need One*, NORTONLIFELOCK (June 17, 2021), https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html [https://perma.cc/G9R7-Q8PJ].

76. *Id.*

77. Kyle Chivers, *What Is Two-Factor Authentication (2-FA) and How Does It Work?*, NORTONLIFELOCK (Oct. 15, 2020), https://us.norton.com/blog/how-to/importance-two-factor-authentication [https://perma.cc/7YYR-G922].

78. Patel, *supra* note 57, at 572-73, 575.

d. The HITECH Amendment to HIPAA

Prior to 2009, HIPAA included loopholes that allowed covered entities to avoid sanctions for violating HIPAA "by claiming their business associates were unaware that they were violating HIPAA."[79] Additionally, penalties for violations of HIPAA were too low to incentivize health care organizations and business associates to comply with HIPAA.[80] To remedy these issues, Congress passed the Health Information Technology for Economic and Clinical Act of 2009 ("HITECH Act" or "HITECH").[81] The HITECH Act expanded enforcement and penalties of HIPAA, business associate duties under HIPAA, and patient rights.[82] The HITECH Act increased monetary penalties and increased enforcement in a variety of ways, including increased public education of PHI and authorization of state attorneys general to bring civil suits.[83] Covered entities were now subject to increased civil penalties for violations of HIPAA.[84]

In addition to increasing enforcement and penalties of HIPAA, HITECH also expanded the duties of business associates under HIPAA. HITECH bound business associates to the HIPAA Security Rule requirements.[85] Additionally, business associates were now subject to civil and criminal penalties for violations of the Security Rule.[86] Thus, as with covered entities, business associates were required to implement, maintain, develop, and document security measures to safeguard PHI; however, business associates, like covered entities, had flexibility in what security measures they implement.[87]

The HITECH Act also expanded patient rights under HIPAA. Under HITECH, patients are allowed to access and obtain their electronic health information.[88] Additionally, HITECH prohibited business associates from marketing, without authorization, e-PHI.[89] Moreover, if patients had originally authorized business associates to use e-PHI, patients can now revoke that authorization.[90] Finally, HITECH requires that any disclosures of PHI be recorded, which includes noting who the information was given to and the purpose of the disclosure.[91] Although HITECH addressed some of the

79. *What Is the HITECH Act?*, HIPAA J., https://www.hipaajournal.com/what-is-the-hitech-act/ [https://perma.cc/UB6R-663S] (last visited Jan. 28, 2022).
80. *Id.*
81. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, 246 (2009) (codified in scattered sections of 42 U.S.C.).
82. *Id.*
83. Jason W. Davis, *HITECH HIPAA Amendments: New Rules on Breach Notification, Business Associate Compliance, and Enforcement*, 21 HEALTH L. 23, 26 (2009).
84. *Id.*
85. *Id.* at 25.
86. *Id.*
87. *Id.*
88. *What Is the HITECH Act?*, *supra* note 79.
89. *Id.*
90. *Id.*
91. *Id.*

limitations of HIPAA, potential privacy issues with HIPAA remain and must be addressed.

2. Potential Privacy Issues with HIPAA

As it stands, HIPAA is still susceptible to privacy issues. Because the Security Rule only requires entities to "determine whether the addressable implementation specification is reasonable and appropriate for that covered entity," covered entities have considerable discretion in determining what security measures to adopt, when to adopt those measures, and whether to adopt an alternative measure.[92] Moreover, the Security Rule lacks guidance for how covered entities should identify possible risks to e-PHI or how to address potential risks to the information.[93] Entities, particularly smaller covered entities, may not have the requisite knowledge or expertise to conduct regular assessments for identifying potential risks.

Additionally, the Security Rule allows covered entities to forgo adopting either the implementation specification or the alternative if the Security Rule can be met otherwise.[94] Of course, the entities must record their rationale for doing so, but this potential loophole could allow covered entities to make an excuse in order to forego implementing a security measure that they may see as a time-waster or a drain on resources.[95] These potential privacy issues became more salient in 2020 when the COVID-19 pandemic forced people to turn to telehealth services for routine medical care.

3. Department of Health and Human Services' Notification of Relaxed Enforcement

In response to the pandemic, HHS issued a notice in March of 2020 detailing limited waivers of select provisions in HIPAA for the duration of COVID-19.[96] The notice states that the Office for Civil Rights ("OCR") will "exercise its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under HIPAA Rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency."[97] OCR is a division of HHS in charge of enforcing federal civil rights laws, including HIPAA.[98] If a provider uses telehealth services and there is a breach

92. *Summary of the HIPAA Security Rule*, *supra* note 42; *see* Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 337 (2007).

93. *See* Hoffman & Podgurski, *supra* note 92, at 351.

94. *Is the Use of Encryption Mandatory?*, *supra* note 56.

95. *Id.*

96. *Notification of Enforcement Discretion*, *supra* note 5; Anna Clark & Joel Thayer, *What Privacy Compliance Looks Like During COVID-19*, LAW360 (Apr. 8, 2020, 1:15 PM), https://www.law360.com/articles/1261184 [https://perma.cc/5PDW-UD7K].

97. *Notification of Enforcement Discretion*, *supra* note 5.

98. *About Us*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/ocr/about-us/index.html [https://perma.cc/AP95-SYXY] (last visited Jan. 24, 2022).

in which e-PHI is intercepted, OCR will not automatically impose a penalty for violating the HIPAA Security Rule during the pandemic.[99] Instead, OCR will use its enforcement discretion and determine if the breach resulted from good faith efforts to provide telehealth services.[100] In determining whether there has been good faith, OCR will consider the facts and circumstances surrounding the breach.[101] Thus, even if a health care provider does not analyze possible privacy risks of a telehealth service or otherwise take steps to ensure patient privacy, they may still use telehealth services to connect with patients without violating HIPAA.[102] This notice does not apply to all entities covered by HIPAA (e.g., health insurance companies who pay for telehealth services), only covered health care providers utilizing telehealth services.[103] Additionally, covered health care providers who want to use audio or video technology in order to provide telehealth services to patients may use any non-public facing platform, including Facebook Messenger, Google Hangouts, and FaceTime, even if those platforms are not HIPAA compliant.[104]

a. Non-Public Facing vs. Public-Facing Platforms

Non-public facing communication platforms only allow authorized parties to communicate.[105] Generally, these non-public facing platforms use end-to-end encryption, enabling only authorized individuals to see the communication that is transmitted.[106] Additionally, non-public facing platforms permit separate user accounts and passwords, allowing those platforms to verify participants.[107] Finally, non-public facing platforms provide users with the ability to control the platform to an extent by allowing users to choose whether to record the communication or to switch off the audio or video.[108] Public-facing platforms, such as Facebook Live and TikTok, are "designed to be open to the public or allow wide or indiscriminate

99. *If a Covered Health Care Provider Uses Telehealth Services During the COVID-19 Outbreak and Electronic Protected Health Information is Intercepted During Transmission, Will OCR Impose a Penalty on the Provider for Violating the HIPAA Security Rule?*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/3025/if-a-covered-health-care-provider-uses-telehealth-services-during-the-covid-19-outbreak-and-electronic-protected-health-information-is-intercepted-during-transmission-will-ocr-impose-a-penalty-on-the-provider/index.html [https://perma.cc/HL9S-NPKS] (last updated Mar. 27, 2020).

100. *Id.*

101. *Id.*

102. *Pandemic Telehealth Fact Sheet*, *supra* note 25.

103. *Notification of Enforcement Discretion*, *supra* note 5.

104. *Id.*

105. *What Is a "Non-Public Facing" Remote Communication Product?*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/3024/what-is-a-non-public-facing-remote-communication-product/index.html [https://perma.cc/95AJ-GGYH] (last visited Jan. 24, 2022).

106. *Id.*

107. *Id.*

108. *Id.*

access to the communication" and are thus not allowed for telehealth services.[109]

Although HHS provides specific qualifications for what applications and video platforms covered entities are allowed to use when connecting with patients, there are still serious implications for patients' privacy.[110] HHS explicitly prohibits the use of public facing platforms for telehealth services, but the Notification does not require that the non-public facing platforms be HIPAA compliant.[111] Thus, the use of even non-public facing platforms may not be secure.[112] Such platforms may not currently use encryption or other security measures to protect patient information.

b. BAAs Under the Notification of Relaxed Enforcement

OCR has not required covered entities to enter into a business associate agreement with vendors of video communication platforms during the pandemic.[113] Relaxing the requirement of BAAs could have negative consequences for patient privacy. Some of the video platforms that had entered into BAAs and complied with HIPAA before the pandemic may be secure and may utilize enhanced security provisions. However, other platforms that had not already offered telehealth services may not be compliant.[114] The Notification mentions vendors, such as Skype and Zoom, that have marketed products claimed to be HIPAA compliant, but OCR has not reviewed the BAAs of these platforms, nor has OCR endorsed these platforms.[115] Because telehealth services were in high demand due to the pandemic, many providers likely were not able to ensure that the chosen platform was HIPAA-compliant.[116]

Business associates are also allowed to share data related to COVID-19, including PHI.[117] The Privacy Rule already allows covered entities to share this data.[118] The justification for this is that federal, state, and local agencies "need quick access to COVID-19 related health data to fight this

109. *Id.*; *Notification of Enforcement Discretion*, *supra* note 5.

110. *Notification of Enforcement Discretion*, *supra* note 5.

111. *Id.*

112. *Notification of Enforcement Discretion*, *supra* note 5; *see* Sharon Bassan, *Data Privacy Considerations for Telehealth Consumers amid COVID-19*, 7 J.L. & BIOSCIENCES 1, 5-6 (2020).

113. *Notification of Enforcement Discretion*, *supra* note 5.

114. *See* Bassan, *supra* note 112, at 5.

115. *Notification of Enforcement Discretion*, *supra* note 5; *see* Bassan, *supra* note 112, at 5.

116. *See* Bassan, *supra* note 112, at 5-6.

117. ROBERT GELLMAN & PAM DIXON, WORLD PRIV. F., COVID-19 AND HIPAA: HHS'S TROUBLED APPROACH TO WAIVING PRIVACY AND SECURITY RULES FOR THE PANDEMIC 13 (2020), https://www.worldprivacyforum.org/2020/09/covid-19-and-hipaa/ [https://perma.cc/29VV-H97G].

118. *Id.* at 3.

pandemic."[119] This justification may not be entirely persuasive because business associates who have already entered into BAAs with health care providers must adhere to those agreements with regards to sharing data.[120] Business associates, thus, must be specifically authorized by the covered entity to release the data to those agencies.[121] Although some business associates may be prevented from disclosing PHI, some health care providers may be using video communications platforms that they have not entered into BAAs with. Additionally, business associates are not limited to disclosing this information to public health agencies; rather, a business associate can disclose PHI to "anyone it believed 'in good faith' could make a contribution to the emergency."[122] Thus, a business associate could potentially release private patient information in good faith to a company that may in turn use the information for a different purpose.[123] Because business associates are not held to the same medical ethical standards as covered entities, business associates may not act with the same level of restraint in disclosing patient information.[124]

c. Waiver of Privacy Notifications to Patients and of Sanctions

OCR encourages doctors and health care providers to notify their patients of the security risks posed by using telehealth services; however, OCR does not require patients to be notified of those risks before doctors engage with their patients over telehealth services.[125] HHS has also waived sanctions and penalties for noncompliance with requirements relating to privacy notices and patient agreement to disclosures of PHI as long as the noncompliance is in good faith.[126] For the duration of the COVID-19 pandemic, covered entities need not acquire a patient's consent to speak with family or friends about the patient's care, nor do covered entities need to "distribute a notice of privacy practices."[127] Additionally, covered entities are

119. GELLMAN & DIXON, *supra* note 117 at 13; *see* Nancy L. Perkins, *Personal Health Information Privacy and COVID-19: HIPAA and California Law Enforcement Forbearance*, ARNOLD & PORTER (Apr. 8, 2020), https://www.arnoldporter.com/en/perspectives/publications/2020/04/personal-health-information-privacy-and-covid-19 [https://perma.cc/3JBA-MR29].

120. Caroline D. Kessler, *HHS OCR to Exercise Enforcement Discretion to Allow Business Associates to Share PHI for Public Health and Health Oversight Activities*, AKIN GUMP (Apr. 9, 2020), https://www.akingump.com/en/experience/practices/cybersecurity-privacy-and-data-protection/ag-data-dive/hhs-ocr-to-exercise-enforcement-discretion-to-allow-business-associates-to-share-phi-for-public-health-and-health-oversight-activities.html [https://perma.cc/43DY-XDAJ].

121. GELLMAN & DIXON, *supra* note 117, at 13-14.

122. GELLMAN & DIXON, *supra* note 117, at 15; *see* Kessler, *supra* note 120.

123. GELLMAN & DIXON, *supra* note 117, at 15 (providing an example of a business associate who releases PHI to a commercial data broker for public health analysis, but intermediary turns out to be a Medicare fraudster).

124. *Id.*

125. *Pandemic Telehealth Fact Sheet*, *supra* note 25.

126. GELLMAN & DIXON, *supra* note 117, at 4-5.

127. *Id.* at 9.

not required to acquiesce to a patient's request for privacy restrictions or for confidential communications.[128]

This relaxation of privacy notifications to patients and the waiver of sanctions has serious implications for patient privacy. Patients may not know that health care providers do not need their permission to speak with family and friends about the patient for the duration of the pandemic.[129] Additionally, patients are unlikely to know what privacy policies are in place or the possible risks to their privacy without receiving the privacy notices from the provider.[130] The Notification of Relaxed Enforcement highlights potential issues for patient privacy during the pandemic, but the Notification also highlights issues with HIPAA that will continue even after the pandemic, thus necessitating reform.

III. ANALYSIS

The potential privacy issues for patients' health information should be addressed by reforming HIPAA. Congress should reform HIPAA so that it maintains flexibility regarding telehealth platforms while protecting patients' personal information by including specific security measures and detailing best practices for health care providers, business associates, and patients. Such security measures and best practices include implementing encryption, firewalls, and two-factor authentication.

Part A of the analysis addresses the feasibility of congressional action on this issue and argues that, although Congress appears unwilling to compromise on many issues, Congress is willing to address healthcare. Part B of this section explores why the FCC should have an expanded role in regulating telehealth services. Part C describes how HIPAA should be reformed to include greater flexibility while also including heightened privacy protections, such as encryption and two-factor authentication. Finally, Part D examines some of the limits of the proposal and addresses possible ways of mitigating those limitations.

A. Although Congress Appears Unwilling to Compromise on any Issues, Congress is Willing to Address and Act on Issues Involving Healthcare

Over the years, Congress has become increasingly polarized, as evidenced by the Pew Research Center's finding that "Democrats and Republicans are farther apart ideologically today than at any time in the past 50 years."[131] Because of this increasing polarization and congressmembers'

128. *Id.*

129. *See* Bassan, *supra* note 112, at 6-7; GELLMAN & DIXON, *supra* note 117, at 9.

130. *See* Bassan, *supra* note 112, at 6-7; GELLMAN & DIXON, *supra* note 117, at 9.

131. Drew DeSilver, *The Polarization in Today's Congress Has Roots That Go Back Decades*, PEW RSCH. CTR. (Mar. 10, 2022), https://www.pewresearch.org/fact-tank/2022/03/10/the-polarization-in-todays-congress-has-roots-that-go-back-decades/ [https://perma.cc/8XMB-BS8R].

fear of losing reelections, Congress has been unwilling to compromise and act on a variety of issues.[132] Polarization and the resulting unwillingness to compromise has led to greater congressional inaction characterized by a "my way or the highway" mentality.[133]

Despite Congress' polarization and apparent unwillingness to compromise, Congress could feasibly address and act on issues involving healthcare in a bipartisan manner. Recent congressional action demonstrates that Congress is willing to address important healthcare issues in general, as well as telehealth in particular. For example, Congress worked quickly to pass the CARES Act in order to expand access to healthcare generally, and telehealth services in particular, during the pandemic.[134]

Furthermore, Senators Tammy Baldwin (D-WI) and Bill Cassidy, M.D. (R-LA) recently introduced the Health Data Use and Privacy Commission Act.[135] This Act would form a commission "to research and give official recommendation[s] to Congress on how to modernize the use of health data and privacy laws to ensure patient privacy and trust while balancing the need of doctors to have information at their fingertips to provide care."[136] The commission would be responsible for reviewing existing state and federal protections for PHI, as well as how health care and other industries use health data.[137] Finally, the commission would be charged with providing recommendations and conclusions on, among other things, "potential threats posed to individual health privacy and legitimate business and policy interests," "[t]he effectiveness of existing statutes [and] regulations . . . in protecting individual health privacy," and "whether federal legislation is necessary, and if so, specific suggestions on proposals to reform, streamline, harmonize, unify, or augment current laws and regulations relating to individual health privacy . . . ."[138] Recent congressional actions and the

---

132. *See* David Davenport, *Congress and the Lost Art of Compromise*, FORBES (Jan. 24, 2018, 1:00 PM), https://www.forbes.com/sites/daviddavenport/2018/01/24/congress-and-the-lost-art-of-compromise/?sh=637b5743d597 [https://perma.cc/8DBL-WMJ3]; Sarah E. Anderson et al., *Biden Wants to Bring Democrats and Republicans Together. Here's Why That's So Challenging.*, WASH. POST (Dec. 21, 2020), https://www.washingtonpost.com/politics/2020/12/21/biden-wants-bring-democrats-republicans-together-heres-why-thats-so-challenging/ [https://perma.cc/F68U-2MGE].

133. Frank Newport, *The Impact of Increased Political Polarization*, GALLUP (Dec. 5, 2019), https://news.gallup.com/opinion/polling-matters/268982/impact-increased-political-polarization.aspx [https://perma.cc/KP24-D98D].

134. Coronavirus Aid, Relief, and Economic Security Act, Pub. L. No. 116-136, 134 Stat. 281 (2020); Amber Phillips, *'Totally Unprecedented in Living Memory': Congress's Bipartisanship on Coronavirus Underscores What a Crisis This Is*, WASH. POST (Mar. 26, 2020, 12:35 PM) https://www.washingtonpost.com/politics/2020/03/26/totally-unprecedented-living-memory-congresss-bipartisanship-coronavirus-underscores-what-crisis-this-is/ [https://perma.cc/WB2Q-EHRH].

135. Press Release, Bill Cassidy, Senator, *Cassidy,* Baldwin Introduce Legislation to Begin Modernization of Health Privacy Laws (Feb. 9, 2022), https://www.cassidy.senate.gov/newsroom/press-releases/cassidy-baldwin-introduce-legislation-to-begin-modernization-of-health-privacy-laws [https://perma.cc/8JVD-6LYM].

136. *Id.*

137. *Id.*

138. *Id.*

proposed bill demonstrate the feasibility of Congress addressing and acting on matters concerning healthcare, despite the intense polarization.

B. The FCC Should Have a Larger Role in Regulating Telehealth Due to its Expertise in Communications and History with Telemedicine

The FCC's long history of ensuring that all Americans have access to telehealth services indicates that the FCC's role in regulating telehealth is critical.[139] Since 1996, the FCC has encouraged and implemented the use of telehealth services, particularly in rural areas.[140] Moreover, the FCC has worked with other agencies to provide telehealth services in a safe and effective manner, indicating that the FCC is capable of further regulating telehealth.[141]

In addition to the FCC's historical involvement in telehealth, the recent statements of FCC Commissioner Geoffrey Starks and Chairwoman Jessica Rosenworcel highlight the FCC's prioritization of improving telehealth. In February 2022, Commissioner Starks made a statement regarding the proposal for further reforms to the Rural Health Care Program.[142] Commissioner Starks highlighted the crucial role that telehealth plays, noting that telehealth "is critically important to communities across the country, and especially in rural America."[143] Similarly, Chairwoman Rosenworcel highlighted the effectiveness and importance of telehealth during the pandemic and noted that the COVID-19 Telehealth Program has allowed the FCC to "expand the reach of communications and the possibilities of telehealth."[144]

The FCC currently has an enforcement process for protecting consumers from harmful uses of telecommunications, and this process could be applied to telehealth.[145] The Telecommunications Consumers Division investigates "the practices of companies engaged in various telecommunications-related activities," resolves "formal complaints brought by consumers," and consults "with internal and external organizations to ensure the FCC rules provide the maximum protection."[146] Applying this type

---

139. *See* Telecommunications Act of 1996, Pub. L. No. 104-104, § 706, 110 Stat. 56, 152 (1996); *FCC Health IT Actions and Activities Timeline*, *supra* note 17.

140. *See* Telecommunications Act § 254; *FCC Health IT Actions and Activities Timeline*, *supra* note 17.

141. *See FCC Health IT Actions and Activities Timeline*, *supra* note 17.

142. FCC Seeks Comment on Further Reforms to Rural Health Care Program, *Further Notice of Proposed Rulemaking*, FCC 22-15 (2022), https://docs.fcc.gov/public/attachments/DOC-380472A4.pdf [https://perma.cc/8UL2-8UNM].

143. *Id.* at para. 1.

144. COVID-19 Telehealth Program, *Report and Order and Order on Reconsideration*, FCC 21-39, para. 6 (2021), https://docs.fcc.gov/public/attachments/FCC-21-39A2.pdf [https://perma.cc/UR3A-MU5R].

145. *See* ENFORCEMENT BUREAU, FCC, ENFORCEMENT OVERVIEW 5 (2020), https://www.fcc.gov/sites/default/files/public_enforcement_overview.pdf [https://perma.cc/M63G-MMKX].

146. *Id.*

of process to telehealth, the FCC would investigate the practices of health care providers and their business associates. Additionally, the FCC would resolve complaints brought by patients and consult with organizations both within and outside of the FCC. Given the FCC's investment in telehealth and its extensive expertise in communications platforms and law, the FCC would play a vital role in ensuring that telehealth services protect patient safety.

C. HIPAA Should Retain Flexibility but Should Include Best Practices for Ensuring Data Privacy, and Agencies Should Coordinate on Implementation of Privacy Standards

1. Maintaining Flexibility

HIPAA should be reformed to maintain the flexibility it has during the pandemic, while still protecting patient privacy. Prior to HHS' Notification of Relaxed Enforcement, it was challenging to use everyday video platforms, such as FaceTime and Facebook Messenger, for telehealth. These everyday platforms typically were not HIPAA-compliant or did not have a BAA.[147] The Notification allows patients to connect with healthcare providers through these common video platforms, even if those platforms were not HIPAA-compliant.[148] This allows patients with limited access to technology and other software to receive healthcare without risking their health through in-person visits.[149]

Although this new flexibility in the type of platforms health care providers may utilize should remain after the pandemic, the privacy of patient information must be addressed.[150] These platforms must be updated to ensure that they will be HIPAA-compliant post-pandemic. Additionally, health care providers must enter into BAAs with these platforms to ensure that there are provisions in place to adequately protect patient information. Although maintaining flexibility with respect to the allowed video platforms is important, more reforms are needed to protect patient privacy.

2. Covered Entities Should Implement Privacy Safeguards

HIPAA should be reformed to include express requirements for security measures that must be implemented before providing telehealth services. Although covered entities vary in ways that may affect the ability of a covered entity to adopt a specific security measure, one such measure that all covered entities should adopt is PHI encryption.[151] There are a variety of

147. Clark & Thayer, *supra* note 96.

148. *Notification of Enforcement Discretion*, *supra* note 5.

149. *See* Steve North, Opinion, *These Four Telehealth Changes Should Stay, Even After the Pandemic*, FAM. PRAC. MGMT., May-June 2021, at 9, 9-10 (2021), https://www.aafp.org/fpm/2021/0500/fpm20210500p9.pdf [https://perma.cc/LXN5-3HK8].

150. *See id.*

151. *See* Patel, *supra* note 57, at 588-91.

encryption methods that allow covered entities to choose the best fit.[152] According to an IBM Security report, the average cost of a data breach has risen to $9.42 million.[153] The report further found that the cost of a data breach decreased at companies that utilized encryption and other security measures.[154] Those companies saved between $1.25 million and $1.40 million for each data breach that occurred.[155] Thus, the cost of a data breach far outweighs the cost of implementing and maintaining encryption.[156]

The requirement to implement and maintain encryption should apply to both covered entities and business associates. All PHI should be encrypted, including when transferred onto a flash drive, CD, or other portable electronic device.[157] Additionally, when sending e-PHI over email, covered entities and business associates should ensure that the email server is secure and that the email is encrypted.[158] Finally, health care providers that record and store video telehealth visits should adopt encryption.[159] In expressly requiring the implementation and maintenance of encryption, HIPAA should direct the FCC to provide guidance on current standards and techniques for encryption to covered entities and business associates in order to mitigate any user error.[160] Such guidance should include methods of conducting regular risk assessments, as well as guidance on which type of encryption to adopt.[161] The FCC has far-reaching expertise in providing guidance on cybersecurity. For example, the FCC has provided a cybersecurity tip sheet for small businesses.[162] Thus, it is qualified to provide similar guidance to covered entities and business associates.

---

152. *See id.* at 588-91.

153. *The Average Cost of a Healthcare Data Breach is Now $9.42 Million*, HIPAA J. (July 29, 2021), https://www.hipaajournal.com/average-cost-of-a-healthcare-data-breach-9-42-million-2021/ [https://perma.cc/V43R-CKRE].

154. *Id.*

155. *Id.*

156. *See id.*; Patel, *supra* note 57, at 590.

157. *See* Roger Hsieh, *Improving HIPAA Enforcement and Protecting Patient Privacy in a Digital Healthcare Environment*, 46 LOY. U. CHI. L.J. 175, 184 n.51 (2014) (noting that "PHI can be stored in a wide variety of mediums . . . which can lead to breaches of patient privacy").

158. *See id.*; Patel, *supra* note 57, at 590.

159. Geoffrey Lottenberg, *COVID-19 Telehealth Boom Demands Better Privacy Practices*, LAW360 (July 2, 2020, 4:11 PM), https://www.law360.com/cybersecurity-privacy/articles/1287404/covid-19-telehealth-boom-demands-better-privacy-practices- [https://perma.cc/ZJD2-87TB].

160. *See* Patel, *supra* note 57, at 582.

161. *See, e.g.*, *id.* at 589-90 (arguing that hospitals and insurance companies should be required to implement asymmetric encryption, that smaller covered entities and business associates should at least utilize symmetric encryption keys, that all entities should "conduct independent audits to determine if they have adequate protection because symmetric encryption may not be enough," and that "risk assessments and other factors, such as financial feasibility, size, and complexity of the entity," should inform the determination of whether to use asymmetric encryption).

162. *Ten Cybersecurity Tips for Small Businesses*, FCC (May 16, 2011), https://apps.fcc.gov/edocs_public/attachmatch/DOC-306595A1.pdf [https://perma.cc/6WBE-RQW5].

3. Best Practices for Maintaining Data Privacy

In addition to requiring certain security measures, HIPAA should include specific best practices that health care providers, business associates, and patients should undertake. HIPAA, while including a list of best practices, could also include the organization that should be responsible for generating more best practices. Given the FCC's extensive background with a variety of technologies and HHS' involvement in telehealth, these two agencies seem best positioned for this task.

Two such best practices that could be listed are firewalls and two-factor authentication.[163] Health care providers that record and store video telehealth visits should have a firewall to ensure that unsanctioned individuals do not gain access to private health information and to prevent threats from malicious software.[164] Health care providers can also implement two-factor authentication as an extra step to ensure patients' private information is protected.[165] By implementing two-factor authentication, health care providers can verify the identity of individuals accessing the private health information.[166]

In addition to implementing security measures such as firewalls and two-factor authentication, health care providers should carefully review BAAs to ensure that the agreement provides the best possible protection. Similarly, covered entities should notify their patients of the potential risks of engaging in telehealth services, including the risks of using video platforms. Additionally, covered entities should notify patients of privacy notices even when not required to do so.

Patients can also take steps before engaging in telehealth services to understand the possible risks and assess whether the risks outweigh the benefits of using the service. One best practice for patients is reading the privacy policy of whichever technology they will be using.[167] In doing so, patients can decide beforehand whether to use that particular technology. When reading the privacy policy, patients should focus on parts of the notice that specify what information can be used or disclosed, "persons authorized to use or disclosure [sic] the information, those to whom disclosure may be made, and each purpose for disclosure."[168]

Because privacy policies are not typically user-friendly, the FCC should direct the Consumer Advisory Committee ("CAC") to provide guidance on how providers can offer streamlined, user-friendly versions of privacy policies. In 2016, the CAC provided broadband labels "to provide consumers of mobile and fixed broadband Internet service with easy-to-

163. Lottenberg, *supra* note 159.
164. *Id.*
165. *See id.*
166. *See* Chivers, *supra* note 77.
167. Bassan, *supra* note 112, at 8.
168. *Id.* at 8-9.

understand information about price and performance."[169] These labels provided consumers with information about the price, speed, and reliability of broadband services, and they served as a "'safe harbor'" for meeting the Open Internet transparency rules.[170] These rules "require broadband Internet service providers to disclose this information to consumers in an accurate, understandable and easy-to-find manner."[171] The FCC should direct the CAC to provide similar guidance on how health care providers can provide easy-to-understand information regarding the possible security risks to patient privacy when using telehealth services. Such guidance should also inform patients of ways they can limit possible security risks.

4. Agency Coordination

Finally, HIPAA should be reformed to include agency coordination. The FCC and HHS should work together to effectively enforce and implement HIPAA. Given HHS' mission to "enhance the health and well-being of all Americans"[172] and the FCC's expertise in regulating and implementing communications law, these two agencies are best positioned to protect patient privacy and ensure telehealth services are safe and effective.

D. The Proposal to Reform HIPAA is Limited by Security Risks Posed by Patients Using Telehealth Services, but Health Care Providers Can Mitigate These Risks

Although covered entities and business associates are legally bound to provide secure and safe platforms for telehealth services, patients can also pose security risks to themselves. Thus, HIPAA does not completely mitigate security risks. Patients pose security risks by using public Wi-Fi, sending information on unsecure websites, and accessing telehealth services outside of a private location.[173] Public Wi-Fi typically uses unsecure networks, which could allow unauthorized people to read data sent from a computer.[174] Using public Wi-Fi also risks that someone could put malware onto a computer.[175] Additionally, sending information on unsecure websites and using telehealth

169. Press Release, FCC, FCC Unveils Consumer Broadband Labels to Provide Greater Transparency to Consumers 1 (Apr. 4, 2016), https://docs.fcc.gov/public/attachments/DOC-338708A1.pdf [https://perma.cc/J3PN-666L].

170. *Id.*

171. *Id.*

172. *About HHS*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/about/index.html [https://perma.cc/QNB8-9JDW] (last visited Jan. 30, 2022).

173. *See Telehealth Privacy for Patients*, HEALTH RES. & SERVS. ADMIN., https://telehealth.hhs.gov/patients/telehealth-privacy-for-patients/ [https://perma.cc/43FC-CY5W] (last updated Dec. 15, 2021).

174. *The Risks of Public Wi-Fi*, NORTONLIFELOCK (May 26, 2018), https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html [https://perma.cc/U5DG-TF3E].

175. *Id.*

services outside of a private location heightens the risk that someone could read a patient's PHI.

Although health care providers are unlikely to completely reduce the security risks patients may pose, there are ways that health care providers can help patients mitigate those risks. Prior to the telehealth visit, health care providers can expressly inform patients to avoid using public Wi-Fi and to attend telehealth appointments from a private location. Additionally, health care providers can advise patients what to look for to ensure that the website or platform is secure. Moreover, health care providers should present patients with a list of possible risks from using public Wi-Fi or unsecure websites. Finally, health care providers should provide patients with the best practices list, including firewalls and two-factor authentication. By explicitly notifying patients of practices that could pose security risks to PHI, health care providers can mitigate security risks and limit exposure to liability.

IV. CONCLUSION

The onset of the COVID-19 pandemic has highlighted ways in which HIPAA should be reformed to address issues with using telehealth services. HHS' Notification of Relaxed Enforcement allows health care providers to offer telehealth services through common platforms such as Facebook Messenger and FaceTime, and thus patients with limited access to more advanced video platforms can connect with their health care team without in-person contact. Although this increased flexibility allows patients and health care providers to easily connect, it also raises privacy concerns. The Notification of Relaxed Enforcement states that OCR will use its enforcement discretion to determine whether to penalize health care providers who utilize non-HIPAA compliant platforms. Allowing providers to use non-HIPAA compliant platforms for telehealth services invites possible security risks to patients' private health information.

The risks highlighted from the use of non-HIPAA compliant platforms also highlights inadequacies in HIPAA as it stands outside of a public health emergency. HIPAA does not mandate covered entities to adopt specific security measures; rather, covered entities only need to adopt security measures after a risk to PHI has been identified. Thus, HIPAA should be reformed to maintain the flexibility of video platforms while mandating specific security measures and providing guidance for best practices in offering telehealth services.

Some Added Security: Applying Lessons from Bankruptcy Law to Strengthen the Collection of Consumer Fraud Penalties

Nicolas A. Florio*

TABLE OF CONTENTS

* J.D., May 2023, The George Washington University Law School; Managing Editor, *Federal Communications Law Journal*, Volume 75; B.A., May 2019, Economics, Fordham University. I would like to thank the staff and Editorial Board members of FCLJ, as well as Professor Michael Beder, for their invaluable assistance with this Note. I would also like to thank all those I have met throughout law school that took the time to invest in my success in any way. And finally, I extend my love and gratitude to my wonderful parents for their unconditional love and support.

I. INTRODUCTION

A government agency's ability to collect fines is a telling indicator of whether an agency is more bark than bite. If an agency cannot practically collect its fines, its constituency takes notice. A constituent's cost of punishment suddenly becomes a predictable metric that can be strategically mitigated, and the agency loses its leverage as a regulator and enforcer over time, while the constituency's maligned behaviors persist. One need only look to the current state of the telecommunications industry to see a potential microcosm of this dynamic.

The Federal Communications Commission ("FCC") infamously struggles to practically collect the civil penalties it imposes on its constituents for consumer fraud.[1] Despite enforcement assistance from the Federal Trade Commission ("FTC"),[2] the FCC's shortcomings have conditioned a telecommunications industry that no longer blinks at the announcement of enormous consumer fraud penalties.[3] Sensational headlines often trumpet massive fines against the industry's largest corporations, but they do not capture reality.[4] In truth, these penalties might go uncollected for several years.[5] As a former Director of Research at the Consumer Federation of America once lamented: "When the lion roars, the gazelles run. The problem is that if the lion roars too much and never eats a meal, the gazelles will stop running."[6]

Indeed, the gazelles of the telecommunications industry have stopped running, but there is greater cause for concern on the horizon. An unresolved disagreement amongst federal courts over a particular section of the United States Bankruptcy Code ("the Code") might offer telecommunications companies a way to completely erase their consumer fraud penalties through Chapter 11 reorganization, further upsetting the FCC and FTC's practical ability to collect their fines.[7] While the United States' bankruptcy system is not intended as a means for corporate debtors to escape accountability for consumer fraud, a general understanding of the corporate bankruptcy process reveals how such an opportunity can arise.

---

1. *See* Alex Byers, *FCC Proposes Millions in Fines, Collects $0*, POLITICO (Nov. 23, 2015, 6:01 PM), https://www.politico.com/story/2015/11/fcc-fine-enforcement-scrutiny-216121 [https://perma.cc/L9PV-DQUE].

2. *See* Press Release, Fed. Trade Comm'n, FTC Enforcement Actions Continue to Target "Crammers" (July 16, 1998), https://www.ftc.gov/news-events/press-releases/1998/07/ftc-enforcement-actions-continue-target-crammers [https://perma.cc/QP6X-QNZW].

3. *See* Byers, *supra* note 1.

4. *See, e.g.*, Diane Bartz & Alina Selyukh, *AT&T to Pay $105 Million to Settle Charges It 'Crammed' Phone Bills*, REUTERS (Oct. 8, 2014, 11:52 AM), https://www.reuters.com/article/us-at-t-cramming-settlement/att-to-pay-105-million-to-settle-charges-it-crammed-phone-bills-idINKCN0HX1QP20141008 [https://perma.cc/R528-CMKA].

5. *See* Byers, *supra* note 1.

6. *Id.*

7. *See* Douglas Mentes, *Reorganized Telecom Company Wipes Out $2 Million FCC Penalty*, 17 No. 6 WESTLAW J. BANKR. 1 (2020).

When a distressed corporation files for relief under Chapter 11 of the Code, the corporation becomes a federally protected debtor.[8] In turn, the government can no longer collect its penalty claims against the debtor corporation.[9] This gives the corporation time to implement a plan of reorganization that restructures its capital arrangements and permits it to exit as a solvent entity.[10] Any creditor whose claim against the corporation is not backed by collateral is classified as an unsecured creditor[11] and ranks low within the creditor hierarchy without any guarantee of recovery.[12] Consumer fraud penalties levied by the FCC and FTC fall under unsecured status.[13] If the debtor corporation seeks to discharge the penalty in its plan of reorganization, it may very well succeed in doing so, despite the fact that that debt was the consequence of fraud.[14] For the FCC and FTC, this is the worst case scenario.

A recent case in the United States Bankruptcy Court for the Southern District of New York brought this exact fear to light. In 2019, Fusion Connect, Inc., a telecommunications provider, filed for bankruptcy and nearly discharged a $2.1 million FCC consumer fraud penalty levied via consent decree.[15] The bankruptcy judge ruled that where the government itself is not an injured victim of the fraudulent scheme, the penalty is dischargeable.[16] But on appeal, the bankruptcy court's ruling was reversed,[17] rekindling an awareness within the federal judiciary of disagreement.[18] And it has significant potential side effects.

Practitioners fear that the *In re Fusion Connect* saga serves as a precursor to what will soon become common practice in the telecommunications industry.[19] Telecommunications companies may begin to test courts with bankruptcy spinoffs.[20] Here, they may offload their consumer fraud penalties into subsidiaries solely for the purpose of discharging them in bankruptcy.[21] And this will not only perpetuate the FCC and FTC's struggles to collect their penalties, but also the agencies' ability to curb mass market consumer fraud. To address these problems, this Note argues that by

8. *See* 11 U.S.C. § 301.
9. 11 U.S.C. § 362.
10. *See* Ralph R. Mabey & Patrick S. Malone, *Chapter 11 Reorganization of Utility Companies*, 22 ENERGY L.J. 277, 282-83 (2001) (providing a background section on general concepts of Chapter 11 bankruptcy).
11. 11 U.S.C. § 506(a)(1).
12. 11 U.S.C. § 1129(b)(2).
13. 11 U.S.C. § 507(a)(8)(G).
14. *See In re* Fusion Connect, Inc., 617 B.R. 36, 44-45 (Bankr. S.D.N.Y. 2020), *rev'd*, 634 B.R. 22 (S.D.N.Y. 2021).
15. *Id.* at 39.
16. *Id.* at 44-45.
17. *In re* Fusion Connect, Inc., 634 B.R. 22, 24 (S.D.N.Y. 2021).
18. Michael L. Cook, *Appellate Court Holds FCC Penalty Claim Survives Chapter 11 Corporate Debtor's Discharge*, SCHULTE ROTH & ZABEL (Sept. 14, 2021), https://www.srz.com/resources/appellate-court-holds-fcc-penalty-claim-survives-chapter-11.html [https://perma.cc/7ZCW-KD3L].
19. *See id.*
20. *See id.*
21. *In re Fusion Connect, Inc.*, 634 B.R. at 38.

modifying the way the FCC and FTC issue their consumer fraud penalties, the agencies can not only protect their claims in bankruptcy but strengthen their overall ability to collect their fines and disincentivize default.

This Note first requires an in-depth background discussion. Section II.A.1 elucidates the relevant framework of Chapter 11 bankruptcy reorganization. Section II.A.2 details the relevant statutes governing the nondischargeability of certain debts. Section II.B then illuminates the *In re Fusion Connect* saga's near successful exploitation of Section 523(a)(2)(A) of the Code. From here, Section II.C.1 explores why the FCC and FTC should heed the warnings identified in *In re Fusion Connect*, namely bankruptcy spinoffs and liability offloading. Section II.C.2 then concludes the background with an examination of consumer fraud in the telecommunications industry.

This Note then proposes a solution that focuses solely on those FCC and FTC penalties levied via consent decrees, as seen in *In re Fusion Connect*. Section III.A explains that the best resolution requires two modifications to the way these agencies draft their agreements. Section III.B suggests that consent decrees should first reduce offloading concerns by stipulating that their penalties cannot be assigned to subsidiaries, independent spinoffs, and other third parties. Section III.C then proposes that consent decrees should attach the corporations' FCC licenses to the penalties to create security interests that characterize the government as a secured creditor. Such a plan offers an effective means at addressing the issues rediscovered by the *In re Fusion Connect* saga and presents a sustainable solution grounded in undisputed bankruptcy law.

II. BACKGROUND

A. The General Framework of Corporate Bankruptcy Law

1. The Mechanics of Chapter 11 Reorganization

Bankruptcy is a unique legal process codified under federal law that permits entities distressed by crippling debts the opportunity to seek relief from their obligations to creditors.[22] It is one of the few contexts where judicial intervention is not punitive, but rather seeks to secure a better outcome than would otherwise be received by all parties without the court's assistance.[23] This is especially the case in "reorganization" bankruptcies, such as those filed under Chapter 11 of the Code.[24] In many ways, a reorganization arguably transforms the court's role into that of a broker, always concerned about striking the deal. Reorganization bankruptcy involves a highly sophisticated framework of procedure, litigation, negotiated transactions, and business decisions. It employs its own terms of the trade to make sense of it all. Accordingly, this Note narrowly examines only a few points within that

22. *See* Mabey & Malone, *supra* note 10, at 277-79.
23. *See id.* at 282.
24. *See id.* at 278.

complex framework and walks through a typical Chapter 11 bankruptcy reorganization from beginning to end.

A bankruptcy proceeding under Chapter 11 of the Code commences with the filing of a Chapter 11 petition in a federal bankruptcy court.[25] A bankruptcy court is a unit of the federal judiciary and is endowed with subject matter jurisdiction over most bankruptcy case matters under Article I of the United States Constitution.[26] Therefore, all bankruptcy law is federal law and subject to the review of federal appellate courts.[27] Bankruptcy appeals, however, have a unique process that, depending on the jurisdiction, may escalate via different paths.[28] For instance, decisions and orders issued by certain bankruptcy courts are generally appealed directly to their corresponding federal district courts.[29] As such, a decision by the United States Bankruptcy Court for the Southern District of New York is generally appealed to the United States District Court for the Southern District of New York.[30] However, the First, Sixth, Eighth, Ninth, and Tenth Circuits employ Bankruptcy Appellate Panels ("BAPs") to review bankruptcy court decisions.[31] Such panels are authorized under 28 U.S.C. § 158(b) and consist typically of three bankruptcy judges appointed by their respective circuit courts.[32] Bankruptcy appeals reviewed by the district court or BAPs may then be appealed up to the circuit courts and then to the United States Supreme Court, following the traditional path of federal appellate review.[33]

A Chapter 11 bankruptcy petition contains itemized schedules of the distressed corporation's financial affairs.[34] This includes itemized schedules of the corporation's assets and liabilities.[35] Assets include tangible assets, as well as ownership interests, revenue contracts, and other non-trivial property that falls under the bankruptcy estate pursuant to 11 U.S.C. § 541.[36] Liabilities include any claims to money owed by the corporation to its creditors, which may be loans, bond payments, contractual obligations, lawsuit judgments, or government civil penalties.[37] This is where the relevant creditors to the bankruptcy petition become apparent, establishing a picture of the corporation's overall capital structure.[38] Here, the assets usable for the generation of funds toward the reorganization are set against the corporation's

25. 11 U.S.C. § 301.
26. U.S. CONST. art. I, § 8, cl. 4; 28 U.S.C. § 151.
27. U.S. CONST. art. I, § 8, cl. 4; *see* 28 U.S.C. § 158(d).
28. *See generally* 28 U.S.C. § 158.
29. 28 U.S.C. § 158(a).
30. *See, e.g.*, *In re* Fusion Connect, Inc., 617 B.R. 36, 40 (Bankr. S.D.N.Y. 2020), *rev'd*, 634 B.R. 22 (S.D.N.Y. 2021).
31. *Court Insider: What Is a Bankruptcy Appellate Panel?*, ADMIN. OFF. U.S. CTS. (Nov. 26, 2012), https://www.uscourts.gov/news/2012/11/26/court-insider-what-bankruptcy-appellate-panel [https://perma.cc/2Z8E-SMNV].
32. 28 U.S.C. § 158(b).
33. 28 U.S.C. § 158(d); FED. R. APP. P. 3, 4.
34. FED. R. BANKR. P. 1007(b)(1).
35. FED. R. BANKR. P. 1007(b)(1)(D).
36. 11 U.S.C. § 541.
37. *See* 11 U.S.C. § 101(5), (12).
38. *See generally* 11 U.S.C. § 521(a)(1)(A).

total debts.[39] Within that capital structure exists a "fulcrum," or the point at which value breaks.[40] In other words, creditors who sit above the fulcrum stand to recover the full value of their claims against the corporation.[41] Those who sit below the fulcrum are at risk of only receiving partial recovery or stand to receive no recovery at all.[42]

The bankruptcy petition separately identifies a list of creditors according to their position within the hierarchy governed by what is called the "absolute priority rule."[43] The absolute priority rule states that a subordinate claim may not be paid recovery until all relative superior claims are paid their recovery in full.[44] Generally speaking, debt is senior to equity.[45] Therefore, creditors are superior to shareholders.[46] The creditor class is separately striated into several categories within the hierarchy.[47] It is most important to distinguish between secured and unsecured creditors. A secured creditor holds a claim against the corporation that has some form of collateral attached to it as security.[48] An unsecured creditor holds a claim against the corporation that does not have any attached collateral.[49] A secured creditor is superior to an unsecured creditor under the absolute priority rule.[50] Generally, unsecured creditors are at higher risk of receiving partial or no recovery of their claims in the bankruptcy reorganization.[51] A secured creditor with a large claim will generally be made whole and may have a lot of influence in the bankruptcy's trajectory.[52]

One of the most important mechanisms of Chapter 11 bankruptcy is the automatic stay. Upon the bankruptcy petition's filing, regardless of its sufficiency or completeness, an automatic stay immediately goes into effect pursuant to 11 U.S.C. § 362.[53] The automatic stay temporarily prevents any creditor, collection agency, or government agency from collecting or pursuing any pre-petition claims against the corporation.[54] The Code makes an exception for certain government actions under 11 U.S.C. § 362(b)(4), stating that the automatic stay does not apply to "the commencement or continuation

---

39. *See* 11 U.S.C. § 521(a)(1)(B)(i); *see also Chapter 11 – Bankruptcy Basics*, ADMIN. OFF. U.S. CTS., https://www.uscourts.gov/services-forms/bankruptcy/bankruptcy-basics/chapter-11-bankruptcy-basics [https://perma.cc/4U6L-AC7K] (last visited Sept. 18, 2022).

40. *See* Nicholas Ortiz, *What Is a Fulcrum Security in Bankruptcy?*, BANKR. L. NETWORK (Dec. 23, 2011, 12:04 PM), https://bankruptcylawnetwork.com/what-is-a-fulcrum-security-in-bankruptcy/ [https://perma.cc/D8ZE-ELPA].

41. *See id.*

42. *See id.*

43. *See* 11 U.S.C. §§ 521(a)(1)(A), 1129(b)(2).

44. *See* 11 U.S.C. § 1129(b)(2).

45. *Id.*

46. *See id.*

47. *See id.*

48. *See* 11 U.S.C. § 506(a)(1).

49. *See id.*

50. 11 U.S.C. § 1129(b)(2).

51. *See* Ortiz, *supra* note 40.

52. *See id.*

53. *See* 11 U.S.C. § 362.

54. *See id.*

of an action or proceeding by a governmental unit . . . to enforce such governmental unit's . . . police and regulatory power, including the enforcement of a judgment other than a money judgment, obtained in an action or proceeding by the governmental unit to enforce such governmental unit's . . . police or regulatory power."[55] This carve-out is important because it contains an exception to an exception. By excepting government actions other than money judgment collections, the Code effectively stays the collection of government penalties.[56] All claims falling under the freeze of the automatic stay therefore remain frozen until their fates are determined by a subsequent confirmed plan of reorganization.[57]

The debtor corporation ultimately seeks to confirm a plan of reorganization that restructures the terms of the corporation's outstanding obligations.[58] The corporation, known officially upon the petition's filing as a Debtor-In-Possession,[59] has 120 days from the petition date to exclusively propose its own plan of reorganization.[60] During this time, not even the creditors can propose their own plans.[61] Pursuant to 11 U.S.C. § 1123(a)-(b), all proposed plans must provide for the treatment of every identified claim holder.[62] The debtor corporation additionally has 180 days from the petition date to obtain acceptances to its proposed plan.[63] After these periods lapse, any creditor may propose its own plan for acceptance.[64] Acceptances are submitted by vote according to class of claim.[65] Claim classes are generally categorized as impaired and unimpaired.[66] Claims belonging to the unimpaired class sit above the fulcrum, while claims belonging to the impaired classes sit at or below the fulcrum.[67] Claims belonging to the unimpaired class are automatically considered accepting of the plan.[68] Votes therefore need only be solicited from creditors holding claims under the impaired classes.[69] The proposed plan wins acceptance from an impaired class if it receives acceptance votes from creditors holding at least two-thirds of the overall debt within that class and if those votes constitute a majority of the total creditors within that class.[70] So long as the proposed plan receives acceptance from at least one class of impaired creditors, the plan may be confirmed by order of the bankruptcy court.[71]

---

55. 11 U.S.C. § 362(b)(4).
56. *See id.*
57. *See* 11 U.S.C. §§ 362(c)(1), 1327(b).
58. *See* Mabey & Malone, *supra* note 10.
59. 11 U.S.C. § 1107.
60. 11 U.S.C. § 1121(b).
61. *See id.*
62. 11 U.S.C. § 1123(a)-(b).
63. 11 U.S.C. § 1121(c)(3).
64. 11 U.S.C. § 1121(c).
65. 11 U.S.C. § 1126(c).
66. *See* 11 U.S.C. § 1126(f).
67. *See* Ortiz, *supra* note 40.
68. 11 U.S.C. § 1126(f).
69. *See id.*
70. 11 U.S.C. § 1126(c).
71. *See id.*

Upon confirmation of the corporation's plan of reorganization, the bankruptcy court orders a discharge of the corporation's pre-petition liabilities pursuant to the plan.[72] The discharge effectively cancels all impaired debts slated for zero recovery under the plan.[73] Thereon, the corporation is legally bound by the plan and must meet its restructured payments and contractual obligations as stipulated.[74] As discussed, depending on the terms of the plan, not all creditors will be made whole, especially creditors whose claims are not backed by collateral.[75] The voting structure governing the plan's confirmation provides for the approval of the plan, despite the existence of many dissenting creditors.[76] And because any given corporate reorganization may implicate millions or billions of dollars of debt and distressed assets across dozens of creditors and third parties, litigation inevitably arises to challenge a debt's dischargeability.

2. 11 U.S.C. § 523 Exceptions to Discharge

Section 523 of the Code codifies which claims cannot be discharged in bankruptcy.[77] Despite the tremendous care with which Congress aimed to draft this section, it is still steeped in controversy, especially in the context of claims implicating fraud. Often, the litigation invoking a Section 523 exception is more a dispute over the interpretation of the statute as opposed to the interpretation of the facts underlying the claim. A survey of this statute's framework reveals why.

Any plan of reorganization that calls for the discharge of a debt may be challenged by the creditor in a separate adversary proceeding.[78] In such circumstances, the plaintiff in the adversary proceeding is typically a creditor holding an impaired claim against the debtor corporation, and the debtor corporation is generally the defendant.[79] The plaintiff commences the adversary proceeding, like any other civil lawsuit,[80] and seeks relief in the form of a friendly treatment of its claim in the reorganization.[81] Adversary proceedings can address various contested matters arising under the bankruptcy from the validity of an interest to the subordination of a debt.[82] The adversary proceeding can also potentially foreclose further litigation of

72. *See* 11 U.S.C. § 1141(d)(1)(a).
73. *See* 11 U.S.C. § 1141(a), (c), (d)(1)(A).
74. 11 U.S.C. § 1141(a).
75. *See* Ortiz, *supra* note 40.
76. *See* 11 U.S.C. § 1126(c).
77. *See* 11 U.S.C. § 523.
78. *See* FED. R. BANKR. P. 7001.
79. *See, e.g.*, *In re* Fusion Connect, Inc., 617 B.R. 36, 40 (Bankr. S.D.N.Y. 2020), *rev'd*, 634 B.R. 22 (S.D.N.Y. 2021).
80. *See* FED. R. BANKR. P. 7003.
81. *See* FED. R. BANKR. P. 7001.
82. *See* FED. R. BANKR. P. 7001(2), (8).

the matter.[83] Therefore, if Creditor A proposes a plan that is hostile to Creditor B's claim against the debtor corporation, Creditor B can directly litigate against the debtor corporation to seek lasting protection and a final determination of its claim's fate.[84]

Creditors often argue for the protection of their claims by asserting that their claims are excepted from discharge.[85] The Code specifically enumerates nineteen different categories of claims that are not dischargeable under Section 523.[86] These categories range from debts arising from domestic support obligations and vehicular personal injury to federal securities law violations.[87] This Note principally examines the exception to discharge provided under Section 523(a)(2)(A) of the Code, which concerns debts arising from fraudulent activity.[88]

Section 523(a)(2)(A) of the Code bars the discharge of a debt "obtained by . . . false pretenses, a false representation, or actual fraud . . . ."[89] However, Section 523 statutory exceptions to discharge pertain only to "individual[s]" and do not reference corporate entities.[90] This distinction is important. Case law widely acknowledges that the term "individual" in the context of the Section 523 exceptions applies only to people who file for consumer bankruptcy protection.[91] Accordingly, Congress passed additional statutes designed to apply the Section 523 exceptions to corporate debtors and added Section 1141(d)(6)(A) to the Code in 2005.[92] This particular statute bars a "debtor that is a corporation" from a discharge of "any debt . . . of a kind specified in paragraph (2)(A) or (2)(B) of Section 523(a) that is owed to a domestic government unit . . . ."[93] However, what was thought to be strong and clear statutory language constructed to hold defrauding corporations accountable to government penalties and fines was actually found to be grossly underdeveloped.

Where the government filed an adversary proceeding on a Section 523(a)(2)(A) claim as the victim of the corporate debtor's fraud, the law and surrounding jurisprudence was well established, consistently finding the debt

83. *See, e.g.*, 10 COLLIER ON BANKRUPTCY ¶ 7001.07 (16th ed. 2022) ("If the debt . . . is held dischargeable by the court after trial, the creditor holding that debt is thereafter barred from suing on it in another court or seeking to enforce it through legal process. Should the creditor commence or continue a suit on the debt thereafter, any judgment obtained is rendered null and void."); *see also* FED. R. BANKR. P. 7001(6).
84. *See* FED. R. BANKR. P. 7001.
85. *See* 11 U.S.C. § 523.
86. *See* 11 U.S.C. § 523(a).
87. *See id.*
88. *See* 11 U.S.C. § 523(a)(2)(A).
89. *Id.*
90. 11 U.S.C. § 523(a).
91. 4 COLLIER ON BANKRUPTCY ¶ 523.04 (16th ed. 2022).
92. *See In re Fusion Connect, Inc.*, 617 B.R. at 40.
93. 11 U.S.C. § 1141(d)(6)(A).

nondischargeable.[94] But when the government was not the victim of the fraud, but was instead attempting to collect a penalty levied for the debtor's fraud against consumers or some other third party, the Code began to unravel and divide federal jurisprudence across circuit jurisdictions.[95]

B. The In re Fusion Connect *Saga*

The apparent underdevelopment of Section 523(a)(2)(A) of the Code has recently returned as a hot button subject in the bankruptcy practice. A recent Chapter 11 case in the United States Bankruptcy Court for the Southern District of New York strained bankruptcy jurisprudence on the statute. The case, *In re Fusion Connect*, rekindled an awareness of disagreement among federal courts on whether government consumer fraud penalties are dischargeable in bankruptcy pursuant to Section 523(a)(2)(A).[96]

In 2015, the Enforcement Bureau of the FCC launched an investigation into allegations of consumer fraud committed by Birch Communications Inc. ("Birch"), better known by the name of its successor, Fusion Connect Inc. ("Fusion").[97] The results of the FCC's investigation concluded that Birch had defrauded its customers, many of which were small businesses.[98] By 2016, Birch had entered into a consent decree by an order of the FCC and agreed to pay the United States an unsecured civil penalty of $4.2 million over five years.[99] For three years, Birch met its monthly obligations pursuant to the consent decree and by 2019 had paid nearly half of its civil penalty.[100] However, the FCC's blissfully passive enforcement of the consent decree would soon come to an end. Bound by the consent decree's assignment of liability, Fusion assumed responsibility for the outstanding penalty in 2018 when it merged with Birch's parent company.[101] And in June of 2019, Fusion voluntarily filed for Chapter 11 in the United States Bankruptcy Court for the Southern District of New York.[102]

Fusion's plan of reorganization called for the discharge of the $2.1 million FCC penalty left unpaid to the United States.[103] The Government commenced an adversary proceeding to challenge Fusion's proposed treatment of the penalty under the plan, claiming that the penalty was

94. *See, e.g.*, Andrews v. Michigan Unemployment Ins. Agency, 891 F.3d 245, 249-50 (6th Cir. 2018) (citing Cohen v. de la Cruz, 523 U.S. 213 (1998)); *see also In re Fusion Connect, Inc.*, 617 B.R. at 41 ("[W]here a governmental unit is the victim of actual fraud, a non-compensatory penalty that forms part of the award is non-dischargeable under section 523(a)(2)(A) . . . .").

95. *See* Anupama Yerramalli et al., *Fines for Defrauding Consumers are Dischargeable*, AM. BANKR. INST. J., Sept. 2020, at 6, 6.

96. *See* Mentes, *supra* note 7, at 1.

97. *See In re* Fusion Connect, Inc., 617 B.R. 36, 38 (Bankr. S.D.N.Y. 2020), *rev'd*, 634 B.R. 22 (S.D.N.Y. 2021).

98. *Id.*

99. *Id.* at 38-39.

100. *Id.* at 39.

101. *Id.*

102. *Id.*

103. *In re Fusion Connect, Inc.*, 617 B.R. at 39.

nondischargeable pursuant to Section 523(a)(2)(A) of the Code[104] and that Birch's FCC consumer fraud penalty constituted a debt "obtained by . . . false pretenses, a false representation, or actual fraud . . . ."[105]

Judge Stuart Bernstein ruled that the unpaid FCC penalty was indeed dischargeable and reasoned that because the FCC itself was not an actual victim of Birch's fraud, Section 523(a)(2)(A) did not bar the penalty's discharge.[106] Judge Bernstein explained that the Code's conception of actual fraud "is tethered to the common law conception of fraud" and cannot substantiate a claim in "the absence of a misrepresentation to the FCC."[107] Citing two United States Supreme Court cases, *Cohen v. de la Cruz* and *Husky International Electronics, Inc. v. Ritz*, Judge Bernstein noted that in both cases, the plaintiffs were the actual defrauded victims and "neither decision extends the notion of common law fraud to someone who has not been defrauded and has not suffered a pecuniary loss."[108] Judge Bernstein additionally borrowed from an analogous 2020 decision from the Delaware Bankruptcy Court that was affirmed on appeal to the United States District Court of Delaware.[109] The case, *In re Exide Technologies*, held that government fines levied for the violation of environmental regulations could be discharged in a corporate reorganization plan.[110] While no fraud was alleged in that case, the Bankruptcy Court offered its thoughts on how it would have ruled.[111] The District Court of Delaware agreed with the Bankruptcy Court's reasoning, affirming that "[Section] 523(a)(2)(A) is not applicable . . . because the claim did not satisfy a prima facie element of fraud: 'that a *creditor* sustained loss and damages as a proximate result of the misrepresentations having been made.'"[112] Following *Cohen*, the Delaware District Court affirmed that this principle required a debt to be traceable to a fraud against the creditor itself.[113]

On appeal to the United States District Court for the Southern District of New York, Judge Bernstein's findings were reversed.[114] The District Court interpreted *Cohen* in a different manner.[115] It particularly emphasized the breadth of *Cohen*'s language in its holding that "[Section] 523(a)(2)(A) bars the discharge of all liability arising from fraud."[116] However, the Supreme Court had originally handed down this ruling to resolve the issue of whether Section 523(a)(2)(A) applied to treble damages imposed on top of actual

104. *Id.*
105. 11 U.S.C. § 523(a)(2)(A).
106. *In re Fusion Connect, Inc.*, 617 B.R. 36, at 44-45.
107. *Id.* at 44.
108. *Id.* at 45.
109. *Id.* at 42.
110. *Id.*
111. *Id.*
112. *In re* Exide Techs., 613 B.R. 79, 87 (D. Del. 2020) (quoting *In re* Exide Techs., 601 B.R. 271, 282 (Bankr. D. Del. 2019)) (emphasis added).
113. *Id.* at 88.
114. *In re* Fusion Connect, Inc., 634 B.R. 22, 24 (S.D.N.Y. 2021).
115. *Id.* at 30-31.
116. *Id.* at 31 (quoting Cohen v. de la Cruz, 523 U.S. 213, 222 (1998)).

damages for judgements arising from fraud.[117] In other words, the pertinent language of *Cohen* applies to claim calculations and does not necessarily inform what type of fraudulent conduct satisfies Section 523(a)(2)(A).[118] But according to the District Court's reasoning, the *Cohen* analysis extended Section 523(a)(2)(A) to cover the FCC penalty as a qualifying debt related to the original fraud, and consequently held "that the FCC Penalty fit[] within the § 523(a)(2)(A) exception to dischargeability."[119]

Despite this reversal, the *In re Fusion Connect* saga revived an awareness of the apparent disagreement surrounding the dischargeability of government penalties levied to punish fraud.[120] Fusion ultimately did not appeal the District Court's decision to the United States Court of Appeals for the Second Circuit. However, this case represents the SDNY Bankruptcy Court and District Court's first commentaries on the question. It is unknown whether Judge Bernstein's opinion is shared amongst any of the other judges under the Second Circuit judiciary. Regardless, the Second Circuit has yet to rule on the question, and there is an apparent disagreement between the Southern District of New York and Delaware over how far *Cohen* should stretch jurisprudence on 523(a)(2)(A) regarding the nondischargeability of government penalties for fraud.[121] Given that these districts are among the country's most influential bankruptcy courts, such a divide might prompt the Supreme Court to eventually address the issue with precision and put the ambiguity to rest.

C. Causes for Concern

1. Looming Concerns over Liability Offloading in Corporate Bankruptcy

One of the discernable concerns coming out of the *In re Fusion Connect* saga is the implications it might have on telecommunications providers' treatment of federal penalties. Where bankruptcy courts are particularly sympathetic towards corporate debtors facing large government penalties, strategic offloading becomes an attractive measure to evade punishment for consumer fraud.[122] The timing here is especially concerning because in October 2021, Johnson & Johnson initiated a controversial bankruptcy offload to distance itself from its talcum powder mass tort liability.[123] This has revived considerable concern and debate over the practice.[124]

117. Cohen v. de la Cruz, 523 U.S. 213, 215 (1998).
118. *Id.* at 222.
119. *In re Fusion Connect, Inc.*, 634 B.R. at 32.
120. Cook, *supra* note 18.
121. *See id.*
122. *See In re* Fusion Connect, Inc., 634 B.R. 22, 38 (S.D.N.Y. 2021).
123. Mike Spector & Dan Levine, *J&J Puts Talc Liabilities into Bankruptcy*, REUTERS (Oct. 15, 2021, 11:50 AM), https://www.reuters.com/business/healthcare-pharmaceuticals/jj-unit-manage-talc-claims-files-bankruptcy-protection-2021-10-14/ [https://perma.cc/X3XP-7LGS].
124. *See id.*

Offloading is the term used to describe the scenario when a corporation creates a subsidiary whose purpose is to accept a transfer of liability and file for bankruptcy protection.[125] While this strategy was designed to shield larger, established corporate entities from failing due to liabilities accrued from unanticipated environmental disasters and product recalls, many criticize the strategy as giving corporations a way to escape accountability for their injurious activities, especially in the context of consumer fraud.[126] As Judge Paul A. Engelmayer noted in his decision reversing Judge Bernstein's ruling in *In re Fusion Connect*, "statutory construction permitting a company—or its assignee—to shed a regulatory fraud penalty in this manner could invite mischief . . . [and] incent the strategic offloading of such a liability onto a successor entity primed soon to file for reorganization under chapter 11."[127] He further added, "The risk of such mischief may be all the greater given that the company . . . had a recent history of fraud."[128] Accordingly, policy implications explicitly warn that telecommunications providers already predisposed to commit consumer fraud may also exploit the perverse incentives offered by liability offloading.[129]

In such scenarios, any corporation liable for millions of dollars in FCC or FTC consumer fraud penalties may create a subsidiary to take on the liability.[130] Once the subsidiary files for bankruptcy, the FCC's ability to collect the judgment is frozen due to the automatic stay.[131] After months or even years of delayed litigation, the debtor subsidiary may seek to confirm a plan that discharges the penalty. Even if not discharged, at best, the penalty's collection is delayed. But in all likelihood, the FCC and debtor subsidiary could enter negotiations on the matter and settle at a much lower amount, effectively undermining the government's ability to collect damages for the debtor's violation of federal law. Such a reality is unsustainable and should no longer be tolerated by the federal government, especially given how pervasive consumer fraud is within the telecommunications industry.[132]

2. Mass Market Consumer Fraud in the Telecommunications Industry

Another discernable concern arising from the *In re Fusion Connect* saga is that, given the potential for telecommunications companies to escape FCC and FTC consumer fraud penalties through reorganization or bankruptcy offloads, consumer fraud in the telecommunications industry will persist

125. *Id.*

126. *See generally* DAVID F. LARCKER ET AL., STAN. CLOSER LOOK SERIES, ENVIRONMENTAL SPINOFFS: THE ATTEMPT TO DUMP LIABILITY THROUGH SPIN AND BANKRUPTCY (2020), https://www.gsb.stanford.edu/sites/default/files/publication-pdf/cgri-closer-look-87-environmental-spinoffs_0.pdf [https://perma.cc/2EXG-CN3H].

127. *In re Fusion Connect, Inc.*, 634 B.R. at 36.

128. *Id.* at 36-37.

129. *See id.*

130. *See id.*

131. *See* 11 U.S.C. § 362(b)(4).

132. *See* discussion *infra* Section II.C.2.

without relative consequence. The consumer fraud at the center of the *In re Fusion Connect* case is indicative of a larger problem within the telecommunications industry. Among the most common fraudulent activities committed against consumers by telecommunications providers are known by their industry terms, "slamming" and "cramming."[133] "Slamming" describes the fraudulent practice of changing consumers' long distance carriers without their authorization and without proper verification.[134] The harm received by the victims of this activity comes in the form of "cramming," where consumers are charged for the long distance services and fees they did not authorize.[135] Many consumers do not become aware of their injury until they receive their telephone bills.[136]

Statistics regarding these consumer fraud practices in the telecommunications industry are staggering. Every few years, the FTC conducts a report on consumer fraud in the United States.[137] The most recent study in 2017 found that as many as 2.4 million Americans were victims of unauthorized billing for Internet services.[138] In addition, as many as 3.7 million Americans were victims of unauthorized billing or payment for cell phone services.[139] And the FCC separately estimates that tens of millions of American households have been injured from cramming alone.[140] Sadly, many of the perpetrators are trusted carriers. In 2019, AT&T settled with the FTC to refund its consumers $60 million for misrepresenting services.[141]

---

133. *See* Ian D. Volner, *FCC Tackles "Slamming and Cramming"*, VENABLE (Aug. 8, 2018), https://www.allaboutadvertisinglaw.com/2018/08/fcc-tackles-slamming-and-cramming.html [https://perma.cc/4K34-4XXK].

134. *Id.*

135. *Id.*

136. *See* FCC, CONSUMER GUIDE: UNDERSTANDING YOUR TELEPHONE BILL 1 (2019) [hereinafter UNDERSTANDING YOUR TELEPHONE BILL], https://www.fcc.gov/sites/default/files/understanding_your_telephone_bill.pdf [https://perma.cc/Y79Z-FN4B].

137. *See* FED. TRADE COMM'N, CONSUMER FRAUD IN THE UNITED STATES: AN FTC SURVEY (2004), https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-ftc-survey/040805confraudrpt.pdf [https://perma.cc/DTW2-M6ZN]; *see* FED. TRADE COMM'N, CONSUMER FRAUD IN THE UNITED STATES: THE SECOND FTC SURVEY (2007), https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-second-federal-trade-commission-survey-staff-report-federal-trade/fraud.pdf [https://perma.cc/SSE7-LEQA]; *see* FED. TRADE COMM'N, CONSUMER FRAUD IN THE UNITED STATES, 2011: THE THIRD FTC SURVEY (2011), https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf [https://perma.cc/5WQG-EFNC]; *see* FED. TRADE COMM'N, MASS MARKET CONSUMER FRAUD IN THE UNITED STATES: A 2017 UPDATE (2017) [hereinafter MASS MARKET CONSUMER FRAUD], https://www.ftc.gov/system/files/documents/reports/mass-market-consumer-fraud-united-states-2017-update/p105502massmarketconsumerfraud2017report.pdf [https://perma.cc/S8RE-B6HT].

138. MASS MARKET CONSUMER FRAUD, *supra* note 137, at 25.

139. *Id.*

140. *See* UNDERSTANDING YOUR TELEPHONE BILL, *supra* note 136, at 1.

141. Press Release, Fed. Trade Comm'n, AT&T Promises to Pay $60 Million to Resolve FTC Allegations It Misled Consumers with 'Unlimited Data' Promises (Nov. 5, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/11/att-pay-60-million-resolve-ftc-allegations-it-misled-consumers-unlimited-data-promises [https://perma.cc/ACK2-2PA2].

Earlier in 2014, the FTC forced the corporation to pay its consumers a total of $105 million as part of a multi-agency settlement for unauthorized billing practices.[142] And in 2014, T-Mobile settled an FCC cramming investigation for $90 million.[143]

What these studies and settlements reveal is that consumer fraud in the telecommunications industry is constantly evolving and continuously perpetrated by the same players. This means a given consumer can be victimized multiple times across different providers and is constantly at risk of injury by fraud. Though the FCC and FTC have levied hefty penalties against these corporations, they have done little to eliminate the activity and the reality of the injuries. With little respect for the enforcement sanctions of these government agencies, it is not out of the question that these companies might entertain bankruptcy offloading to shift future liability for these penalties in debtor-friendly bankruptcy forums. What is needed is a solution that not only disincentives this temptation but also galvanizes the FCC and FTC's ability to collect their judgments and curb mass market consumer fraud.

III. ANALYSIS

A. A Two-Pronged Legal Solution

The concerns raised by the potential dischargeability of FCC and FTC consumer fraud penalties are twofold. The first concern is that telecommunications companies will begin to repeatedly deploy strategic offloading as a measure to escape repercussions for their consumer fraud. The second concern is that if the FCC and FTC cannot collect their monetary penalties across all jurisdictions because their claims are dischargeable, rampant consumer fraud in the telecommunications industry will persist. The only way to solve these problems is to give these agencies some bite behind their practical ability to collect fines. The gazelles need to fear the lion's roar again. Therefore, the best legal solution will primarily employ drafting mechanisms and settled bankruptcy law across all jurisdictions to address both the offloading and dischargeability concerns.

The solution's two-pronged approach was designed with the public's interest in mind. Disincentivizing bankruptcy offloads is arguably more important than protecting the FCC and FTC's ability to fully recover their penalties disputed in bankruptcy. The solution is not a mechanism designed to deny telecommunications companies their rights to seek bankruptcy protection and relief. The following solution is largely built on the premise

142. Press Release, Fed. Trade Comm'n, AT&T to Pay $80 Million to FTC for Consumer Refunds in Mobile Cramming Case (Oct. 8, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/10/att-pay-80-million-ftc-consumer-refunds-mobile-cramming-case [https://perma.cc/WZ8W-34CD].

143. Press Release, Fed. Trade Comm'n, T-Mobile to Pay at Least $90 Million, Including Full Consumer Refunds To Settle FTC Mobile Cramming Case (Dec. 19, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/t-mobile-pay-least-90-million-including-full-consumer-refunds [https://perma.cc/U2PR-X7TY].

that an FCC or FTC penalty for consumer fraud should never even remotely incentivize bankruptcy in the first place.

There is an inherent tradeoff between protecting the government's interest and creating inefficiencies within bankruptcy reorganizations. The best way to protect the FCC and FTC's penalties in bankruptcy is by restructuring future penalties into secured claims. However, given the scale of these consumer fraud penalties, such secured claims would impair many creditors who would otherwise have been unimpaired due to the absolute priority rule.[144] In other words, the government is protected at the market's expense. This is a tremendous inefficiency that cannot be bypassed. Accordingly, the following solution separately addresses both the disincentivization of bankruptcy offloads and discharge concerns. By this approach, the solution is a mechanism that better serves the FCC and FTC's practical ability to collect their fines outside of bankruptcy.

Additionally, this Note's proposed solution is limited only to FCC and FTC fines levied via consent decrees and does not examine fines imposed by forfeiture orders. This maintains the solution's focus within the fact pattern of the problem identified by the *In re Fusion Connect* saga, which concerned an unsecured penalty imposed by an FCC consent decree.[145] Despite this narrow focus, penalties levied via forfeiture orders may give rise to the same offload and discharge concerns. For instance, FCC forfeiture orders are also generally unsecured arrangements.[146] As such, the following solution, while tailored to consent decrees, can be applied to other enforcement mechanisms imposing a monetary penalty. Ultimately, it encourages FCC and FTC practitioners to reconsider how they draft and structure two main enforcement principles, namely their assignment provisions and their claim interest status. And while these concepts are narrow, they can be broadly applied to forfeiture orders and other enforcement vehicles at the FCC and FTC's disposal.

B. Addressing Offloading Concerns

Bankruptcy offloading concerns will best be addressed through drafting modifications to the FCC and FTC's current consent decree standards. The FCC and FTC issue consent decrees (also known as consent orders) to resolve

144. *See generally* 11 U.S.C. § 1129.

145. *See In re* Fusion Connect, Inc., 617 B.R. 36, 38-39 (Bankr. S.D.N.Y. 2020), *rev'd*, 634 B.R. 22 (S.D.N.Y. 2021).

146. *See, e.g.*, Mega Moo Radio Co., *Forfeiture Order*, DA 22-199, paras. 7-8 (2022), https://www.fcc.gov/document/forfeiture-order-issued-mega-moo-radio-co [https://perma.cc/78S2-2AJD] (document available for PDF download at linked webpage); *see also* Tele Circuit Network Corp., *Forfeiture Order*, 36 FCC Rcd 7664 (11), paras. 54-55 (2021), https://www.fcc.gov/document/fcc-fines-tele-circuit-4145000-cramming-slamming-violations-0 [https://perma.cc/DB3F-7X96] (document available for PDF download at linked webpage).

investigations against companies accused of committing consumer fraud.[147] These agreements contain the findings of the investigations and stipulate the terms of any penalties levied as remedy.[148] While each consent decree contains detailed provisions tailored to the circumstances of each investigation, they also include boilerplate language that could better serve to protect the government's interests.[149]

The FCC and FTC can improve the way they draft their boilerplate provisions for assignments to deter larger telecommunications providers from pursuing bankruptcy spinoffs. FCC consent decrees usually contain a standard covenant stating "[X Corporation] agrees that the provisions of this Consent Decree shall be binding on its successors, assignees, and transferees."[150] This language was designed to ensure that the government's claim against the company would survive any corporate merger, sale, or acquisition.[151] In fact, this was the same mechanism that shifted Birch Communications' FCC consumer fraud penalty onto Fusion Connect's balance sheet.[152] Alternatively, the FTC addresses assignments by including the penalized corporation's "successors and assigns" within the definition of the consent decree's "Respondents."[153] While these provisions are clearly useful, they should be more nuanced. An ideal covenant would prevent the penalized company from offloading the penalty onto a subsidiary under its own umbrella or a divested spinoff. An ideal covenant would also limit the company's ability to transfer the bill for the penalty to an adjacent third party. Essentially, the consent decree should only permit the penalty's movement to upward assignment along the chain of ownership, not downward or lateral.

Such modification frustrates the business incentive that would drive a penalized company to entertain a strategic offloading as an attractive measure to erase the fine. There is no material benefit to keeping a government penalty on a company's balance sheet. For instance, there are no tax deduction benefits associated with government fines, and without this tax liability offset, the penalty is fully realized.[154] A basic understanding of accounting informs

147. *See, e.g.*, Birch Communications Inc., *Consent Decree*, 31 FCC Rcd 13510 (16), para. 1 (2016) [hereinafter *Birch Communications Consent Decree*], https://www.fcc.gov/document/birch-communications-inc-1 [https://perma.cc/WA9J-9KEM] (document available for PDF download at linked webpage); *see also* Turn Inc., *Decision and Order*, Dkt. No. C-4612, at 1 (2016) [hereinafter *Turn Inc. Decision and Order*], https://www.ftc.gov/system/files/documents/cases/152_3099_c4612_turn_decision_and_order.pdf [https://perma.cc/7NEY-CG84] (forming the basis of the terms underlying the accompanying consent order, *see* Turn Inc., *Consent Order*, File No. 1523099, at 1 (2016), https://www.ftc.gov/system/files/documents/cases/161214_turn_agreement.pdf [https://perma.cc/VSY5-MGHY]).

148. *See, e.g.*, *Birch Communications Consent Decree*, *supra* note 147, *passim*; *see also Turn Inc. Decision and Order*, *supra* note 147, *passim*.

149. *See generally Birch Communications Consent Decree*, *supra* note 147, *passim*; *see also Turn Inc. Decision and Order*, *supra* note 147, *passim*.

150. *E.g., Birch Communications Consent Decree*, *supra* note 147, at para. 28.

151. *In re* Fusion Connect, Inc., 617 B.R. 36, 39 (Bankr. S.D.N.Y. 2020), *rev'd*, 634 B.R. 22 (S.D.N.Y. 2021).

152. *See id.*

153. *See, e.g.*, *Turn Inc. Decision and Order*, *supra* note 147, at 3.

154. *See* 26 U.S.C. § 162(f).

that this reduces owner's equity.[155] Shareholders will have greater cause for irritation, not only because of the reduced value of their investments, but also because of the business' poor standing in Environmental, Social, and Governance (ESG) evaluations.[156] With such pressures across corporate America, incentivizing telecommunications providers to timely pay their penalties in full will discourage the accumulation of future penalties over time.

C. Addressing Discharge Concerns

Bankruptcy discharge concerns will also best be addressed through drafting modifications to the consent decrees. However, this requires a more complex modification than what was sufficient to address strategic offloading concerns. As discussed earlier, bankruptcy rights cannot be waived away like the assignment of a debt, otherwise, as the Ninth Circuit rationalized, "astute creditors would routinely require their debtors to waive."[157] Likewise, the consent decree cannot simply stipulate that the penalties are nondischargeable.[158] Additionally, continuing to argue nondischargeability on Section 523(a)(2)(A) grounds would require the FCC and FTC to account for the disagreement on this statute's application. This would impractically necessitate that the agencies identify how they are materially injured by a given consumer fraud, and that would be difficult if not specifically detailed in the consent decree. Any injury would be difficult to quantify and may not hold up across circuits. And because Congress narrowly limited which exceptions to discharge apply to corporations under Section 1141(d)(6)(a) of the Code, many Section 523 exceptions are defanged.[159] For example, arguing that a consumer fraud penalty is nondischargeable under Section 523(a)(7) because it is "a fine, penalty, or forfeiture payable to and for the benefit of a governmental unit . . ."[160] will be ineffective because this exception only applies to individual debtors.[161] Therefore, the more efficient legal solution would be for the FCC and FTC to structure their consent decrees in such a way that renders the agencies as secured creditors to the penalized corporation.

Consent decrees' penalty provisions already behave like debt agreements. They set the civil penalties' total monetary amounts, the term installments over which the penalties will be paid, and the modes of

155. Adam Hayes, *Expanded Accounting Equation: Definition, Formula, How It Works*, INVESTOPEDIA, https://www.investopedia.com/terms/e/expanded-accounting-equation.asp [https://perma.cc/LE2S-FKJL] (last updated July 13, 2022).

156. *See generally What Is Environmental, Social, and Governance (ESG) Investing?*, INVESTOPEDIA, https://www.investopedia.com/terms/e/environmental-social-and-governance-esg-criteria.asp [https://perma.cc/L6EK-FDRG] (last updated Sept. 27, 2022).

157. *In re* Thorpe Insulation Co., 671 F.3d 1011, 1026 (9th Cir. 2012) (quoting Bank of China v. Huang (*In re Huang*), 275 F.3d 1173, 1177 (9th Cir. 2002)).

158. *See id.*

159. 11 U.S.C. § 1141(d)(6)(a).

160. 11 U.S.C. § 523(a)(7).

161. 11 U.S.C. § 1141(d)(6)(a).

payment.[162] In fact, consent decrees sometimes specify that the penalties shall be treated as "claims" and "debts" as those terms are defined under Section 3701(b)(1) of the Debt Collection Improvement Act of 1996.[163] Pursuant to that statute, "the term 'claim' or 'debt' means any amount of funds or property that has been determined by an appropriate official of the Federal Government to be owed to the United States by a person, organization, or entity other than another Federal agency."[164] The statute specifically encompasses "any fines or penalties assessed by an agency."[165]

In choosing a property to attach to the penalty, many reasons point to FCC licenses as the most appropriate option. The first reason is that FCC licenses are highly valuable assets that a telecommunications provider would prefer not to surrender. Telecommunications providers have spent billions of dollars on their spectrum empires, indicating that such a loss of this property would directly injure their business operations.[166] This would highly disincentivize a company's default on its penalty payments. In addition, FCC licenses are intangible assets that do not carry the burdens of depreciation, administrability costs, and maintenance that come inherent to the surrender and auction of tangible and real property. The FCC already enjoys a Nobel Prize-winning, highly efficient, and lucrative auctioning infrastructure for its licenses.[167] Any forfeited licenses could easily be auctioned back on the open market to recover the unrealized proceeds (and potentially more) from a default on the payment terms of the consent decree.

Despite the many benefits of securing consumer fraud penalties with FCC licenses, there are a few unique qualities about these licenses that require additional attention. Practitioners may initially raise concerns that the FCC has previously stated that the Federal Communications Act of 1934 generally prohibits the creation of security interests in FCC licenses.[168] However, the applicable statute provides as follows: "No . . . station license, or any rights thereunder, shall be transferred, assigned, or disposed of in any manner, . . . or by transfer of control of any corporation holding such permit or license, to any person except upon application to the Commission and upon finding by the Commission that the public interest, convenience, and necessity will be

---

162. *E.g., Birch Communications Consent Decree*, *supra* note 147, at para. 22.

163. *E.g.,* Assurance Wireless USA, LP, f/k/a Virgin Mobile USA, LP, Sprint Corp., and T-Mobile US, Inc., *Consent Decree*, 35 FCC Rcd 12679 (16), para. 24 (2020), https://www.fcc.gov/document/fcc-reaches-200-million-settlement-sprint-lifeline-investigation [https://perma.cc/9PLE-GELN].

164. 31 U.S.C. § 3701(b)(1).

165. 31 U.S.C. § 3701(b)(1)(F).

166. *See, e.g.*, Emma Roth, *AT&T, Dish, and T-Mobile Spend Billions on More 5G Spectrum*, VERGE (Jan. 15, 2022, 3:29 PM), https://www.theverge.com/2022/1/15/22885320/att-dish-tmobile-5g-spectrum-billions-auction [https://perma.cc/DX8C-QBUA].

167. *See* Taylor Kubota, *The Economic Science Behind Wilson's and Milgrom's Nobel Prize*, STAN. NEWS (Oct. 12, 2020), https://news.stanford.edu/2020/10/12/economic-science-behind-wilsons-milgroms-nobel-prize/ [https://perma.cc/V6GM-R7K4].

168. *See* Kirk Merkley, *Memorandum Opinion and Order*, 94 F.C.C. 2d 829, 831, 839 (1983) [hereinafter *Kirk Merkley Memorandum Opinion and Order*] (acknowledging the FCC's general recognition of security interests in FCC licenses as "contrary to established law and policy" under the 47 U.S.C. § 310(d)).

served thereby."[169] This statute effectively conditions the attachment of a security interest in an FCC license on the FCC's approval.[170] This condition was originally intended to protect licensee independence and prevent licenses from falling under the ownership of ineligible license holders, such as financial institutions and foreign entities.[171] Accordingly, if the FCC or FTC were to secure their civil penalties with FCC licenses, the only legal barrier to these agreements would be the FCC's own approval. Surely the FCC would recognize the public benefit this proposed resolution seeks to bestow. Therefore, this question should not be cause for much further concern.

Perhaps the most difficult legal question surrounding the use of FCC licenses to secure civil penalties is how to attach a license that is comparable to the value of the penalty. Any telecommunications provider holds many FCC licenses ranging in bands and value.[172] These licenses are acquired over many years and purchased at auction over a wide range of winning bids.[173] Many extrinsic factors went into these purchase prices, including market competition and consumer demand.[174] While a security interest's collateral need not match the value of the debt, the Code provides that a creditor's claim may bifurcate into a secured claim up to the value of the security interest and a general unsecured claim for the remainder.[175] But creditors can often request a pledge of collateral that exceeds the value of the debt if there are high risks involved in the transaction.[176] Similarly, the FCC and FTC may justify a pledge of collateral that exceeds the value of their penalties because the penalties were procured by a violation of federal law. As a standard policy, the agencies may consider requiring a penalized company to pledge an FCC license or package of FCC licenses that was purchased at a price no less than the amount of the penalty and no more than a certain percentage premium to that amount. The buffer would have to fall into a reasonable range so as to remain within common market practices and any existing legal limits. The FCC and FTC may also consider specifying that the penalized company pledge as collateral the FCC license or package of FCC licenses most recently purchased from the execution of the consent decree that satisfies this value condition. While there may be a more economical or equitable way to structure these terms, these proposals serve as reasonable suggestions and springboards for thought.

Assuming the FCC licenses are successfully attached pursuant to the terms of the consent decree, the civil penalty is adequately shielded from

169. 47 U.S.C. § 310(d).

170. *See id.*

171. *See Kirk Merkley Memorandum Opinion and Order*, *supra* note 168, at 830-31.

172. *See generally* 19 FCC MOBILE WIRELESS SERVICES COMPETITION ANN. REP. 39-43 (2016),
https://www.fcc.gov/document/19th-mobile-wireless-competition-report [https://perma.cc/HFW5-9Z59] (report available for PDF download at linked webpage).

173. *See generally id.*

174. *See generally id.*

175. 11 U.S.C. § 506(a)(1).

176. *See* Will Kenton, *Over-Collateralization (OC)*, INVESTOPEDIA, https://www.investopedia.com/terms/o/overcollateralization.asp [https://perma.cc/7RZ7-TTEF] (last updated May 18, 2020).

discharge in bankruptcy. The Code provides that secured creditors in a Chapter 11 reorganization plan cannot have their claims discharged by the debtor corporation without the debtor's surrender of the attached collateral.[177] At worst, the terms of penalty may be renegotiated to better accommodate the distressed company's plan of reorganization.[178] In this case, that might mean a lengthened term or a reduced penalty. If the company's reorganization fails and results in liquidation, the penalty's secured status at least renders it superior to nearly all other debts, essentially guaranteeing the penalty's full payment from the proceeds of the short sale.[179] Either way, attaching a security interest to the penalty offers the FCC and FTC greater protection of their practical ability to collect their fines tied up in bankruptcy. And this mechanism holds across all bankruptcy jurisdictions.

IV. CONCLUSION

This Note is intended to show how the FCC and FTC could apply bankruptcy law mechanisms to not only protect their consumer fraud penalties disputed in Chapter 11 reorganization but also strengthen their overall ability to collect fines and enforce authority. This is an important time for practitioners to consider the potential problems identified by this Note. Bankruptcy may be a niche area of law, but its effects touch all aspects of business, regulation, and enforcement. This Note's solution attempts to balance those considerations and hopes that in time the FCC and FTC will heed this warning for some added security.

177. *See* 11 U.S.C. § 1129(b)(2)(A)(i).
178. *See* 11 U.S.C. § 1123.
179. *See id.*

You're Only Mostly Dead: Protecting Your Digital Ghost from Unauthorized Resurrection

Rebecca J. Roberts*

TABLE OF CONTENTS

* J.D., May 2023, The George Washington University Law School. Senior Managing Editor, Federal Communications Law Journal, Volume 75. B.A., 2018, Pyschology and Performance Studies, Texas A&M Univeristy. I want to thank my parents for their constant support. I would also like to thank the entire Cardozo Inn for being such a fun and encouraging community.

I. INTRODUCTION

"You married the most, most, most, most, most genius man in the whole world, Kanye West," said the Robert Kardashian hologram custom ordered by Kanye West.[1] In 2020, a production company holographically resurrected the deceased Robert Kardashian using artificial intelligence.[2] This lifelike hologram was programmed to say and do things that the real Robert Kardashian never said or did while still alive—including high praise of his daughter's then-husband, Kanye West, who purchased the hologram for his then-wife's birthday.[3]

Artificial intelligence ("AI") is a constantly evolving field that plays a substantial role in the manufacture of synthetic media.[4] As AI technology improves and expands, advanced synthetic media known as "digital clones" and "deepfakes" have started to emerge.[5] This synthetic media is created using photos, videos, and audio of a person, which can then be programmed to do and say anything the programmer wishes.[6] They manifest as chatbots, audio clips, videos, holograms, and other varieties of audio-visual media.[7] Production of these digital clones varies from glitchy videos that individuals can create for free on an easily accessible app, to highly expensive holograms like that of Robert Kardashian.[8] These digital clones in some cases are so incredibly lifelike that they seem real—tricking viewers into believing they are seeing something truly authentic—when they are actually just AI-created synthetic media.[9]

---

1. Alyx Gorman, *Kim Kardashian's Father Resurrected as Hologram in Birthday Present from Kanye West*, GUARDIAN (Oct. 29, 2020, 11:18 PM), https://www.theguardian.com/lifeandstyle/2020/oct/30/robert-kardashian-resurrected-as-a-hologram-for-kim-kardashian-wests-birthday [https://perma.cc/G5ZB-URQM].
2. *See id.*; *see also The Synthetic Reality Co.*, KALEIDA, https://www.wearekaleida.com/synthetic-reality [https://perma.cc/56YD-AA7L] (last visited Apr. 12, 2022).
3. *See* Gorman, *supra* note 1.
4. *See* Craig S. Smith, *A.I. Here, There, Everywhere*, N.Y. TIMES (Mar. 9, 2021), https://www.nytimes.com/2021/02/23/technology/ai-innovation-privacy-seniors-education.html [https://perma.cc/3SVT-KSMA].
5. *See* U.S. DEP'T HOMELAND SEC., INCREASING THREAT OF DEEPFAKE IDENTITIES 3 (2021), https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf [https://perma.cc/DK6T-62HZ]; *see also* Jon Truby & Rafael Brown, *Human Digital Thought Clones: The* Holy Grail *of Artificial Intelligence for Big Data*, 30 INFO. & COMM. TECH. L. 140, 140-41 (2021).
6. *See* INCREASING THREAT OF DEEPFAKE IDENTITIES, *supra* note 5, at 3, 5, 27.
7. *See id.* at 5.
8. *See id.* at 9.
9. *Id.* at 3.

Due to the high volume of digital media created during one's lifetime,[10] digital clones can be produced post-mortem.[11] Digital cloning technology allows for the creation of holograms, audio messages, videos, etc. of a dead person doing or saying something they never said or did while still alive.[12] This type of technology can be useful in the world of entertainment, for example, as it provides opportunities to reanimate actors who passed before their film finished shooting.[13] However, synthetic media also presents several ethical concerns. After someone dies, a video could emerge of their digital clone saying something deplorable going against everything they believed in while still alive. If such synthetic media is truly indistinguishable from authentic media, a person's voice, life, and legacy is put at risk, and there is nothing that can be done because they are no longer alive to refute it.

Through the years, courts have consistently held that people have no personal rights after death[14] and that reputation and dignity are not maintained after death.[15] While some states have post-mortem privacy laws protecting against the commercial use of a deceased celebrity's likeness,[16] this would not protect private figures from unauthorized digital clone creation and use, nor would it protect against noncommercial unauthorized creation and use. Because current legislation and common law are inconsistent and almost entirely hypothetical, and because they do not go further than protecting certain situations in which post-mortem digital clones may be created and used, this issue requires a novel approach.[17] Through probate law and estate planning, the deceased have an atypical right to control how their property is distributed and used.[18] This Note will argue that there should be an explicit safeguard within probate law protecting against the unauthorized creation and use of a deceased person's digital clone.

The Background section will explain how artificial intelligence has enabled the production of synthetic media depicting real people. There are some ethical and legal concerns that arise from both existing and impending post-mortem synthetic technology. This section will also assess untested

---

10. Bernard Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, FORBES (May 21, 2018, 12:42 AM), https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/ [https://perma.cc/3XU4-TLH5].

11. *See* Shannon Flynn Smith, Comment, *If It Looks like Tupac, Walks like Tupac, and Raps like Tupac, It's Probably Tupac: Virtual Cloning and Postmortem Right-of-Publicity Implications*, 2013 MICH. ST. L. REV. 1719, 1725 (2013).

12. *See id.*

13. *See* Joel Anderson, Comment, *What's Wrong with This Picture? Dead or Alive: Protecting Actors in the Age of Virtual Reanimation*, 25 LOY. L.A. ENT. L. REV. 155, 157 (2005).

14. *See* Natalie M. Banta, *Death and Privacy in the Digital Age*, 94 N.C. L. REV. 927, 935-36 (2016).

15. *See id.* at 938-39.

16. *See* RIGHT OF PUBLICITY COMMITTEE, INT'L TRADEMARK ASSOC., RIGHT OF PUBLICITY STATE OF THE LAW SURVEY (2019) [hereinafter RIGHT OF PUBLICITY SURVEY], https://www.inta.org/wp-content/uploads/public-files/advocacy/committee-reports/INTA_2019_rop_survey.pdf [https://perma.cc/N7WM-9XLM%22].

17. *See infra* Section II.C.

18. *See* Banta, *supra* note 14, at 936.

solutions that could potentially protect against digital cloning and synthetic media in different fields of the law. Post-mortem privacy rights are only extended to celebrities under existing privacy law.[19] Although there may be copyrightable and trademarkable elements within the field of artificial intelligence, there are no proven or guaranteed protections against unauthorized digital cloning.[20] Criminal law is beginning to prohibit certain aspects of deepfake technology, but such laws do not prohibit unauthorized use unless there is a severe and tangible harm.[21]

The Analysis will compare the benefits and potential harms that could come with the growing prevalence of post-mortem digital cloning technology, as well as discuss the successes and failures of attempted claims against it. While there are some possible solutions for victims of unauthorized digital cloning, legislators have not been able to keep up with the growing prevalence of this technology, and there are several gaps in protection. Further, post-mortem rights are practically non-existent in every field of law except probate law. Current standards within probate law regarding digital assets and digital estate planning do not currently include specific protections against post-mortem digital cloning, but they could be extended to do so. The final section of the Analysis will present estate planning and probate law as an innovative way to preempt unauthorized post-mortem digital clones. Requiring explicit, affirmative permission from a decedent is the best way to successfully protect a deceased person's estate from the unauthorized creation and use of post-mortem digital clones.

II. BACKGROUND

A. Artificial Intelligence Capabilities Have Advanced to Producing Lifelike Synthetic Media, like Digital Cloning

The term "artificial intelligence" was first used in the 1950s in an effort to describe the process of teaching computers to understand and recreate human reasoning.[22] After many years of development, AI seems to have a hand in so much of society's day-to-day life—from vehicles, to phones, to Google Home hubs.[23] While there are certainly a wide variety of benefits attributable to the prevalence of AI, its fast growing adaptation also presents a series of concerns for the future.[24] AI uses algorithmic technology to learn our routines and interests, which allows for personalized advertising and lifestyle convenience.[25] However, with such access to personal data, there are

19. *See infra* Section II.C.1.
20. *See infra* Section II.C.2.
21. *See infra* Section II.C.3.
22. *See* N.Y.C. MAYOR'S OFF. OF THE CHIEF TECH. OFFICER, AI STRATEGY: THE NEW YORK CITY ARTIFICIAL INTELLIGENCE STRATEGY 14 (2021), https://www1.nyc.gov/assets/cto/downloads/ai-strategy/nyc_ai_strategy.pdf [https://perma.cc/2HNJ-FEBY].
23. Smith, *supra* note 4.
24. *Id.*
25. *See id.*

concerns about privacy and how daily interactions with AI might be used.[26] Further, as AI capabilities increase, there is concern that in the wrong hands the technology may be used in more malicious ways.[27]

Synthetic media is content created through the use of AI—equipping algorithmic deep learning technology to create incredibly lifelike artificial media.[28] This technology can modify or manipulate currently existing photos and videos of a person by superimposing them onto other existing media—creating what is colloquially known as a "deepfake" or "digital clone."[29] By exchanging aspects of existing media with other existing media, a person can create hyper-realistic media depicting something that does not actually exist.[30] Popular deepfake media shows politicians, celebrities, and even private citizens doing or saying something they have never done or said.[31] Similarly, there also exists AI technology that takes existing audio clips of a person and programs software to recreate that person's voice saying anything they want.[32] Throughout this Note, the terms "synthetic media," "deepfakes," and "digital clones" will be interchangeably used to refer to any kind of AI-generated media mimicking a real person that has been created using the person's preexisting media outputs.

People's lives and reputations are at stake now that there is such potentially deceptive technology out there that could leave the public with a false impression of someone's behavior.[33] Political figures could equip deepfake technology to present opposing parties doing or saying something that is not congruent with their true political or moral standpoints.[34] Courts have also recently become aware that a more robust system of authentication may be needed for certain pieces of evidence in order to admit them as

26. *See id.*

27. *See* Cade Metz, *Efforts to Acknowledge the Risks of New A.I. Technology*, N.Y. TIMES (Oct. 22, 2018), https://www.nytimes.com/2018/10/22/business/efforts-to-acknowledge-the-risks-of-new-ai-technology.html [https://perma.cc/6UAW-QCH6]; *see also* INCREASING THREAT OF DEEPFAKE IDENTITIES, *supra* note 5, at 10.

28. Ian Sample, *What Are Deepfakes – And How Can You Spot Them?*, GUARDIAN (Jan. 13, 2020, 5:00 AM), https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them [https://perma.cc/U8L5-B8JH].

29. *Id.*

30. *See id.*

31. *Id.*

32. Jennifer Kite-Powell, *The Rise of Voice Cloning and DeepFakes in the Disinformation Wars*, FORBES (Sept. 21, 2021, 3:14 PM), https://www.forbes.com/sites/jenniferhicks/2021/09/21/the-rise-of-voice-cloning-and-deep-fakes-in-the-disinformation-wars/ [https://perma.cc/JB5U-KG7Z].

33. *See id.*

34. Rob Toews, *Deepfakes Are Going to Wreak Havoc on Society. We Are Not Prepared.*, FORBES (May 25, 2020, 11:54 PM), https://www.forbes.com/sites/robtoews/2020/05/25/deepfakes-are-going-to-wreak-havoc-on-society-we-are-not-prepared/ [https://perma.cc/96NP-EXHG].

reliable.[35] Audio files, photos, and videos can no longer be taken at face value.[36]

State legislators have recently begun analyzing these arising issues and enacting new legislation to regulate the effects of deepfakes and artificial intelligence, primarily related to election interference and pornography.[37] Congress also recently voted to require that the Department of Homeland Security issue annual reports for the next five years on potential harms that may arise from the increasing use of deepfake technology.[38] In 2021, the Department released an infographic detailing possible threats and scenarios that could arise from such synthetic media.[39] Even though the concept of AI has been around since the 1950's, and has a prevalent role in everyday life, there is still very little legislative or judicial guidance on how to protect the public from the number of harms it could potentially bring about.

B. Digital Cloning Is Not Limited to the Living

Films, television shows, and books have predicted the idea of "digital cloning" for decades.[40] The popular television show *Black Mirror* has even addressed the possible dangers that could emerge from post-mortem digital clones.[41] *Black Mirror* is popular for exhibiting not-yet existing technology and then asking its audience a series of "what ifs" in an attempt to warn against the dangers that certain advanced technology could bring about.[42] Some episodes even have technology that does not seem too far off from what already exists today.[43]

In the episode "Be Right Back," the main character orders an AI bot to imitate her recently deceased boyfriend.[44] The bot starts as a voice on the other end of a phone call—integrating preexisting audio recordings of his voice

---

35. *See* Matt Reynolds, *Courts and Lawyers Struggle with Growing Prevalence of Deepfakes*, A.B.A. J. (June 9, 2020, 9:29 AM), https://www.abajournal.com/web/article/courts-and-lawyers-struggle-with-growing-prevalence-of-deepfakes [https://perma.cc/T3N9-K4RA].

36. *See id.*

37. Scott Briscoe, *U.S. Laws Address Deepfakes*, ASIS INT'L (Jan. 12, 2021), https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2021/january/U-S-Laws-Address-Deepfakes/ [https://perma.cc/MEQ6-HA8R].

38. *Id.*; National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 5709, 133 Stat. 2168, 2168-70 (2019).

39. *See* INCREASING THREAT OF DEEPFAKE IDENTITIES, *supra* note 5, at 18.

40. *See, e.g.*, Joseph J. Beard, *Clones, Bones, and Twilight Zones: Protecting the Digital Persona of the Quick the Dead, and the Imaginary*, 16 BERKELEY TECH. L.J. 1165, 1250-54 (2001).

41. Oscar Rickett, *How Far off Are We from the Digital Clones of 'Black Mirror'?*, VICE (Jan. 15, 2018, 7:36 AM), https://www.vice.com/en/article/zmq8vy/how-far-off-are-we-from-the-digital-clones-of-black-mirror [https://perma.cc/6XHY-DLPY].

42. *See* Oihab Allal-Chérif, *'Black Mirror': The Dark Side of Technology*, CONVERSATION (June 4, 2019, 5:47 PM), https://theconversation.com/black-mirror-the-dark-side-of-technology-118298 [https://perma.cc/JWW7-ZWCG].

43. Justin Render, *10 Technologies from Black Mirror That Have Already Been Invented*, SCREENRANT (Oct. 24, 2019), https://screenrant.com/black-mirror-technologies-already-invented/ [https://perma.cc/79R9-5FTH].

44. *Black Mirror: Be Right Back* (Channel 4 television broadcast Feb. 11, 2013).

with algorithmic deep learning technology from his social media posts—so that his girlfriend can feel as though she is really speaking with him.[45] After upgrading the service, the girlfriend receives a full-size, realistic, tangible clone of him—manufactured from even more preexisting audio-visual media.[46] The AI bot was supposedly meant to bring solace to those grieving the loss of a loved one, but the episode reminds its audience that humanity requires more than a performance of the media captured or posted online during one's lifetime.[47]

For years, *Black Mirror*-levels of technology somehow felt futuristic, inevitable, and impossible at the same time. However, as artificial intelligence develops, the likelihood of indistinguishably lifelike digital clones also increases.[48] Today, a phone call with a deceased loved one is not entirely out of the question.[49] A company called HereAfter is giving people the opportunity to record stories about their life before they die, creating a kind of "life story avatar" for their loved ones to listen to after they pass away.[50] When HereAfter co-creator James Vlahos was in the process of losing his father to cancer, he created the "Dadbot" using stories from his father and predictive algorithms to allow for text conversation with a digital version of his father.[51] He was even able to show his father the Dadbot before he died, who expressed enthusiasm at the idea of members of his family being able to learn things about him in the years after his death.[52] These life story avatars use predictive algorithms to fill in the holes, but the substantive aspects of the conversation are facts recorded by the person before they die with the knowledge of how it will later be used.[53]

Similar companies like Eternime have proposed services allowing users to let a software program inundate their life—their social media, online communications, etc.—in order to learn as much as possible about them until they die, with the hope of creating digital immortality for those they leave behind.[54] There are also facilities like University of Southern California's Institute for Creative Technologies, which built an interactive hologram exhibit using recorded stories from Holocaust survivors to teach future

45. *Id.*
46. *Id.*
47. *See id.*; *see also* Rickett, *supra* note 41.
48. *See* Rickett, *supra* note 41.
49. HEREAFTER, https://www.hereafter.ai [https://perma.cc/X5JD-QQZK] (last visited Apr. 12, 2022).
50. *See* Leslie Katz, *Talk with Your Dead Loved Ones – Through a Chatbox*, CNET (Dec. 17, 2021, 10:46 AM), https://www.cnet.com/news/hereafter-ai-lets-you-talk-with-your-dead-loved-ones-through-a-chatbot/ [https://perma.cc/3U95-3R9E].
51. *See* James Vlahos, *A Son's Race to Give His Dying Father Immortality*, WIRED (Jul. 18, 2017, 6:00 AM), https://www.wired.com/story/a-sons-race-to-give-his-dying-father-artificial-immortality/ [https://perma.cc/Z5CE-HNFK].
52. *See id.*
53. *Id.*
54. *See* Marius Ursache, *The Journey to Digital Immortality*, MEDIUM (Oct. 23, 2015), https://medium.com/@mariusursache/the-journey-to-digital-immortality-33fcbd79949 [https://perma.cc/93VM-QBST].

generations.[55] All of the aforementioned projects have a very important component in common—permission to use the preexisting media needed to create these varying digital clones was affirmatively given by the deceased for that express purpose while they were still alive.

Alternatively, there are people like Eugenia Kuyda, who spent years building a neural network to mimic her friend who passed away—using old text messages from him to create a chatbot similar to the Dadbot.[56] Her project was met with mixed responses, and she even received a message from a friend that she had not learned the lesson that the *Black Mirror* "Be Right Back" episode intended to teach.[57] There was also no indication that her friend, nor his relatives, had ever given Kuyuda permission for the text messages to be used in such a way.[58] In 2020, Microsoft received a patent for software that aims to use a person's social media presence to create conversational chatbots that mimic their personality.[59] It is unclear what levels of permission Microsoft would seek from users or social media sites prior to creating these hypothetical chatbots.[60]

In the film world, the practice of digitally reanimating actors and celebrities for movies is also on the rise.[61] In 2016, a *Star Wars* prequel brought back a character from the original 1977 films.[62] The actor, Peter Cushing, who played the character in the original films had since passed away.[63] Instead of recasting the character, Lucasfilm studios opted to use visual effects to digitally reanimate the deceased actor.[64] The studio obtained permission from Cushing's estate.[65] These kinds of "digital actors" are present in a number of films where an actor may have passed away during filming.[66] Studios like Lucasfilm even admit to obtaining digital scans of all their actors for post-production editing, which could ultimately be used for digital

55. *See* Leslie Katz, *Holograms of Holocaust Survivors Let Crucial Stories Live On*, CNET (Feb. 11, 2013, 10:40 AM), https://www.cnet.com/news/holograms-of-holocaust-survivors-let-crucial-stories-live-on/ [https://perma.cc/GA9A-7QZW].

56. *See* Casey Newton, *Speak, Memory – When Her Best Friend Died, She Rebuilt Him Using Artificial Intelligence*, VERGE, https://www.theverge.com/a/luka-artificial-intelligence-memorial-roman-mazurenko-bot [https://perma.cc/4XFX-UJWB] (last visited Apr. 12, 2022); *see also* Vlahos, *supra* note 51.

57. *See* Newton, *supra* note 56.

58. *See id.*

59. *See* Dalvin Brown, *AI Chat Bots Can Bring You Back from the Dead, Sort Of*, WASH. POST (Feb. 4, 2021, 11:53 AM), https://www.washingtonpost.com/technology/2021/02/04/chat-bots-reincarnation-dead/ [https://perma.cc/VJP4-FP54]; U.S. Patent No. 10,853,717 B2 (filed Apr. 11, 2017) (issued Dec. 1, 2020).

60. *See* Brown, *supra* note 59.

61. *See Rogue One: What Peter Cushing's Digital Resurrection Means for the Industry*, TODAY (Dec. 17, 2016) [hereinafter *Peter Cushing's Digital Resurrection*], https://www.todayonline.com/entertainment/rogue-one-what-peter-cushings-digital-resurrection-means-industry [https://perma.cc/A8XE-DQFS].

62. *Id.*

63. *Id.*

64. *Id.*

65. *Id.*

66. *See, e.g.*, Smith, *supra* note 11, at 1725-28.

reanimation if needed.[67] In 2019, the family of James Dean granted permission for his likeness to be wholly digitally reanimated for a brand new film about the Vietnam War.[68]

In 2021, a documentarian recreated the late Anthony Bourdain's voice for his film about Bourdain by manipulating preexisting video and audio files of him.[69] Members of the public were unnerved upon learning that the audio was synthetic and that it was generated without permission from Bourdain's ex-wife.[70] The synthetic audio was a reading of an email sent by Bourdain while he was still alive, so while the audio itself was digitally manufactured, the words were still Bourdain's.[71]

The company that created the Robert Kardashian hologram, Kaleida, claims to use synthetic reality technologies to resurrect "pop singers, heads of state[,] and historical figures."[72] Holographic reanimations of deceased musicians, like the Tupac hologram Superbowl XLVI performance, are widely known examples of post-mortem digital cloning.[73] Despite Tupac's express disapproval of digital cloning, he was reanimated performing for millions of people a song he had never sung while alive.[74] Similarly, Prince expressed disgust and horror at the idea of a hologram being created of him.[75] But after Prince's passing, there were reports that Justin Timberlake would be performing with a Prince hologram at the Superbowl LII halftime show.[76] This did not end up occurring, possibly because of the backlash surrounding the reports, as Prince's explicit opposition to holographic performances was widely known.[77] Conversely, an upcoming Amy Winehouse posthumous hologram tour was announced, with support from the Winehouse estate.[78]

Clearly, artificial intelligence in the form of posthumous digital cloning is already part of the collective, national zeitgeist. Whether it manifests itself

---

67. Ryan Britt, *Lucasfilm Has Digital Clones of Your Favorite 'Star Wars' Characters*, INVERSE (Apr. 6, 2018), https://www.inverse.com/article/43342-star-wars-digital-leia-flying-last-jedi-vfx-episode-ix [https://perma.cc/T6XC-TQCM].

68. Brian Welk, *James Dean to Be Digitally Reanimated in CGI for Vietnam War Movie 'Finding Jack'*, WRAP (Nov. 6, 2019, 7:43 AM), https://www.thewrap.com/james-dean-to-be-digitally-reanimated-in-cgi-for-vietnam-war-movie-finding-jack/ [https://perma.cc/B9ZN-XNKJ].

69. *See* Helen Rosner, *The Ethics of a Deepfake Anthony Bourdain Voice*, NEW YORKER (July 17, 2021), https://www.newyorker.com/culture/annals-of-gastronomy/the-ethics-of-a-deepfake-anthony-bourdain-voice [https://perma.cc/N494-9QTZ].

70. *See id.*

71. *See id.*

72. *The Synthetic Reality Co.*, *supra* note 2.

73. *See, e.g.*, Chris Young, *How It Works: 13 Famous People Brought Back to Life as Holograms*, INTERESTING ENG'G (Mar. 12, 2020), https://interestingengineering.com/how-it-works-13-famous-people-brought-back-to-life-as-holograms [https://perma.cc/X6KE-ZUL8].

74. *See* Smith, *supra* note 11, at 1720-21.

75. *See* Dee Lockett, *We May Never Know the Truth About Justin Timberlake's Prince Hologram*, VULTURE (Feb. 6, 2018), https://www.vulture.com/2018/02/whats-the-truth-about-justin-timberlakes-prince-hologram.html [https://perma.cc/5RZB-MUNQ].

76. *See id.*

77. *See id.*

78. Seamus Duff, *Amy Winehouse 'Hologram Set to Go On Tour' in 'Celebration' of the Star*, MIRROR (Aug. 21, 2021, 4:05 PM), https://www.mirror.co.uk/3am/celebrity-news/amy-winehouse-hologram-set-go-24807401 [https://perma.cc/D436-6D86].

as a performative hologram, audio clip, CGI actor, or interactive chatbot, dying can place a person's digital footprint at risk of manipulation or resurrection. Without requiring specific and affirmative action from the decedent to protect against unauthorized use, there is no way to predict how their voice and likeness might be used after death.

C. *Current Law Does Not Provide Adequate Support Against the Unauthorized Creation of Digital Clones*

1. Privacy Law

Privacy law can be split into four sub-categories: intrusion upon seclusion, appropriation of name or likeness, public disclosure of private facts, and false light publicity.[79] Should one find themself a victim of deepfake technology, bringing a claim of false light, libel, and/or defamation is likely the best course of legal action—especially if the deepfake shows one in a misleading or harmful light.[80] However, common law dictates that personal injuries die with a person, while injuries to one's property or estate survive them.[81] This is further detailed in the *Second Restatement of Torts*: "There is no action for the invasion of the privacy of one already deceased, in the absence of statute."[82] Many authors have rightfully questioned why the dead do not have rights to privacy, dignity, or autonomy.[83] This concept goes back to the 1860s, and courts have since held that because privacy rights protect against personally and uniquely felt harms, the dead have no such rights because they are unable to vocalize or experience such harms.[84] Therefore, privacy rights die when you die.[85]

As of 2021, both Idaho and Nevada have statutes criminalizing libel or defamation of the dead,[86] and Oklahoma has a statute stating that a threat to publish libel concerning the dead relative of a person "shall be liable civilly and criminally to have the same intent as though the publication had been made…"[87] In prior years, most states had similar criminal and civil statutes protecting against "blackening the memory of the dead."[88] But the steady invalidation and repeal of such statutes over the recent years suggests that

79. RESTATEMENT (SECOND) OF TORTS §§ 652A-652I (AM. L. INST. 1965).

80. *See* Alexander Ryan & Andrew Hii, *Disinformation Takes on a New Face: 'Deepfakes' and the Current Legal Landscape*, GILBERT & TOBIN (Oct. 4, 2019), https://www.gtlaw.com.au/knowledge/disinformation-takes-new-face-deepfakes-current-legal-landscape [https://perma.cc/SG8K-JPRY].

81. *See* Shafer v. Grimes, 23 Iowa 550, 553 (1867).

82. RESTATEMENT (SECOND) OF TORTS § 652I cmt. b (AM. L. INST. 1965).

83. *See, e.g.*, Kirsten Rabe Smolensky, *Rights of the Dead*, 37 HOFSTRA L. REV. 763, 763-65 (2009).

84. *See* Banta, *supra* note 14, at 935-36.

85. *Id.* at 932-33.

86. IDAHO CODE § 18-4801 (2021); NEV. REV. STAT. § 200.510 (2021).

87. OKLA. STAT. tit. 21, § 778 (2022).

88. *See* William H. Binder, Note, *Publicity Rights and Defamation of the Deceased: Resurrection or R.I.P?*, 12 DEPAUL-LCA J. ART & ENT. L. 297, 322-25 (2002).

courts are uneasy to limit free speech in such a manner.[89] As such, courts continue to follow a civil common law standard that there is no liability for publishing defamatory remarks about a deceased person.[90]

Under the category of appropriation is the right of publicity.[91] There are currently 36 states that have some variation of statute or common law protecting against the unauthorized use of a person's likeness for commercial gain.[92] These laws vary by state and are intended to protect a person's "personality rights" or "rights of publicity"—phrases coined by a 1953 case, *Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc.*[93] These rights suggest that if a person's likeness has value, using it for commercial purposes without their permission is infringing upon their right to earn money (i.e., their property rights).[94] Most of these laws require that the person whose likeness is being misappropriated holds a level of recognizability, so celebrities are typically the only individuals who are successful in these kinds of suits.[95] Further, these laws typically protect against the unauthorized *commercial* use of a person's likeness, leading celebrities to also find greater success in these types of suits, as non-celebrity individuals are less likely to find their likeness abused for commercial use.[96]

While 36 states protect the right of publicity, there are only 25 states that have extended such rights to include protection after death.[97] Each state that *does* recognize post-mortem publicity rights has varying criteria for such a claim—including the amount of time after death that a claim can be brought.[98] Additionally, in order to make a claim of violation of post-mortem publicity rights, the decedent must have been domiciled in a state with a post-mortem publicity right statute.[99] The estate of Marilyn Monroe encountered difficulty litigating against a company that was selling unauthorized photographs of her for commercial gain.[100] At the time of litigation, New York did not have a post-mortem publicity right statute—since then, New York has enacted such a statute.[101] Because Marilyn Monroe was domiciled in New

89. *See id.*; *see generally* Garrison v. Louisiana, 379 U.S. 64 (1964).
90. *See* Binder, *supra* note 88, at 317-18.
91. RESTATEMENT (SECOND) OF TORTS § 652I (AM. L. INST. 1965).
92. *See* RIGHT OF PUBLICITY SURVEY, *supra* note 16.
93. *See* Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866, 868 (2d Cir. 1953).
94. *See* Peter L. Felcher & Edward L. Rubin, *Privacy, Publicity, and the Portrayal of Real People by the Media*, 88 YALE L.J. 1577, 1588 (1979).
95. *See* Jennifer L. Carpenter, *Internet Publication: The Case for an Expanded Right of Publicity for Non-Celebrities*, 6 VA. J.L. & TECH. 1, 5-6 (2001).
96. *See id.* at 6.
97. *See* RIGHT OF PUBLICITY SURVEY, *supra* note 16.
98. *See id.*
99. *See generally* Milton H. Greene Archives, Inc. v. Marilyn Monroe LLC, 692 F.3d 983, 1000 (9th Cir. 2012).
100. *See id.* at 991-92.
101. *See* James P. Flynn, *Le Morte d'Elvis: The Birth of New Claims as New York Statute Recognizes Post Mortem Right of Publicity*, NAT'L L. REV. (Jan. 19, 2021), https://www.natlawreview.com/article/le-morte-d-elvis-birth-new-claims-new-york-statute-recognizes-post-mortem-right [https://perma.cc/W9G2-39SQ].

York at the time of her death, her estate was unable to make any viable claims against the infringing party.[102]

As technology develops, room for misappropriation of a person's likeness grows to new mediums—specifically, that of a digital clone.[103] Some suggest that there should be a federal right-of-publicity statute specifically addressing post-mortem virtual clones to create a more universal standard.[104] However, such a statute would do nothing to protect private individuals whose estate suffers no compensatory damage from such a privacy violation.

2. Trademark and Copyright Law

You cannot obtain a trademark registration for your identity or persona.[105] It is possible, though difficult, for a celebrity to obtain a trademark for their likeness so long as their trademark application features a mark specific to their likeness—i.e., their name or a distinguishing feature.[106]

Further, this trademark must also function in conjunction alongside a source of goods or services.[107] Thus, such a trademark is bound by commercial use, and any claim of trademark infringement would require some loss of commercial value.[108]

The Lanham Act is a federal statute that prohibits misleading consumers into believing a product is falsely endorsed by another person.[109] While such cases do not necessarily require that a plaintiff actually register a trademark with the United States Patent and Trademark Office, courts have to identify whether such a false endorsement truly creates demonstrable consumer confusion.[110] For example, the U.S. Court of Appeals for the Second Circuit recently emphasized a plaintiff's level of celebrity and notoriety while analyzing the "consumer confusion" element of their Lanham Act claim.[111]

Using artificial intelligence to create a digital clone of a person whose specific features have been trademarked—most likely a celebrity—could be considered trademark infringement so long as it was in the unauthorized advertising of a commercial product.[112] Additionally, using artificial intelligence to create a digital clone of someone promoting a product could be considered a breach of the Lanham Act if it has the potential to create

---

102. *See Milton H. Greene Archives, Inc.*, 692 F.3d at 1000.

103. *See* Smith, *supra* note 11, at 1725.

104. *See, e.g.*, *id.* at 1719.

105. Daniel A. Rozansky et al., *Protecting Image and Likeness Through Trademark Law*, NAT'L L. REV. (Oct. 19. 2021), https://www.natlawreview.com/article/protecting-image-and-likeness-through-trademark-law [https://perma.cc/38QR-2GDM].

106. *See id.*

107. *Id.*

108. *See id.*

109. *See* 15 U.S.C. § 1125(a)(1)(A).

110. Rozansky et al., *supra* note 105.

111. Electra v. 59 Murray Enters., Inc., 987 F.3d 233, 257-59 (2d Cir. 2021) (determining whether professional models' images could appear in ad campaigns for gentlemen's clubs without their consent).

112. Rozansky et al., *supra* note 105.

consumer confusion.[113] However, like the publicity law statutes, each of these types of claims require that the unauthorized use of a digital clone be in a commercial setting.

Alternatively, depending on where a person is getting the media to create a digital clone, unauthorized use could be a case of copyright infringement. Condé Nast tested this theory by attempting to get a deepfake video of Kim Kardashian—created by manipulating a video of Kardashian originally posted by Condé Nast—taken off Instagram and YouTube.[114] However, under the Fair Use Doctrine, it is likely that this deepfake video is not actually infringing upon a copyright.[115] The video could be considered transformative in nature—making a statement on influencer culture by manipulating what the deepfake says—and it was only using a small portion of the original Condé Nast video.[116] The video was quickly removed from YouTube using its internal Content ID claim feature,[117] but as of October 2022, the video remains on Instagram.[118] An interesting separate conundrum is whether a digital clone itself might be copyrightable.[119] The World Intellectual Property Organization approached this, and a number of other similar, hypothetical questions in a recent session on intellectual property and artificial intelligence.[120]

Texts and emails could be considered intellectual property.[121] But while the unauthorized publishing of texts and/or emails could certainly lead to infringing upon someone's intellectual property, it is possible that using them to create a chatbot (as discussed previously) might also fall within the Fair Use Doctrine.[122] Creating a deep learning, algorithmic chatbot using someone else's text messages could be considered derivative or even educational. Therefore, relying on copyright, trademark, or intellectual property law to protect against the unauthorized creation and use of a digital clone—post-mortem or not—does not appear to be a viable route.

---

113. *See* 15 U.S.C. § 1125(a)(1)(A); *see also* Brenna Gibbs, *Is Seeing Still Believing? Deepfakes and Their Future in the Law*, MICH. TECH. L. REV. BLOG (Oct. 30, 2019), http://mttlr.org/2019/10/is-seeing-still-believing-deepfakes-and-their-future-in-the-law/ [https://perma.cc/V9KC-3SD7].

114. Samantha Cole, *The Kim Kardashian Deepfake Shows Copyright Claims Are Not the Answer*, VICE (June 19, 2019, 2:18 PM), https://www.vice.com/en/article/j5wngd/kim-kardashian-deepfake-mark-zuckerberg-facebook-youtube [https://perma.cc/EJV8-ZCYA].

115. *Id.*

116. *Id.*

117. *Id.*

118. Bill Posters (@bill_posters_uk), INSTAGRAM (June 1, 2019), https://www.instagram.com/p/ByKg-uKlP4C/ [https://perma.cc/9C3R-5LCN].

119. *See* Truby & Brown, *supra* note 5, at 159-60.

120. *See* generallyWORLD INTELL. PROP. ORG. SECRETARIAT, WIPO CONVERSATION ON INTELLECTUAL PROPERTY (IP) AND ARTIFICIAL INTELLIGENCE (AI) (2020), https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_ai_2_ge_20/wipo_ip_ai_2_ge_20_1_rev.pdf [https://perma.cc/L4LC-QAMX].

121. *See* Matt Knight, *The Legal Conundrum of Publishing Text Messages*, SIDEBAR SATURDAYS (July 8, 2017), https://www.sidebarsaturdays.com/2017/07/08/httpwp-mep7vddb-tq-2/ [https://perma.cc/3GEZ-E8DE].

122. *See id.*

3. Criminal Law

As digital cloning and deepfake technology becomes more prevalent and easier to create, the threat and fear of cybercrime increases.[123] In 2021, the Federal Bureau of Investigation ("FBI") released a report warning against malicious actors who may use synthetic content in a criminal manner.[124] Deepfake videos and photos creating the illusion of someone in a compromising position could lead to threats of extortion.[125] Virginia was the first state to criminalize the sharing of deepfake pornography, which superimposes images to make it look as though someone is performing pornographic acts.[126] Other states, like Texas, have focused on criminalizing deepfake technology that targets political figures and/or elections.[127]

With existing audio files on hand, it is also possible for a malicious actor to recreate a person's voice using artificial intelligence capabilities.[128] There have already been a variety of attempted fraudulent swindles using such technology.[129] For example, fraudsters are now able to use voice cloning technology to bypass voice biometric systems, which are meant to confirm a person's identity.[130] Monica Sedky, an attorney for the U.S. Department of Justice, has suggested that using a cloned voice in such a fraudulent effort could likely be prosecuted under 18 U.S.C. §§ 1028 and 1029—federal fraud and aggravated identity theft statutes.[131] While there are no reports of it happening yet, the ability to voice clone someone who has already passed away may eventually lead to identity theft and Social Security fraud—

123. *See* Dave McKay, *How Deepfakes Are Powering a New Type of Cyber Crime*, HOW-TO GEEK (July 23, 2021, 8:00 AM), https://www.howtogeek.com/devops/how-deepfakes-are-powering-a-new-type-of-cyber-crime/ [https://perma.cc/NBD8-C6H9].

124. CYBER DIV., FED. BUREAU INVESTIGATION, MALICIOUS ACTORS ALMOST CERTAINLY WILL LEVERAGE SYNTHETIC CONTENT FOR CYBER AND FOREIGN INFLUENCE OPERATIONS 1 (2021), https://www.ic3.gov/Media/News/2021/210310-2.pdf [https://perma.cc/J8BY-AXSV].

125. *See* McKay, *supra* note 123.

126. *See* Harmon Leon, *Deepfake Revenge Porn Is Finally Illegal – At Least in One State*, OBSERVER (July 3, 2019, 8:30 AM), https://observer.com/2019/07/deepfakes-revenge-porn-illegal-virginia/ [https://perma.cc/LAS5-W6KW].

127. *See* Kenneth Artz, *Texas Outlaws 'Deepfakes' – But the Legal System May Not Be Able to Stop Them*, LAW.COM (Oct. 11, 2019, 1:20 PM), https://www.law.com/texaslawyer/2019/10/11/texas-outlaws-deepfakes-but-the-legal-system-may-not-be-able-to-stop-them/ [https://perma.cc/TR2M-7LAT].

128. INCREASING THREAT OF DEEPFAKE IDENTITIES, *supra* note 5, at 5.

129. *See, e.g.*, Thomas Brewster, *Fraudsters Cloned Company Director's Voice in $35 Million Bank Heist, Police Find*, FORBES (Oct. 14, 2021, 7:01 AM), https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=3d76f3e57559 [https://perma.cc/75B2-ZTPU]; *see also* Lorenzo Franceschi-Bicchierai, *Listen to This Deepfake Audio Impersonating a CEO in Brazen Fraud Attempt*, VICE (July 23, 2020, 5:01 PM), https://www.vice.com/en/article/pkyqvb/deepfake-audio-impersonating-ceo-fraud-attempt [https://perma.cc/688H-YW2J].

130. *See* Kite-Powell, *supra* note 32.

131. Kyle Wiggers, *Voice Cloning Experts Cover Crime, Positive Use Case, and Safeguards*, VENTUREBEAT (Jan. 29, 2020, 2:10 PM), https://venturebeat.com/2020/01/29/ftc-voice-cloning-seminar-crime-use-cases-safeguards-ai-machine-learning/ [https://perma.cc/BCD7-AXFU].

allowing fraudsters to use voice cloning technology to make it seem like someone is still alive, so as to continue receiving financial benefits from the government.[132]

Although the FBI has made efforts to warn the public about the dangers of deepfake technology, there are very few criminal sanctions to fight against potential malicious behavior. Only a few states have even made the effort to propose laws that fight against the most drastic iterations of digital cloning technology—pornographic images and political figure manipulation.[133] And the federal government seems to be in a wait and see cycle, trying to determine the biggest potential threats arising from deepfake technology. As of now, there are no criminal sanctions in place to mitigate unauthorized post-mortem digital cloning without a showing of clear, tangible harm arising from fraudulent use.

III. ANALYSIS

Regulating the creation and use of digital cloning and synthetic media is not intended to place a chilling effect on the development of artificial intelligence. Synthetic media can certainly bring about valuable benefits to society. For example, voice cloning technology can give back the voice of someone who is no longer able to audibly communicate.[134] Post-mortem digital cloning can bring comfort to those mourning their loved ones.[135] Interactive chat bots can reconnect children to their deceased family members.[136] And interactive holograms can tell future generations stories from historical events, straight from the mouths of the people who actually experienced them.[137]

But there are also many harms that have already arisen from deepfake technology—revenge porn, political interference, harm to reputation.[138] As technology grows, there will almost certainly come a time where society can no longer identify whether media is real or synthetic. And in response to the fear of posted, online media being manipulated while one is still alive or even after one's passing, there may arise an extreme chilling effect—minimizing societal online engagements and fearing new, exciting technological advances.

---

132. *Cf.* Tresa Baldas, *Social Security Scammers Invented Wild Cover Stories, Posed as Dead Relatives, Feds Say*, USA TODAY (Oct. 2, 2019, 7:19 PM), https://www.usatoday.com/story/news/nation/2019/10/02/feds-target-social-security-scammers-living-off-dead-relatives/3841975002/ [https://perma.cc/GS5W-YFBB] (revealing a man who raised the pitch of his voice on phone calls to pretend to be his dead mother).

133. *See* Briscoe, *supra* note 37.

134. *See* Kite-Powell, *supra* note 32.

135. *See* Ursache, *supra* note 54; *see also* Sarah Beth Guevara, *Breonna Taylor Gets Immortalized in an Augmented Reality App*, GOOD MORNING AM. (Dec. 17, 2021), https://www.goodmorningamerica.com/living/story/breonna-taylor-immortalized-augmented-reality-app-81678852 [https://perma.cc/Y987-URWM].

136. *See* Vlahos, *supra* note 51.

137. *See* Katz, *supra* note 55.

138. *See supra* Section II.A.

This section will address specific attempts to curb deepfakes and digital cloning. But as this technology is so new, these types of claims remain highly speculative. Courts have yet to set a precedent for claims against unauthorized digital cloning, and legislators have only produced limits to the most severe instances.[139] Further, these hypothetical legal claims could not be applied post-mortem. This section will present probate law as a novel solution to this issue, arguing that modern estate planning should require a digital legacy clause, dictating how one's digital assets should be accessed and used after death. Existing probate law should also be expanded to further safeguard against unauthorized digital cloning.

A. Lackluster Solutions to Curb Deepfakes and Digital Cloning

Artificial intelligence will likely continue growing at unprecedented speeds, and hopefully legislators will eventually catch up with these developments. Some believe deepfake technology should not be regulated at all,[140] while others grow concerned that the rate of legislation is not in step with the rate of technological growth.[141] In 2021, the Deep Fakes Accountability Act was introduced in Congress.[142] This act would require producers of deepfakes to include digital watermarks and disclosures on their products, ensuring that the public is aware they are viewing synthetic media.[143] But skeptics have voiced concerns that those with bad intentions will simply not abide by such regulations, regardless of whether they are passed.[144]

Some deepfake apps and websites are free and readily accessible to the public.[145] Synthetic media creations using this kind of software are typically limited to superimposing one's face onto preselected characters or celebrities or manipulating a photo of someone by assigning to it a variety of preprogrammed moves.[146] These websites have a variety of terms and conditions, suggesting that their content is self-regulated in some way. For example, one of the terms that Avatarify sets forth requires that users "not use the App in any way that violates any rights of a third party, including

139. *See supra* Section II.C.3.

140. *See generally Chapter 5: AI Policy and Governance*, *in* STAN. INST. FOR HUM.-CENTERED AI, THE AI INDEX 2022 ANNUAL REPORT 172 (2022), https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report_Master.pdf [https://perma.cc/UKB7-AECC].

141. *See, e.g.*, Cade Metz, *How Will We Outsmart A.I. Liars?*, N.Y. TIMES (Nov. 19, 2018), https://www.nytimes.com/2018/11/19/science/artificial-intelligence-deepfakes-fake-news.html [https://perma.cc/6VH8-V3CL].

142. DEEP FAKES Accountability Act, H.R. 2395, 117th Cong. (2021).

143. *Id.*

144. Mathew Ingram, *Legislation Aimed At Stopping Deepfakes Is a Bad Idea*, COLUM. JOURNALISM REV. (July 1, 2019), https://www.cjr.org/analysis/legislation-deepfakes.php [https://perma.cc/A8FZ-SC3A].

145. Geoffrey A. Fowler, *Anyone with an iPhone Can Now Make Deepfakes. We Aren't Ready for What Happens Next.*, WASH. POST (Mar. 25, 2021, 8:00 AM), https://www.washingtonpost.com/technology/2021/03/25/deepfake-video-apps/ [https://perma.cc/X9GE-NA3J].

146. *Id.*

intellectual property rights, data privacy rights, rights of publicity and privacy rights."[147] Similarly, Deepfakes Web prohibits users from "[i]nfringement of property rights, portrait rights, publicity rights, personal rights, honor rights[,] or privacy rights of Company or any third party."[148] However, these sites provide no clear indication on how they intend to enforce compliance.[149]

So, what could one do after discovering the existence of an unauthorized digital clone of themself? Currently, there is no clear way to make a claim against the unauthorized use of one's likeness in deepfake technology. Courts have referenced "deep fake" or "deepfake" technology in fewer than 10 published decisions, and each instance was more of a passing mention than an actual analysis into its legal merits as a claim or defense.[150] Existing publicity rights law only has the potential to protect recognizable celebrities from the unauthorized creation of digital clones used for commercial purposes—and only in states with such publicity rights laws.[151]

Regardless of the failure or success of a right of publicity claim in such a scenario, the existing laws would likely not extend to protect private parties, or even celebrities, against any non-commercial use of an unauthorized digital clone.[152] If the digital clone were pornographic in nature, depending on the state's deepfake statutes, civil or criminal action could be brought.[153] Similarly, if the digital clone were being used to improperly influence a political race, depending on the state's deepfake statutes, civil or criminal action could also be brought.[154] Here too, courts have not yet had the opportunity to make a ruling on such a suit. If none of the above criteria applies but a person still wishes to find relief against the unauthorized creation and use of a digital clone of themselves, a defamation or libel claim would likely be the next best option.[155] But this, too, has yet to be tested in court.

Each of these potential methods through which claims could be made would require a showing of harm to a particular person. But this kind of reasoning does not work after death, as it has long been held that deceased persons cannot experience harm.[156] Even with the existence of hypothetically successful solutions to curb deepfakes and digital cloning, none of these solutions could be applied to protect private parties post-mortem. Celebrities should not be the only ones who can protect their legacy after death. While someone is alive, they can identify media that has been made to look like them

147. *Terms of Service*, AVATARIFY, https://avatarify.ai/terms [https://perma.cc/R5P7-H8PC] (last modified July 17, 2020).

148. *Terms of Use*, DEEPFAKES WEB, https://deepfakesweb.com/terms [https://perma.cc/V6CS-5JTU] (last modified Feb. 21, 2021).

149. *See* Fowler, *supra* note 145.

150. *See, e.g.*, People v. Smith, 969 N.W.2d 548, 565 (Mich. 2021) ("[W]e are mindful that in the age of fake social-media accounts, hacked accounts, and so-called deep fakes, a trial court faced with the question whether a social-media account is authentic must itself be mindful of these concerns."); *Aerotek, Inc. v. Boyd*, 624 S.W.3d 199, 214 (Tex. 2021).

151. *See supra* Section II.C.1.

152. *See id.*

153. *See supra* Section II.C.3.

154. *See id.*

155. *See supra* Section II.C.1.

156. *See id.*

doing something or saying something they never did or said. They could try to refute it, sue the creator, or request injunctive relief. But after someone dies and can no longer bring a claim, what is to keep people from creating synthetic media that is indistinguishable from real media and sharing it with the world? Without standing, how can your family, estate, or personal representative protect your digital persona after you die?

B. The Solution to Unauthorized Post-Mortem Digital Cloning Uses the Legal Mechanisms Controlling Property Through Probate Law

Property rights are typically the exclusive right awarded to deceased people,[157] and probate law gives credence toward a decedent's intent before death regarding their property.[158] The Uniform Probate Code indicates that one of its primary purposes is "to discover and make effective the intent of a decedent in distribution of the decedent's property."[159] The idea of inheritance law has existed since Roman times.[160] And people have tried to apply the Roman concept of post-mortem rights to a variety of claims—most of which, like privacy rights, have been unsuccessful.[161] As previously discussed, in the United States, the right to privacy is not maintained after death.[162]

Many courts have granted certain privacy rights to dead bodies—holding that images exploiting corpses, or actions degrading corpses, should not be allowed.[163] However, the courts consistently cite to the feelings of the family members left behind, not the feelings of the person who has died, as the reasoning behind such decisions: "Family members have a personal stake in honoring and mourning their dead and objecting to unwarranted public exploitation that, by intruding upon their own grief, tends to degrade the rites and respect they seek to accord to the deceased person who was once their own."[164] Further, these instances typically must be so egregious that they shock the conscience.[165]

In the 1890s, the City of New York wished to raise money to erect a statue of Mary Hamilton Schuyler in order to honor her philanthropy from when she was alive.[166] Her family objected to the statue, claiming that she was a private person and would not have wanted her image celebrated in such a way.[167] The court reasoned that any findings in support of protecting the dead are exclusively in relation to how it affects the living and that, in this case, the Schuyler family would not be deeply harmed by the erection of such

157. *See id.*
158. UNIF. PROB. CODE § 1-102(b)(2) (amended 2020).
159. *Id.*
160. *See generally* Max Radin, *Fundamental Concepts of the Roman Law*, 13 CALIF. L. REV. 207, 224-26 (1925).
161. *See, e.g.*, Smolensky, *supra* note 83, at 790, 795.
162. *See supra* Section II.C.1.
163. *See, e.g.*, Marsh v. Cnty. of San Diego, 680 F.3d 1148, 1157 (9th Cir. 2012).
164. Nat'l Archives & Recs. Admin. v. Favish, 541 U.S. 157, 168 (2004).
165. *See Marsh*, 680 F.3d at 1154-55.
166. *See* Schuyler v. Curtis, 42 N.E. 22, 24 (N.Y. 1895).
167. *Id.* at 24-25.

a statue.[168] The dissent in this case, however, articulated similar concerns addressed in this Note about maintaining the right to conserve one's image and privacy in life and death:

> The evidence does not establish that Mrs. Schuyler was a public character, nor that she was in such public station, or so prominent in public works, as to make her name and memory public property . . . . [S]he was never a public character, and in no just sense can it be said that, because of what she chose to do in the private walks of life, she dedicated her memory to the state or nation, as public property. To hold that by reason of her constant and avowed interest in philanthropical works unconnected with public station, the right accrued to an association of individuals, strangers to her blood, to erect a statue of her, typifying a human virtue, through contributions solicited from the general public, is, in my judgment, to assert a proposition at war with the moral sense, and I believe it to be in violation of the sacred right of privacy, whose mantle should cover not only the person of the individual, but every personal interest which he possesses and is entitled to regard as private . . . . [169]

Unfortunately, the dissenter was unable to convince his fellow justices that Mrs. Schuyler's wishes should be honored.

As discussed, protecting the rights and wishes of the deceased is rarely, if ever, a priority of courts except in certain probate matters.[170] In fact, successful claims supporting post-mortem rights are often those concerning property rights.[171] There is a reason why publicity rights are a consistently successful tort claim that can be made on behalf of the deceased.[172] While publicity rights are technically within the scope of privacy law, the reasoning for these claims are typically based in property law, as it is the celebrity's estate that suffers from the unauthorized commercial use of the decedent's likeness.[173]

C. Digital Assets Are Already Included in Existing Probate Law

In 2015, the Revised Uniform Fiduciary Access to Digital Assets Act ("RUFADAA") was approved and recommended for enactment by the Uniform Law Commission.[174] As of March 2021, 48 states have enacted laws addressing what happens to a person's digital assets after they die—46 of

168. *Id.* at 27.
169. *Id.* at 28 (Gray, J., dissenting).
170. *See* Smolensky, *supra* note 83, at 763, 772.
171. *See id.* at 765.
172. *See id.*
173. *See id.* at 769.
174. REVISED UNIF. FIDUCIARY ACCESS TO DIGIT. ASSETS ACT (UNIF. L. COMM'N 2015).

which adopted RUFADAA or some version of it.[175] RUFADAA defines a digital asset as "an electronic record in which an individual has a right or interest."[176] Courts have yet to officially define what a "digital asset" is,[177] but it is colloquially accepted that types of digital assets include emails, text messages, electronic files on the cloud (like photos and videos), social media accounts, and more.[178]

RUFADAA provides that if explicitly drafted in a person's will, digital fiduciaries can be given managerial access to a decedent's digital assets.[179] This 2015 revision came about after the original act was met with strong opposition due to its lack of requirement for express consent by the decedent prior to their death.[180] The opposition was partially based on concerns for a decedent's personal privacy in electronic communications.[181] Online service providers are subject to the Stored Communications Act, which imposes certain privacy requirements.[182] The original Uniform Fiduciary Access to Digital Assets Act, by allowing fiduciaries access without affirmative action on the part of the decedent, risked placing these online service providers in conflict with federal law.[183]

The revised act, on the other hand, requires that the decedent take an affirmative step in their estate planning process to assign a digital executor to manage their digital assets—by maintaining exclusive control, deleting online profiles, distributing digital assets among the decedent's beneficiaries, etc.[184] This affirmative step sometimes occurs in online tools provided by certain companies,[185] like the Facebook Legacy Contact.[186] There are also a number

---

175. *Access to Digital Assets of Decedents*, NAT'L CONF. STATE LEGISLATURES (Mar. 26, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/access-to-digital-assets-of-decedents.aspx#2020 [https://perma.cc/447S-KLXM].

176. REVISED UNIF. FIDUCIARY ACCESS TO DIGIT. ASSETS ACT § 2.10.

177. Joseph Ronderos, Note, *Is Access Enough?: Addressing Inheritability of Digital Assets Using the Three-Tier System Under the Revised Uniform Fiduciary Access to Digital Assets Act*, 18 TRANSACTIONS: TENN. J. BUS. L. 1031, 1047 (2017).

178. *See Digital Asset Estate Planning: What You Should Know*, PNC INSIGHTS (Aug. 24, 2021) [hereinafter *Digital Asset Estate Planning*], https://www.pnc.com/insights/wealth-management/living-well/digital-asset-estate-planning-what-you-should-know.html [https://perma.cc/66RM-62L4].

179. *See* REVISED UNIF. FIDUCIARY ACCESS TO DIGIT. ASSETS ACT §§ 6, 15.

180. *See* Betsy Simmons Hannibal, *The Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA)*, NOLO, https://www.nolo.com/legal-encyclopedia/ufadaa.html [https://perma.cc/MQH7-V7FP] (last visited Apr. 12, 2022).

181. *See id.*

182. *See generally* Sasha A. Klein & Mark R. Parthemer, *Who Will Delete the Digital You? Understanding Fiduciary Access to Digital Assets*, PROB. & PROP. MAG, JULY-AUG. 2017.

183. *See id.*

184. *See* Rachel Sommer, *What is RUFADAA and Why Should You Care?*, EASEENET (Apr. 19, 2021), https://easeenet.com/blog/what-is-rufadaa-and-why-should-you-care/ [https://perma.cc/C4S9-665H].

185. *See, e.g.*, Jennifer Pattison Tuohy, *Apple Will Soon Let You Pass on Your iCloud Data When You Die*, VERGE (Nov. 10, 2021, 8:49 PM), https://www.theverge.com/2021/11/10/22774873/apple-digital-legacy-program-comes-to-ios15-iphones-macs [https://perma.cc/EYX7-R542].

186. *See generally What Is a Legacy Contact and What Can They Do With My Facebook Account?*, FACEBOOK, https://www.facebook.com/help/1568013990080948 [https://perma.cc/Q5EK-VMS7] (last visited Apr. 12, 2022).

of digital vault services that provide assistance to its users in digital estate planning.[187] Other ways to provide for one's digital assets are through wills or trusts.[188] Unfortunately, many people die without having conducted any estate planning.[189] And in the absence of an active assignment of a digital estate custodian, all digital assets remain under the terms of the relevant service provider—potentially infinitely excluding access to their digital records after death.[190]

After an examination of current legislation and common law standards regarding post-mortem legal mechanisms, probate law is a logical area to seek protection against unauthorized post-mortem digital cloning technology. By enacting some version of RUFADAA, most states' probate laws already provide direction for a variety of digital assets.[191] As such, RUFADAA should be expanded to specifically preclude a decedent's digital assets from being used to create any kind of digital clone without their express approval.

D. The Media Used to Create Digital Clones Should Be Considered Digital Assets, and RUFADAA Should Be Expanded to Protect Against Their Unauthorized Use

The world has become almost exclusively digital.[192] Any photos, videos, or audio that might be used to create a digital clone of someone almost certainly lives in their digital cloud or on their social media profile.[193] Likewise, texts, emails, and social media posts found online or in the cloud could be used to create algorithmic post-mortem chatbots.[194] Even in using Eternime or the Microsoft patent project, unfettered access to a person's social media accounts would be required.[195] Courts should be led by RUFADAA's definition of a digital asset and interpret each of these potential digital cloning ingredients as a digital asset that is controlled and protected through probate law after death. Estate planning in the modern era now involves the consideration of who will have access, control, and possession of your digital assets after you die.[196] But this consideration should go a step further. During estate planning, a person should ask themselves: "How do I want my digital

187. *See* Cheryl Winokur Munk, *Organizing Digital Assets—A Life and Death Matter*, FORBES (July 14, 2020, 10:00 AM), https://www.forbes.com/sites/cherylwinokurmunk/2020/07/14/dont-let-digital-assets-get-lost-or-stolen-in-cyberspace/ [https://perma.cc/MV4C-TX2V].

188. *See Digital Asset Estate Planning*, *supra* note 178.

189. *See* Alberto B. Lopez, *Posthumous Privacy, Decedent Intent, and Post-Mortem Access to Digital Assets*, 24 GEO. MASON L. REV. 183, 187 (2016).

190. *See* Ronderos, *supra* note 177, at 1038.

191. REVISED UNIF. FIDUCIARY ACCESS TO DIGIT. ASSETS ACT prefatory note (UNIF. L. COMM'N 2015).

192. *See* Natalie M. Banta, *Inherit the Cloud: The Role of Private Contracts in Distributing or Deleting Digital Assets at Death*, 83 FORDHAM L. REV. 799, 800-03 (2014).

193. *See id.*

194. *See id.*

195. *See supra* Section II.B.

196. *See* Lopez, *supra* note 189, at 187.

assets to be used after I die? Do I want my digital assets to be used to digitally resurrect me after death?"

Just as probate courts allow for certain provisions in a person's will to determine how their property should be used after they die,[197] so too should probate courts allow for stipulations on how their digital property should be used. People should be able to expressly allow for their digital assets to be used for post-mortem digital cloning—for science, innovation, mourning, or any other purpose that could be conceived. Alternatively, people should be able to definitively lay out in their will that they do not wish for their digital assets to be used in such a way.

Some celebrities and actors have already begun getting digital scans of themselves while still alive (or still young), in order to potentially use them for future projects.[198] While some are hesitant to have their likeness digitally scanned,[199] others see it as an opportunity to preemptively bring in more financial support for their estate after they die.[200] With such proactive behavior, the actors are clearly making an effort to ensure proper future use of their digital scans after they die.[201] These digital scans would certainly be considered digital assets—assets that are specifically laid out in the person's will, with details on how to access and use them after they die. Although such thorough digital scans would not be required for a digital clone to be created, the decedent's intentions for their use should be valued in the same way as a decedent's intention for any other digital asset's use. Like a celebrity planning for their death, so too should private citizens be mindful and prepared to address how their digital assets should be used after their death.

Most states require express consent for someone to be able to access a decedent's digital assets under RUFADAA-like probate statutes.[202] A future decedent is required to expressly identify their digital fiduciary—someone who can act in their best interest after they die regarding accessing and managing their digital assets.[203] Without so expressing, such media cannot be touched.[204] A simple way to assign a digital fiduciary is through a digital legacy-type clause in one's will.[205] After dictating who their digital fiduciary should be, the future decedent should then expressly identify in their digital legacy clause how they wish their digital assets to be used—including whether they would allow for their digital assets to be used to create a digital clone of themself after their death. Digital legacy clauses should certainly

197. *See generally* RESTATEMENT (FIRST) OF PROP. § 437 (AM. L. INST. 1936).

198. *See* Ben Laney, Comment, *Bringing the Dead Back to Life: Preparing the Estate for a Post-Mortem Acting Role*, 12 EST. PLAN. & CMTY. PROP. L.J. 349, 352-53 (2020).

199. Chris Lee, *Digital Doubles Are Revolutionizing Hollywood. But Why Do Some Movie Stars Hate Them?*, VULTURE (Dec. 12, 2018), https://www.vulture.com/2018/12/why-do-movie-stars-hate-being-digitally-scanned.html [https://perma.cc/NSR7-WHXD].

200. *See Peter Cushing's Digital Resurrection*, *supra* note 61; *see also* Laney, *supra* note 196, at 352-53.

201. *See* Laney, *supra* note 198, at 352-53.

202. *See* Sommer, *supra* note 184.

203. *See id.*

204. *See id.*

205. *See* REVISED UNIF. FIDUCIARY ACCESS TO DIGIT. ASSETS ACT § 6 (UNIF. L. COMM'N 2015).

expand over the years as technology grows and further digital capabilities emerge.

To further safeguard against post-mortem digital cloning, RUFADAA statutes should be expanded to not only protect against the unauthorized access of a decedent's digital assets, but also their unauthorized use. Section 15 of RUFADAA states that a digital fiduciary may not use a decedent's digital assets to "impersonate the user."[206] RUFADAA statutes should be expanded to insist that unless express permission exists, digital assets should not be used by anyone in such a way that impersonates or digitally resurrects the decedent. Further, as RUFADAA specifically protects against unauthorized access to a decedent's social media account, a digital fiduciary or beneficiary should not be allowed to then give access to sites like Eternime[207] (or whatever the Microsoft patent becomes)[208] without express permission from the decedent. By expanding RUFADAA, even if a person dies before expressing how they wish their digital assets to be used, there is still a defense against unauthorized digital cloning.

It could be difficult to protect against an instance in which a fiduciary goes against the decedent's express wishes and creates (or commissions the creation of) a digital clone of the decedent. As the person authorized to protect a person's digital assets, there would be no immediate recompense if the fiduciary themselves breached their fiduciary duty. So, when assigning a digital fiduciary, one must select a person they are confident will follow through with their requests after death.

Further, fiduciaries under RUFADAA have the same fiduciary duties as those under other areas of probate law.[209] They must act in the best interest of the decedent, and they have a legal duty of care, loyalty, and confidentiality regarding their management of the digital assets.[210] As previously stated, RUFADAA also already protects against a fiduciary's use of a digital asset to impersonate the user.[211] Creating a digital clone of someone doing and saying things that they never did or said while still alive could certainly be interpreted as a type of impersonation of them. Should a digital fiduciary breach their duties, as with any type of fiduciary, interested parties or next of kin would need to file a petition in probate court and have a judge determine whether the digital fiduciary should be replaced and whether injunctive relief is available.[212]

The rule against perpetuities prevents someone from using a will to control their private property for a time long past the lives of those living at the time the will was written.[213] While only a few states still maintain a

206. *Id.*
207. Ursache, *supra* note 54.
208. Brown, *supra* note 59.
209. *See generally* Klein & Parthemer, *supra* note 182.
210. REVISED UNIF. FIDUCIARY ACCESS TO DIGIT. ASSETS ACT § 15.
211. *Id.*
212. *See, e.g.*, *In re* Karavidas, 999 N.E.2d 296, 301 (Ill. 2013).
213. GEORGE GLEASON BOGERT ET AL., THE LAW OF TRUSTS & TRUSTEES § 213 (3d ed. 2007).

common law rule against perpetuities,[214] there has also been no judicial consideration about how it would apply to the control of a decedent's digital assets. Most current post-mortem publicity rights statutes identify the length of time that estates can claim protection for the decedents in question.[215] These state statute time frames range from 10 to 100 years.[216] Again, with the constant evolution of technology, social media, and online hosting platforms, the fate and length of everyone's online presence and digital legacy is largely unknown.[217] However, when determining the length of time for post-mortem protections against the unauthorized creation of digital clones, as set forth in a person's will, following the publicity right statutes and allowing for a limit of no more than 100 years seems a reasonable constraint.

A decedent's affirmative action prior to their death could encourage proper digital cloning when desired. But by requiring affirmative action on the part of the decedent, unauthorized post-mortem digital cloning would be minimized, leading to fewer fears of putting oneself out into the world digitally only to have one's digital footprint taken over and maliciously or unsuitably resurrected after death.

IV. CONCLUSION

Over the next few years, artificial intelligence will only grow in popularity and become more accessible to the general public. There must be preemptive action to protect against a free range of artificial intelligence creations—especially synthetic media. To protect private citizens against the unauthorized creation and use of synthetic media and digital clones after death, probate law should automatically disallow such actions unless explicit permission is given prior to death. This will allow for an atmosphere that supports innovation and technology while also avoiding litigation to determine whether certain kinds of technology cross the line of misappropriation. Setting firm boundaries now, while synthetic media and digital clones are still in their formative years, will avoid instances of gross unauthorized misappropriation of such technology in the years to come.

214. *Id.* at § 214.
215. *See* RIGHT OF PUBLICITY SURVEY, *supra* note 16.
216. *See id.*
217. *See* Banta, *supra* note 192, at 800-03.