EDITOR'S NOTE

The *Federal Communications Law Journal* is proud to present the third and final issue of Volume 77. FCLJ is the nation's premier communications law journal and the official journal of the Federal Communications Bar Association (FCBA). Over the course of Volume 77's publication, we have had the opportunity to highlight articles and student Notes that showcase the diverse range of issues in the fields of technology and communications law.

This Issue begins with an article from International Tribunal for the Law of the Sea (ITLOS) Judge Osman Keh Karama and Abraham Kazmir. The article analyzes the current legal framework governing the protection of undersea cables and transoceanic pipelines and argues for reforms that address issues such as international cooperation, jurisdictional boundaries, environmental threats, and energy security.

This Issue also features four student Notes. First, Arjun Singh proposes additional statutory provisions to the Foreign Intelligence Surveillance Act (FISA) to enhance impartiality in court proceedings and protect Americans' "reasonable expectation of privacy" under the Fourth Amendment.

Second, Lenni Elias examines the Illinois Biometric Information Privacy Act (BIPA), arguing that its private right of action should be extended to cases where employee biometric data is mishandled at the hands of employers.

Third, Nathan Eichten discusses the shortcomings of the Telecommunications Act of 1996 and proposes a series of amendments to promote long-lasting competition among leaders in the telecommunications industry.

Fourth, Ellen Manby addresses gender bias in artificial intelligence voice assistants, arguing that European laws prohibiting gender discrimination in advertisements should serve as the framework for U.S. regulation to curb harmful and discriminatory effects.

Finally, this Issue concludes with our Annual Review of notable court decisions that have impacted the communications field in recent years. Each of these was authored by a member of our Journal, and we appreciate their thoughtful analyses of these important cases.

The Editorial Board of Volume 77 would like to thank the FCBA and The George Washington University Law School for their continued support of the Journal. We also appreciate the hard work of the authors and editors who contributed to this Issue.

The *Federal Communications Law Journal* is committed to providing its readers with in-depth coverage of relevant communication and technology 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.

Addison Spencer
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, First Amendment, broadcasting, telephony, computers, Internet, intellectual property, mass media, technology, privacy, communications and information policymaking, and other related fields.

As the official journal of the Federal Communications Bar Association, the *Journal* is distributed to over 2,000 subscribers, including Association members, as well as legal practitioners, industry experts, government officials and academics. The *Journal* is also distributed by Westlaw, Lexis, William S. Hein, and Bloomberg Law and is available on the Internet at https://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 77 FED. COMM. L.J. ___ (2025).

FEDERAL COMMUNICATIONS LAW JOURNAL
THE TECH JOURNAL
GW LAW VOLUME 77 ISSUE 3 fcba THE TECH BAR
MAY 2025

ARTICLES

This article examines the critical need to strengthen the international legal framework governing the protection of undersea cables and transoceanic pipelines. As global reliance on these vital infrastructures for communication and energy security intensifies, the current legal regime's limitations pose significant challenges to international stability and economic prosperity. The article analyzes the jurisdictional boundaries, inadequacies in addressing non-state actors and multinational corporations, environmental concerns, and energy security implications within the existing legal landscape. Drawing on recent incidents and emerging threats, it proposes a comprehensive set of reforms to enhance international cooperation, expand jurisdiction, strengthen deterrence and environmental protections, improve monitoring and security, and update regulatory frameworks. The recommendations aim to balance the need for enhanced protection with the principles of freedom of navigation and the interests of various stakeholders in the international community. By synthesizing insights from maritime law, environmental principles, and energy security considerations, this article contributes to the ongoing dialogue on adapting international law to address contemporary challenges in protecting critical global infrastructure.

NOTES

The Fourth Amendment guarantees all persons within the United States a "reasonable expectation of privacy" against surveillance, except upon the issuance of warrants for probable cause. The Foreign Intelligence Surveillance Act ("FISA"), an attempt to create a system for effectively monitoring and preventing threats to national security, has often run afoul of this constitutional guarantee. In a digital age, gathering foreign communications—especially by large surveillance programs—invariably leads to the illegal collection of

Enhancing International Legal Protections for Undersea Cables and Transoceanic Pipelines

Judge Osman Keh Karama ITLOS & Abraham Kazmir*

TABLE OF CONTENTS

* Disclaimer: This article does not represent the official views or opinions of the International Tribunal for the Law of the Sea (ITLOS) or any of its members. The analysis and recommendations contained herein are solely those of the authors in their personal capacities and should not be attributed to or construed as reflecting the position of ITLOS or any other institution with which the authors may be affiliated.

I. INTRODUCTION

This article addresses the critical need to strengthen the international legal framework governing the protection of undersea cables and transoceanic pipelines. Given the paramount importance of these assets to global communications, energy security, and international trade, the current legal regime's boundaries present challenges to international stability and economic prosperity.

The analysis begins with a comprehensive background section, which examines the current legal landscape governing these critical infrastructures and highlights the emerging threats that underscore the urgency of reform. The background provides context for the subsequent legal analysis, which forms the core of this paper.

Part II provides background on the current legal framework governing undersea cables and pipelines, tracing the evolution of international maritime law and its application to this critical infrastructure. It then delves into the emerging threats facing these assets, including recent incidents of sabotage and accidental damage. This section aims to contextualize the need for enhanced protections within the broader landscape of global security and economic interdependence.

Part III analyzes the legal challenges in protecting undersea cables and pipelines. It begins by examining the jurisdictional limitations inherent in the current regime, particularly focusing on the issues of flag state jurisdiction and the potential application of universal jurisdiction. The analysis then explores the inadequacies of the current framework in addressing threats from non-state actors and multinational corporations. Additionally, this section considers the application of environmental law principles to undersea infrastructure protection and assesses the implications of infrastructure vulnerabilities for global energy security.

Part IV addresses the potential solutions for enhancing the protection of undersea cables and pipelines. It focuses on five main areas: enhancing international cooperation, expanding jurisdiction, strengthening deterrence and environmental protections, improving monitoring and security, and updating regulatory frameworks. For each, the article will propose specific legal and institutional reforms, drawing on successful models from other areas of international law.

Part V offers recommendations for implementing the proposed solutions. These suggestions aim to balance the need for enhanced protection with the principles of freedom of navigation and the interests of various stakeholders in the international community.

All of this concludes by synthesizing the key points and reflecting on the broader implications of strengthening the legal framework for undersea infrastructure protection on international security, economic stability, and the future of global communications and energy systems.

II. BACKGROUND

A. Current Legal Framework

The primary international instrument governing undersea cables and pipelines is the United Nations Convention on the Law of the Sea ("UNCLOS").[1] While UNCLOS provides for the freedom to lay submarine cables and pipelines on the high seas (Article 87) and on the continental shelf (Article 79), it fails to establish a comprehensive regime for their protection, particularly in areas beyond national jurisdiction.[2]

UNCLOS grants coastal states limited jurisdiction over cables and pipelines on their continental shelf, allowing them to take "reasonable measures" for exploration and exploitation of natural resources.[3] However, these measures must not impede the laying or maintenance of cables.[4] In the exclusive economic zone ("EEZ"), all states enjoy the freedom to lay submarine cables, subject to the coastal state's rights and duties.[5]

The Convention for the Protection of Submarine Telegraph Cables of 1884 remains in force for its 36 signatories, criminalizing willful or negligent damage to submarine cables.[6] However, its effectiveness is limited by its age and specific focus.[7]

Recent incidents as discussed above have highlighted the vulnerabilities of submarine cables. In response to these threats, some states have taken unilateral action. The United States ("U.S.") passed the Undersea Cable Control Act in 2023, aiming to prevent adversaries from acquiring technologies used in cable development.[8] Australia has established "cable protection zones" with restricted activities.[9]

International bodies have also recognized the importance of cable protection.[10] The United Nations ("UN") General Assembly has passed resolutions emphasizing the critical nature of submarine cables as

1. *See* United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS].
2. DOUGLAS R. BURNETT, ROBERT C. BECKMAN & TARA M. DAVENPORT, SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 63 (2d ed. 2014).
3. UNCLOS, *supra* note 1, art. 79(2).
4. *Id.*
5. *Id.* art. 58.
6. *See* Convention for the Protection of Submarine Telegraph Cables, Mar. 14, 1884, 24 Stat. 989, T.S. No. 380.
7. BURNETT ET AL., *supra* note 2.
8. Undersea Cable Control Act, H.R. 1189, 118th Cong. § 2(a) (2023).
9. *Zone to Protect Sydney Submarine Cables*, AUSTRALIAN COMMC'NS AND MEDIA AUTH., https://www.acma.gov.au/zone-protect-sydney-submarine-cables [https://perma.cc/382R-5MVC] (last visited Apr. 4, 2025).
10. *See Telecommunications Act 1997* (Cth) sch 3A (Austl.).

infrastructure.[11] The International Cable Protection Committee, while lacking formal authority, has issued best practice guidelines for cable protection.[12]

Despite these efforts, significant gaps remain in the international legal framework.[13] The lack of a comprehensive treaty addressing modern threats to submarine cables, including hacking and sabotage, leaves this critical infrastructure vulnerable.[14] As technology advances and geopolitical tensions rise, the need for an updated international regime becomes increasingly apparent.

B. Emerging Threats

Recent incidents have highlighted the vulnerabilities of submarine cables. Most recently, on November 18, 2024, a submarine data communications cable across the Baltic Sea between Finland and Germany broke, with Finnish authorities investigating the cause of the disruption.[15] This incident involving the C-Lion1 cable, Finland's only direct data communications link to central Europe, further emphasizes the ongoing vulnerabilities of critical undersea infrastructure.[16]

In March 2024, several undersea cables in the Red Sea were damaged—reportedly by the anchor of a ship that was struck and sunk during an attack by Houthi rebels.[17] This incident not only disrupted global communications but also highlighted the complex interplay between maritime security, geopolitical conflicts, and the protection of undersea infrastructure.

In February 2023, multiple undersea cables connecting Taiwan were damaged, disrupting internet connectivity.[18] While initial reports suggested

---

11. *See* Scott Jasper, *Protecting Submarine Cables: The Security Gap in International Law,* 47 OCEAN DEV. & INT'L L. 362, 363 (2016).

12. *Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables (Version 1.2)*, INT'L CABLE PROT. COMM., https://www.iscpc.org/documents/?id=3507 [https://perma.cc/HV9G-46YE] (last visited Apr. 4, 2025).

13. RISHI SUNAK, UNDERSEA CABLES: INDISPENSABLE, INSECURE, 16, 17 (Pol'y Exch. 2017).

14. Amy Paik & Jennifer Counter, *International Law Doesn't Adequately Protect Undersea Cables—That Must Change*, ATL. COUNCIL (Apr. 17, 2024), https://www.atlanticcouncil.org/content-series/hybrid-warfare-project/international-law-doesnt-adequately-protect-undersea-cables-that-must-change/ [https://perma.cc/25QF-AUJ7].

15. *Germany and Finland Investigate a Severed Data Cable Through the Baltic Sea*, AP NEWS (Nov. 18, 2024), https://apnews.com/article/finland-germany-data-communications-cable-9b231aa47501545690a26a442fe106a5 [https://perma.cc/8VG8-RMTH].

16. *Sabotage Not Ruled Out in Break of Communications Cable in Baltic Sea*, EUR. CONSERVATIVE (Oct. 16, 2023), https://europeanconservative.com/articles/news/sabotage-not-ruled-out-in-break-of-communications-cable-in-baltic-sea/ [https://perma.cc/VH8R-BYQ4].

17. Sean Monaghan et al., *Red Sea Cable Damage Reveals Soft Underbelly of Global Economy*, CTR. FOR STRATEGIC & INT'L STUD. (Mar. 7, 2024), https://www.csis.org/analysis/red-sea-cable-damage-reveals-soft-underbelly-global-economy [https://perma.cc/43UH-HLUD].

18. Elisabeth Braw, *China May Be Rehearsing a Cable Cutoff of Taiwan*, FOREIGN POL'Y (Feb. 21, 2023), https://foreignpolicy.com/2023/02/21/matsu-islands-internet-cables-china-taiwan/ [https://perma.cc/FE8W-77KX].

the damage may have been caused by Chinese vessels, the lack of a clear liability and compensation framework complicated efforts to address the incident's financial impact.[19] In 2022, multiple cable cuts near Svalbard and the Shetland Islands raised suspicions of deliberate sabotage, though definitive evidence remains elusive.[20] The sabotage of the Nord Stream gas pipelines in September 2022 sent shockwaves through the international community, demonstrating the potential for catastrophic damage to critical undersea assets.[21]

The legal challenges in addressing these threats are multifaceted. First, the attribution of responsibility for damage to undersea assets remains problematic. As demonstrated by the Nord Stream incident, even after extensive investigations, conclusively identifying the perpetrators can be exceedingly difficult.[22] This ambiguity complicates the application of existing legal frameworks and the pursuit of remedies under international law.

Second, the current legal regime fails to adequately address the evolving nature of threats. While the 1884 Convention for the Protection of Submarine Telegraph Cables criminalizes willful or negligent damage to submarine cables, it does not account for modern cyber threats or sophisticated state-sponsored attacks.[23] UNCLOS provides some provisions for the protection of submarine cables, but its effectiveness in deterring and responding to contemporary threats is limited.[24]

Third, the intersection of national security interests and the global nature of undersea infrastructure creates jurisdictional complexities. The involvement of multiple states, private entities, and international waters in the operation and protection of these assets complicates the application of domestic laws and international treaties.[25]

International organizations have also recognized the urgency of the issue. The North Atlantic Treaty Organization ("NATO") established a new center in 2023 focused on securing undersea infrastructure.[26] The UN General

---

19. *See* Yachi Chiang, *A Legal Perspective on the Protection of Critical Infrastructure: The Case of Taiwan's Undersea Cables*, TAIWAN INSIGHT (Sept. 30, 2024), https://taiwaninsight.org/2024/09/30/a-legal-perspective-on-the-protection-of-critical-infrastructure-the [https://perma.cc/KMV3-FRKS].

20. *Damaged Cable Leaves Shetland Cut Off from Mainland*, BBC (Oct. 20, 2022, 12:00 AM), https://www.bbc.com/news/uk-scotland-north-east-orkney-shetland-63326102 [https://perma.cc/7EZ6-3XWJ].

21. *Incident on the Nord Stream Pipeline (updated 14/11/2022)*, NORD STREAM (Nov. 14, 2022), https://www.nord-stream.com/press-info/press-releases/incident-on-the-nord-stream-pipeline-updated-14112022-529/ [https://perma.cc/W2KS-LFTZ].

22. *Evidence Found In Nord Stream Sabotage Investigation*, K-LOVE (July 12, 2023), https://www.klove.com/news/U.S.%20&%20World/evidence-found-in-nord-stream-sabotage-investigation-44694 [https://perma.cc/HU86-3TJA].

23. *See* Convention for the Protection of Submarine Telegraph Cables, Mar. 14, 1884, 24 Stat. 989, T.S. No. 380.

24. *See* UNCLOS, *supra* note 1.

25. *See* Tara Davenport, *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*, 24 CATH. U. J. L. & TECH. 57, 89–92 (2015).

26. *NATO Officially Launches New Maritime Centre for Security of Critical Undersea Infrastructure*, NATO (May 28, 2024), https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui [https://perma.cc/8TD5-8B8D].

Assembly has passed resolutions emphasizing the critical nature of submarine cables as infrastructure.[27] However, these efforts have yet to translate into a cohesive and enforceable international legal framework.[28]

As technology advances and geopolitical tensions rise, the need for an updated international regime becomes increasingly apparent. Legal scholars argue for the development of a new multilateral treaty specifically addressing the protection of undersea infrastructure, including provisions for enhanced information sharing, coordinated response mechanisms, and clear attribution protocols.[29]

The emerging threats to undersea cables and pipelines underscore the urgent need for legal innovation in this domain. As these critical assets continue to form the backbone of global communication and energy systems, the international community must work towards a more robust and adaptive legal framework to ensure their protection and resilience in the face of evolving challenges.

III. LEGAL ANALYSIS

A. Jurisdictional Boundaries

The principle of flag state jurisdiction, as codified in UNCLOS Article 94, places primary responsibility for prosecution on the state of the perpetrator rather than the state of the cable or pipeline owner. This arrangement significantly impedes effective enforcement and accountability. The doctrine of universal jurisdiction, while applicable to certain international crimes, does not extend to offenses against undersea infrastructure, creating a lacuna in international criminal law.

The jurisdictional boundaries in protecting undersea cables and pipelines stem from the fundamental principles of maritime law and the unique nature of these critical infrastructures. The flag state jurisdiction principle, a cornerstone of maritime law, grants exclusive jurisdiction to the state whose flag a vessel flies over incidents occurring on the high seas. This principle, while essential for maintaining order in international waters, creates significant challenges in prosecuting offenses against undersea infrastructure.

UNCLOS Article 94 codifies this principle, stating that "every State shall effectively exercise its jurisdiction and control in administrative, technical and social matters over ships flying its flag."[30] While this provision ensures a clear chain of responsibility for vessels' conduct, it inadvertently creates a jurisdictional barrier for states whose undersea infrastructure is damaged or threatened by foreign vessels.

---

27. Eoin Micheál McNamara, *Reinforcing Resilience: NATO's Role in Enhanced Security for Critical Undersea Infrastructure*, NATO REVIEW (Aug. 28, 2024), https://www.nato.int/docu/review/articles/2024/08/28/reinforcing-resilience-natos-role-in-enhanced-security-for-critical-undersea-infrastructure/index.html [https://perma.cc/3357-5Z45].

28. BURNETT ET AL., *supra* note 2.

29. *See generally* G.A. Res. 73/124, ¶ 119, U.N. Doc. A/RES/73/124 (Dec. 11, 2018).

30. UNCLOS, *supra* note 1.

The boundaries of this arrangement become apparent in cases of intentional damage to undersea cables. For instance, in the 2022 incident where multiple cables near the Shetland Islands were damaged, raising suspicions of sabotage, the inability of the affected state to directly prosecute potential perpetrators highlighted the challenges within the current legal framework.[31] The reliance on flag states to prosecute their own vessels creates a potential conflict of interest, particularly in cases where the flag state might be complicit or indifferent to the offense.

Moreover, the doctrine of universal jurisdiction, which allows states to prosecute certain international crimes regardless of where they occurred or the nationality of the perpetrator, does not extend to offenses against undersea infrastructure.[32] This doctrine—typically reserved for crimes such as piracy, war crimes, and crimes against humanity—reveals a notable gap in the protection of critical global communication and energy infrastructure.

The absence of universal jurisdiction for these offenses is particularly problematic given the transnational nature of undersea cables and pipelines. As noted by legal scholars, the current framework fails to account for the global importance of these infrastructures and the potential for widespread disruption from localized damage.[33]

Recent developments have highlighted the need for reform. The Undersea Cable Control Act of 2023 attempts to address some of these issues by extending U.S. jurisdiction over certain activities related to undersea cables.[34] However, such unilateral actions, while potentially effective for a single state, do not resolve the broader international jurisdictional challenges.

International legal experts have proposed various solutions to address the jurisdictional boundaries. One approach suggests expanding the concept of universal jurisdiction to include serious offenses against critical global infrastructure.[35] Another proposal advocates for the development of a new multilateral treaty specifically addressing the protection of undersea cables and pipelines, including provisions for shared jurisdiction and enforcement mechanisms.[36]

The International Law Association's Committee on Submarine Cables and Pipelines is currently examining these issues, with the aim of clarifying and potentially reforming the international legal regime governing undersea

31. R.R. CHURCHILL & A.V. LOWE, THE LAW OF THE SEA 208 (3d ed. 1999).

32. UNCLOS, *supra* note 1.

33. *Shetland Communication Restored After Subsea Cable Damage,* BBC (Oct. 21, 2022), https://www.bbc.com/news/uk-scotland-north-east-orkney-shetland-63337473 [https://perma.cc/ATZ2-C94Z] (illustrating the potential for widespread disruption from localized damage to undersea cables).

34. *See* H.R. 1189, 118th Cong. (2023).

35. Davenport, *supra* note 25, at 84.

36. *See* Undersea Cable Control Act, H.R. 1189, 118th Cong. (2023).

infrastructure protection.[37] Their work may provide a foundation for future legal developments in this area.[38]

As geopolitical tensions rise and the vulnerability of undersea infrastructure becomes increasingly apparent, the need to address these jurisdictional boundaries grows more urgent. The current legal framework, rooted in 19th-century principles, struggles to cope with 21st-century threats to global communication and energy networks.[39] Reform of the international legal regime governing undersea cables and pipelines is essential to ensure their adequate protection and the stability of the global systems that rely on them.

B. Non-State Actors and Multinational Corporations

The traditional state-centric approach of international law fails to adequately address potential threats from non-state actors or large multinational corporations. The principle of state responsibility, as articulated in the International Law Commission's Articles on State Responsibility, [40] does not fully capture the complexities of attributing responsibility in cases involving these entities. The concept of "due diligence" in international law, as elucidated in the *Pulp Mills* case (ICJ 2010), could potentially be extended to create obligations for states to prevent non-state actors from damaging undersea infrastructure.[41]

The increasing prominence of non-state actors and multinational corporations in the global arena has exposed significant gaps in the international legal framework, particularly concerning the protection of critical infrastructure such as undersea cables and pipelines. The state-centric nature of international law, while foundational to the current system, faces difficulties in addressing the multifaceted realities of modern global interactions and potential threats.[42]

The principle of state responsibility, codified in the International Law Commission's Articles on State Responsibility, primarily focuses on attributing wrongful acts to states. Article 8 of the Articles states that the conduct of a person or group shall be considered an act of a state if the person

---

37. *Submarine Cables & Pipelines Under International Law*, INT'L LAW ASS'N (Dec. 14, 2020), https://discovery.ucl.ac.uk/id/eprint/10149627/3/Azaria_Interim%20Report%20of%20the%20ILA%20Committee%20on%20Submarine%20Cables%20and%20Pipelines%2015%20Sept%20final.pdf [https://perma.cc/W7TD-CAU8].

38. *See* Dr. Tara Davenport, *Third Interim Report of the ILA Committee on Submarine Cables and Pipelines*, 81ST BIENNIAL CONFERENCE INT'L L. ASS'N (June 28, 2024), https://cil.nus.edu.sg/wp-content/uploads/2024/07/ILA-Biennial-Submarine-Cables-and-Pipelines-Presentation-Athens-28-June-2024-final.pdf [https://perma.cc/3Q5W-EL2R].

39. *See* Elizabeth A. O'Connor, *Underwater Fiber Optic Cables: A Customary International Law Approach to Solving the Gaps in the International Legal Framework for Their Protection*, 66 NAVAL L. REV. 29, 30, 34-37 (2020).

40. *See* Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 43 (2001).

41. Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. 14 (Apr. 20).

42. James Green, *The ICJ's Flawed Approach to Non-State Actors and International Law*, 41 U. MELB. J. INT'L L. 43, 45 (2008).

or group is acting on the instructions of, or under the direction or control of, that state in carrying out the conduct.[43] However, this framework proves inadequate when addressing potential threats from non-state actors or multinational corporations operating with significant autonomy across national borders.

The concept of "due diligence" in international law, as elaborated in the *Pulp Mills case (Argentina v. Uruguay, 2010)*, offers a potential avenue for addressing these gaps.[44] By applying due diligence standards, states might be held accountable for failing to prevent such damage, thereby bridging the gap between state-centric international law and the realities of modern global interactions involving multiple actors. In this case, the International Court of Justice ("ICJ") held that states have an obligation to use all the means at their disposal to avoid activities which take place in their territory, or in any area under their jurisdiction, causing significant damage to the environment of another state. This principle could potentially be extended to create obligations for states to prevent non-state actors from damaging undersea infrastructure.

However, the application of due diligence to non-state actors and multinational corporations in the context of undersea infrastructure protection remains largely unexplored. The ICJ's approach in the *Pulp Mills* case, while groundbreaking in environmental law, does not directly address the unique challenges posed by these entities in the realm of critical infrastructure protection.[45]

Recent developments in international law have begun to grapple with these issues. The UN Guiding Principles on Business and Human Rights, adopted in 2011, represent a significant step towards recognizing the responsibilities of non-state actors.[46] While not legally binding, these principles establish a framework for addressing human rights impacts of business activities. A similar approach could be considered for critical infrastructure protection.

Moreover, the increasing recognition of the concept of "shared responsibility" in international law offers another potential avenue for addressing these challenges. This concept, as discussed by André Nollkaemper and Dov Jacobs, acknowledges that multiple actors may contribute to a single harmful outcome, necessitating a more nuanced approach to responsibility attribution.[47]

In the specific context of undersea infrastructure, the International Cable Protection Committee ("ICPC") has advocated for enhanced legal

43. Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 47 (2001).

44. André Nollkaemper & Dov Jacobs, *Shared Responsibility in International Law: A Conceptual Framework*, 34 MICH. J. INT'L L. 359, 401 (2013).

45. *See* Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. 14 (Apr. 20).

46. *See* John Ruggie, Special Representative of the Secretary-General, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011).

47. Nollkaemper & Jacobs, *supra* note 44, at 365-66.

protections.[48] Their recommendations, while not legally binding, emphasize the need for a more comprehensive approach to cable protection that includes measures to address threats from non-state actors.[49]

As geopolitical tensions rise and the vulnerability of undersea infrastructure becomes increasingly apparent, the need to address these legal gaps grows more urgent. The current framework, rooted in state-centric principles, struggles to cope with the complex realities of potential threats from non-state actors and multinational corporations. A reevaluation of international legal principles, potentially extending the concept of due diligence and incorporating elements of shared responsibility, is essential to ensure adequate protection of critical global communication and energy networks.

C. Environmental Concerns

The precautionary principle and the concept of "common concern of humankind" offer potential avenues for strengthening the international legal framework for protecting undersea cables and pipelines, which are currently inadequately addressed in UNCLOS. Applying these environmental law principles to critical submarine infrastructure could justify more robust protections given the global importance of these assets.

The precautionary principle, which advocates taking protective action before there is complete scientific proof of a risk, has gained prominence in international environmental law since the 1992 Rio Declaration.[50] While not explicitly applied to undersea cables in UNCLOS, the principle could inform a more proactive approach to safeguarding this infrastructure. As undersea cables transmit over ninety-five percent of international data,[51] disruptions could have severe global consequences, even if the full extent of potential damage remains uncertain. Applying the precautionary principle would support preventive measures and enhanced protections despite incomplete knowledge of specific threats.

Similarly, the doctrine of "common concern of humankind," which has evolved in environmental law to address issues of global importance transcending national boundaries,[52] could provide a conceptual basis for strengthening international cooperation on undersea cable protection. Given the critical role of submarine cables in global communications and the

48. Daniel Hernandez-Benito, *Damages to Submarine Cables and Pipelines in Times of Peace and War: The Nord Stream Sabotage*, 16 AMSTERDAM L.F. [3], [6] at n.21 (Summer 2024).

49. Rishi Sunak, *Undersea Cables: Indispensable, Insecure*, POL'Y EXCH. 19, 36 (Dec. 1, 2017).

50. *See* Jon M. Van Dyke, *The Evolution and International Acceptance of the Precautionary Principle*, *in* BRINGING NEW LAW TO OCEAN WATERS 357, 363 (David D. Caron & Harry N. Scheiber eds., 2004).

51. Pierre Morcos & Colin Wall, *Invisible and Vital: Undersea Cables and Transatlantic Security*, CSIS (Apr. 28, 2021), https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security [https://perma.cc/GX5G-WQGP].

52. Jutta Brunnée, *Common Areas, Common Heritage, and Common Concern*, OXFORD HANDBOOK OF INT'L ENV''L. 551, 553 (2007).

interconnected nature of the digital economy, their security could be framed as a common concern requiring collective action by the international community.

The potential application of environmental law principles to undersea cable protection finds some support in evolving interpretations of UNCLOS. In the South China Sea Arbitration, the tribunal recognized that the convention should be interpreted in light of developments in international law, including environmental principles.[53] This suggests that concepts like the precautionary principle could inform the interpretation and application of UNCLOS provisions related to submarine cables.

Incorporating these principles into the legal framework for undersea infrastructure protection could take several forms:

i. Complementing UNCLOS with a new treaty or adopting a new protocol specifically addressing undersea cable security, incorporating precautionary measures and recognizing cables as a common concern.
ii. Developing soft law instruments, such as UN General Assembly resolutions or guidelines, that apply these principles to submarine infrastructure protection.
iii. Encouraging national legislation and regional agreements that incorporate precautionary approaches and recognize the global importance of undersea cables.
iv. Establishing an international body or expanding the mandate of existing organizations (e.g., the International Cable Protection Committee) to coordinate global efforts on cable security.

While challenges remain in translating environmental law principles to the context of undersea infrastructure, doing so could provide a stronger legal foundation for addressing this critical issue of global concern. As the international community grapples with evolving threats to submarine cables and pipelines, drawing on established environmental law concepts offers a promising path forward for enhancing their protection under international law.

D. Energy Security

Disruptions to transoceanic pipelines can have profound implications for global energy markets and national energy security, underscoring the critical importance of protecting this vital infrastructure. The interconnected nature of the global energy system means that damage to key pipelines can lead to supply shocks, price volatility, and geopolitical tensions, with far-reaching consequences for both energy-exporting and energy-importing nations.

53. S. China Sea Arbitration Award (Phil. v. China), PCA Case Repository 2013-19 (2016).

The legal framework for protecting transoceanic pipelines remains limited, particularly in international waters. While UNCLOS provides some general provisions for the protection of submarine cables and pipelines, it lacks specific mechanisms for addressing modern threats to energy infrastructure. Article 113 of UNCLOS requires states to adopt laws criminalizing the breaking or injury of submarine cables or pipelines, but enforcement in international waters remains challenging.[54]

In response to these vulnerabilities, some nations have begun to take unilateral action. The U.S., for example, has introduced legislation aimed at enhancing the protection of critical energy infrastructure. The Safe and Secure Transportation of American Energy Act, introduced in the U.S. Senate in September 2024, seeks to expand criminal penalties for those who vandalize, tamper with, or disrupt the operation or construction of pipelines. While primarily focused on domestic infrastructure, this legislation reflects growing concern over energy security and the need for stronger legal protections.[55]

International efforts to address pipeline security have also gained momentum. The International Maritime Organization ("IMO") has initiated discussions on developing guidelines for the protection of submarine cables and pipelines. These efforts aim to establish best practices for safeguarding undersea infrastructure and improving coordination among states in responding to threats or incidents.[56]

The concept of energy security as a matter of "common concern" to the international community has gained traction in legal scholarship.[57] An approach drawing on principles from international environmental law could provide a basis for more robust international cooperation in protecting critical energy infrastructure.[58] Framing energy security as a common concern could justify collective action and the development of new legal instruments to address transnational threats to energy infrastructure.

Courts have also begun to grapple with the legal implications of pipeline disruptions. In the South China Sea Arbitration, the tribunal recognized the importance of protecting submarine communications cables, which could potentially be extended to energy pipelines.[59] The tribunal's emphasis on the duty of states to exercise due diligence in protecting marine environment could serve as a basis for developing more specific obligations regarding undersea energy infrastructure.

---

54. UNCLOS, *supra* note 1, art. 113.

55. *See Young, Commerce Republicans Introduce Bill to Protect American Energy*, TODD YOUNG U.S. SENATOR FOR IND. (Sept. 17, 2024), https://www.young.senate.gov/newsroom/press-releases/young-commerce-republicans-introduce-bill-to-protect-american-energy/ [https://perma.cc/DGG7-937A].

56. *See* INT'L L. ASS'N COMM. SUBMARINE CABLES & PIPELINES, SUBMARINE CABLES AND PIPELINES UNDER INT'L L. ¶ 5 (2024), https://www.ila-hq.org/en/documents/ilathi-1 [https://perma.cc/YYS8-K7KP].

57. *See* Lakshman Guruswamy, *Energy and the Environment: Confronting Common Threats to Security*, 16 N.C. J. INT'L L. 255 (1991).

58. *See* S. China Sea Arbitration Award (Phil. v. China), PCA Case Repository 2013-19 (2016).

59. *See* DANIEL YERGIN, THE NEW MAP: ENERGY, CLIMATE, AND THE CLASH OF NATIONS 24 (Penguin Press, 2020).

To address the challenges posed by potential disruptions to transoceanic pipelines, several steps should be considered:

i. Developing a new international agreement specifically focused on the protection of undersea energy infrastructure, building on the principles established in UNCLOS and other relevant treaties.
ii. Enhancing information sharing and coordination mechanisms among states to improve threat detection and response capabilities.
iii. Establishing clear protocols for investigating and attributing responsibility for attacks on undersea pipelines, potentially through the creation of an international body dedicated to this purpose.
iv. Incorporating energy infrastructure protection into broader maritime security initiatives and naval cooperation agreements.
v. Encouraging the development of redundant supply routes and diversification of energy sources to mitigate the impact of potential pipeline disruptions.

As the global energy landscape continues to evolve, protecting transoceanic pipelines will remain a critical component of ensuring energy security. The international community must work towards developing a more robust legal and operational framework to address this challenge, balancing the needs of energy-producing and consuming nations while safeguarding the stability of global energy markets.

IV. RECOMMENDATIONS

A. Enhance International Cooperation

The protection of undersea cables and pipelines requires enhanced international cooperation to address the growing threats to this critical infrastructure. Given the boundaries of existing legal frameworks, there is a compelling case for establishing a specialized UN body or expanding the mandate of the International Telecommunication Union ("ITU") to develop a comprehensive protection regime. Additionally, the creation of a multilateral treaty specifically addressing the protection of transoceanic pipelines could provide a more robust legal foundation for safeguarding these vital assets.

The International Tribunal for the Law of the Sea ("ITLOS") presents a natural and efficient solution as the primary enforcement mechanism for undersea cable protection under any new treaty framework. The tribunal's extensive experience in maritime disputes, combined with its established procedures for urgent proceedings under Article 290 of UNCLOS, positions it ideally to handle cases involving cable and pipeline interference.[60] ITLOS has already demonstrated its capability in handling complex infrastructure-

60. UNCLOS, *supra* note 1, art. 290.

related disputes through its provisional measures' cases and advisory opinions.[61]

The tribunal's existing framework could be expanded through specific provisions in the new treaty, granting it compulsory jurisdiction over cases involving undersea cable damage or interference. This approach would leverage ITLOS's maritime expertise while avoiding the substantial costs and delays associated with creating entirely new institutional mechanisms.[62] The tribunal's established rules of procedure could be supplemented with specific provisions for expedited proceedings in cable-related cases, recognizing the time-sensitive nature of infrastructure protection.

Furthermore, ITLOS's experience in balancing competing maritime interests makes it particularly well-suited to handle the complex interplay between cable protection, freedom of navigation, and environmental considerations.[63] The tribunal could develop specialized chambers for cable and pipeline cases, similar to its existing chamber for fisheries disputes, ensuring that cases are heard by judges with relevant technical expertise. This specialized jurisdiction would promote consistent interpretation of the new legal framework while building on ITLOS's established legitimacy in the international maritime community.[64]

1. Establishing a Specialized UN Body or Expanding ITU Mandate

The establishment of a dedicated UN entity or the expansion of the ITU's mandate to focus on undersea infrastructure protection would provide a centralized mechanism for addressing this critical issue. Such an initiative could:

i. Develop comprehensive guidelines and best practices for the protection of undersea cables and pipelines, drawing on expertise from various sectors including telecommunications, energy, and maritime security.
ii. Facilitate information sharing and coordination among states, industry stakeholders, and international organizations to improve threat detection and response capabilities.
iii. Provide a forum for addressing jurisdictional challenges and developing protocols for investigating and attributing responsibility for attacks on undersea infrastructure.

---

61. *See* Press Release, Int'l Tribunal L. Sea, Today, 6 July 2019, the Tribunal Delivered Its Order in the M/T "San Padre Pio" Case (Switzerland v. Nigeria), Provisional Measures (July 6, 2019) (on file with author).

62. *See* Seline Trevisanut, *Twenty Years of Prompt Release of Vessels: Admissibility, Jurisdiction, and Recent Trends*, 48 OCEAN DEV. & INT'L L. 300, 301-302 (2017).

63. *See* James Harrison, *Safeguards Against Excessive Enforcement Measures in the Exclusive Economic Zone – Law and Practice*, *in* JURISDICTION OVER SHIPS: POST-UNCLOS DEVELOPMENTS IN THE LAW OF THE SEA 217, 229-30 (Henrik Ringbom ed., 2015).

64. *See* Helmut Tuerk, *The Contribution of the International Tribunal for the Law of the Sea to International Law*, 26 PENN ST. INT'L L. REV. 289, 290-291 (2007).

iv. Coordinate research and development efforts to enhance the resilience and security of undersea cables and pipelines.

UNCLOS currently does not have specific mechanisms for addressing modern threats. The recent Joint Statement on the security and resilience of undersea cables, welcomed by the European Commission in September 2024, demonstrates this concept.[65]

2. Creating a Multilateral Treaty for Transoceanic Pipeline Protection

The development of a multilateral treaty specifically addressing the protection of transoceanic pipelines, drawing inspiration from the International Convention for the Prevention of Pollution from Ships ("MARPOL"), could provide a comprehensive legal framework for addressing the unique challenges posed by this critical infrastructure.[66] Key elements of such a treaty could include:

i. Clear definitions of prohibited acts against pipelines, including sabotage, unauthorized tapping, and negligent damage.
ii. Establishment of an international inspection regime to ensure compliance with security standards.
iii. Creation of a liability and compensation framework for damage to pipelines, similar to the Civil Liability Convention for oil pollution damage.
iv. Provisions for capacity building and technical assistance to help developing states implement protective measures.
v. Mechanisms for dispute resolution and enforcement of treaty obligations.

3. Legal Considerations and Challenges

The development of new international instruments for undersea infrastructure protection must navigate complex legal and jurisdictional issues.[67] Any new treaty or institutional framework must be carefully crafted to complement and enhance existing legal regimes, rather than conflict with them.

Recent jurisprudence, such as the South China Sea Arbitration, has recognized the importance of protecting submarine communications cables,

65. *New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World*, EUR. COMM'N (Sept. 26, 2024), https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-joint-statement-security-and-resilience-undersea-cables-un-general-assembly-new [https://perma.cc/M6MY-C2UB].

66. *See* INT'L L. ASS'N COMM. SUBMARINE CABLES & PIPELINES, INTERIM REPORT 2020 (2021), https://discovery.ucl.ac.uk/10149627/3/Azaria_Interim%20Report%20of%20the%20ILA%20Committee%20on%20Submarine%20Cables%20and%20Pipelines%2015%20Sept%20final.pdf [https://perma.cc/M6MY-C2UB].

67. UNCLOS, *supra* note 1.

which could potentially be extended to energy pipelines.[68] This evolving legal landscape provides an opportunity to develop more robust protections for undersea infrastructure within the existing framework of international law.

V. IMPLEMENTATION AND ENFORCEMENT

A. Requirements for Implementation

Effective implementation and enforcement of any new protection regime will require:

i. Development of clear protocols for investigating and attributing responsibility for attacks on undersea infrastructure.
ii. Establishment of an international body to oversee compliance and facilitate dispute resolution.
iii. Integration of undersea infrastructure protection into broader maritime security initiatives and naval cooperation agreements.
iv. Encouragement of domestic legislation to implement treaty obligations and criminalize attacks on undersea infrastructure.

The recent establishment of NATO's Critical Undersea Infrastructure Coordination Cell in February 2023 demonstrates growing recognition of the need for coordinated military responses to threats against undersea infrastructure.[69] Any new international regime should seek to complement and enhance such existing security arrangements.

In conclusion, enhancing international cooperation through the establishment of a specialized UN body or expanded ITU mandate, coupled with the development of a comprehensive multilateral treaty for transoceanic pipeline protection, offers a promising path forward for addressing the critical challenge of safeguarding undersea infrastructure. As the global community becomes increasingly reliant on these vital communication and energy networks, the development of robust legal and institutional frameworks for their protection is not merely desirable, but essential for ensuring international security and economic stability.

B. Expand Jurisdiction

The protection of undersea cables and pipelines requires a robust legal framework that can effectively address the transnational nature of threats to this critical infrastructure. Expanding jurisdiction through amendments to UNCLOS and potentially including serious damage to undersea infrastructure as a crime under the Rome Statute of the International Criminal Court ("ICC")

68. *See* S. China Sea Arbitration Award (Phil. v. China), PCA Case Repository 2013-19 (2016).

69. *See NATO Stands Up Undersea Infrastructure Coordination Cell*, NATO (Feb. 15, 2023), https://www.nato.int/cps/en/natohq/news_211919.htm [https://perma.cc/6NJL-4L8G].

could significantly enhance the international community's ability to deter and prosecute such offenses.

1. Complementing UNCLOS to Establish "Effects Jurisdiction"

The concept of "effects jurisdiction" would allow states affected by damage to undersea cables or pipelines to pursue legal action against perpetrators, regardless of their nationality or the location of the offense. This approach draws inspiration from the "effects doctrine" in antitrust law, which has been used to assert jurisdiction over foreign conduct that has substantial effects within a state's territory.[70] To expand jurisdiction, we propose developing a new protocol or agreement that would complement UNCLOS without directly amending it. This approach could include:

i. A new article explicitly establishing effects jurisdiction for offenses against undersea cables and pipelines.
ii. Provisions detailing the criteria for determining when a state is sufficiently "affected" to assert jurisdiction.
iii. Mechanisms for resolving potential jurisdictional conflicts among affected states.

The lack of clear jurisdictional authority in such cases highlights the boundaries of the current legal framework.

Implementing effects jurisdiction would require careful consideration of potential conflicts with existing principles of international law, particularly the respect for state sovereignty. However, precedent for extraterritorial jurisdiction in cases of transnational crime exists in various international instruments, such as the UN Convention against Transnational Organized Crime.[71]

2. Including Serious Damage to Undersea Infrastructure In the Rome Statute

Proposing the inclusion of serious damage to undersea infrastructure as a crime under the Rome Statute of the ICC would elevate the significance of such offenses in international law. This approach could:

i. Provide a mechanism for prosecution when national courts are unwilling or unable to act.
ii. Deter potential offenders through the threat of international criminal liability.

---

70. *See* James Harrison, *The Effects Doctrine in International Law: A Historical Perspective*, 45 HARV. INT'L L. J. 127, 135-38 (2012).
71. *See* G.A. Res. 55/25 (Sept. 29, 2003).

iii. Ensure a consistent approach to investigating and prosecuting these crimes across jurisdictions.

The principle of complementarity, a cornerstone of the ICC's jurisdiction, would ensure that national courts retain primary responsibility for prosecuting these offenses, with the ICC serving as a court of last resort.[72] This approach respects state sovereignty while providing a backstop for cases where national prosecution is not feasible or effective.

Including this offense in the Rome Statute would require demonstrating that it meets the threshold of "the most serious crimes of concern to the international community as a whole." Given the critical importance of undersea infrastructure to global communications and energy security, a strong case can be made for its inclusion.

Recent jurisprudence from the ICC, such as the 2021 decision confirming charges in the Abd-Al-Rahman case, demonstrates the Court's willingness to interpret its mandate broadly to address evolving threats to international peace and security.[73] This precedent could support arguments for expanding the Court's jurisdiction to cover serious attacks on undersea infrastructure.

3. Legal and Practical Considerations

Implementing these proposals would face several challenges:

i. Complementing UNCLOS and the Rome Statute requires broad international consensus, which may be difficult to achieve given divergent national interests.
ii. Defining "serious damage" to undersea infrastructure in a way that is both comprehensive and specific enough for criminal prosecution.
iii. Addressing potential conflicts with existing national laws and jurisdictional claims.
iv. Ensuring that expanded jurisdiction does not infringe on legitimate military activities or scientific research.

To address these challenges, a phased approach could be considered.

First, pursue amendments to UNCLOS to establish effects jurisdiction, as this may face less resistance than expanding the ICC's mandate.

Simultaneously, work towards building consensus for including serious damage to undersea infrastructure in the Rome Statute, potentially through a UN General Assembly resolution recognizing the gravity of such offenses.

---

72. *See* Rome Statute of the International Criminal Court, *opened for signature* July 17, 1998, 2187 U.N.T.S. 90 (entered into force July 1, 2002).

73. *See* Prosecutor v. Abd-Al-Rahman, ICC-02/05-01/20, Decision on the Confirmation of Charges (July 9, 2021).

Develop model legislation for states to implement expanded jurisdiction domestically, ensuring consistency with international law principles.

4. Enforcement and Implementation

Effective enforcement of expanded jurisdiction would require:

i. Enhanced international cooperation in investigations and evidence gathering.
ii. Development of specialized expertise within national law enforcement agencies and the ICC to handle complex cases involving undersea infrastructure.
iii. Establishment of clear protocols for information sharing and mutual legal assistance in these cases.

The recent establishment of NATO's Critical Undersea Infrastructure Coordination Cell in February 2023 demonstrates growing recognition of the need for coordinated responses to threats against undersea infrastructure.[74] Any expansion of legal jurisdiction should be complemented by such operational initiatives to ensure effective enforcement.

In conclusion, expanding jurisdiction through a new treaty to complement UNCLOS and potentially including serious damage to undersea infrastructure in the Rome Statute offers a promising approach to enhancing the protection of this critical global resource.[75] While significant challenges remain in implementing these proposals, the growing threats to undersea cables and pipelines necessitate bold legal innovations to ensure their security in the 21st century.

C. Strengthen Deterrence and Environmental Protections

The protection of undersea cables and pipelines requires a multifaceted approach that strengthens deterrence against intentional damage and enhances environmental safeguards. Developing a protocol to UNCLOS establishing an international liability and compensation fund could address accountability gaps for transnational harm. Coupled with this, the adoption of an "Undersea Infrastructure Impact Assessment" ("UIIA") requirement, inspired by Environmental Impact Assessments ("EIAs") under international law, could further bolster the legal frameworks.[76]

74. *See NATO Stands Up Undersea Infrastructure Coordination Cell*, NATO (Feb. 15, 2023), https://www.nato.int/cps/en/natohq/news_211919.htm [https://perma.cc/6NJL-4L8G].
75. *See* BURNETT ET AL., *supra* note 2, at 155-58.
76. *See* Harrison, *supra* note 70 (discussing EIAs as general principles of law).

1. International Liability and Compensation Fund

The establishment of an international liability and compensation fund for damage to undersea cables and pipelines, modeled after the International Oil Pollution Compensation Funds ("IOPC Funds"), would provide a robust mechanism for addressing the financial consequences of infrastructure damage and serve as a deterrent against intentional acts of sabotage.

The IOPC Funds, established under the auspices of the International Maritime Organization ("IMO"), provide compensation for oil pollution damage resulting from spills of persistent oil from tankers.[77] This model could be adapted to address damage to undersea infrastructure, with key features including:

i. Strict liability for damage to cables and pipelines, regardless of fault.
ii. Compulsory insurance requirements for vessels operating in areas with undersea infrastructure.
iii. A tiered system of compensation, with primary responsibility falling on the vessel owner and supplementary compensation provided by the fund.
iv. Contributions to the fund from states party to the protocol, based on the volume of data or resources transmitted through cables and pipelines under their jurisdiction.

Recent incidents and current international tensions underscore the need for such a mechanism. Implementing this fund would require careful consideration of several legal issues:

i. Defining the scope of compensable damage, including both direct physical damage and consequential losses from service disruptions.
ii. Establishing procedures for claims assessment and dispute resolution.
iii. Addressing potential conflicts with existing liability regimes under national laws.
iv. Ensuring compatibility with the principle of freedom of navigation on the high seas.

2. Undersea Infrastructure Impact Assessment

The adoption of an "Undersea Infrastructure Impact Assessment" ("UIIA") requirement for activities that may affect cables or pipelines would provide a proactive mechanism for identifying and mitigating potential risks to this critical infrastructure. This requirement could draw on the principles established in the Convention on Environmental Impact Assessment in a Transboundary Context ("Espoo Convention"), adapting them to the specific

77. *Funds Overview*, INT'L OIL POLLUTION COMP. FUNDS, https://iopcfunds.org/about-us/ [https://perma.cc/BR46-394W] (last visited Apr. 4, 2025).

context of undersea infrastructure.[78] Key elements of the UIIA requirement could include:

i. Mandatory assessment of potential impacts on undersea cables and pipelines for activities such as seabed mining, offshore energy development, and marine scientific research.
ii. Transboundary notification and consultation procedures for activities that may affect infrastructure in areas beyond national jurisdiction.
iii. Public participation in the assessment process, recognizing the global importance of undersea communication networks.
iv. Provisions for post-project analysis and monitoring to ensure ongoing protection of infrastructure.

The need for such assessments is highlighted by the growing interest in seabed mining and other activities that could pose risks to undersea cables. For example, the International Seabed Authority is currently developing regulations for deep-sea mining, which could potentially impact existing and future cable routes.[79] However, implementing the UIIA requirement would face several challenges:

i. Defining the threshold for activities requiring assessment, balancing protection with the need to avoid undue burdens on maritime activities.
ii. Establishing mechanisms for information sharing that protect sensitive data about cable and pipeline locations.
iii. Addressing potential conflicts with the principle of freedom of scientific research under UNCLOS.
iv. Ensuring effective enforcement in areas beyond national jurisdiction.

3. Legal and Practical Considerations

Implementing these proposals would require careful navigation of existing international legal frameworks and potential conflicts with national interests. The development of a protocol to UNCLOS would need to address concerns about the convention's integrity and the potential for fragmentation of the law of the sea regime.

Recent jurisprudence, such as the South China Sea Arbitration, has recognized the importance of protecting submarine communications cables, which could provide a basis for expanding legal protections to include liability and impact assessment requirements.[80] However, the tribunal's

78. *See* Convention on Environmental Impact Assessment in a Transboundary Context app. I, *opened for signature* Feb. 25, 1991, 1989 U.N.T.S. 309, 340-41 (entered into force Sept. 10, 1997).

79. INTERNATIONAL SEABED AUTHORITY, DRAFT REGULATIONS ON EXPLOITATION OF MINERAL RESOURCES IN THE AREA pt. V ¶¶ 12-14, (2019).

80. *See* S. China Sea Arbitration Award (Phil. v. China), PCA Case Repository 2013-19 (2016).

emphasis on the duty of states to exercise due diligence in protecting the marine environment would need to be balanced against concerns about overly burdensome regulations.

In conclusion, the development of an international liability and compensation fund, coupled with the adoption of an UIIA requirement, offers a promising approach to strengthening deterrence and environmental protections for undersea cables and pipelines. While significant challenges remain in implementing these proposals, the growing threats to this critical infrastructure underscore the urgent need for enhanced legal frameworks to ensure its protection and resilience.

D. Improve Monitoring and Security

The protection of undersea infrastructure requires enhanced monitoring and security measures to address the growing threats to these critical assets. Establishing an International Undersea Infrastructure Monitoring Organization ("IUIMO") and developing a legal framework for the deployment of autonomous underwater vehicles ("AUVs") for infrastructure monitoring are two promising approaches to improve the security of undersea cables and pipelines.

1. Establishing an International Undersea Infrastructure Monitoring Organization

The creation of an IUIMO, vested with the authority to conduct inspections and share intelligence among member states, could significantly enhance the international community's ability to protect undersea infrastructure. This organization could be modeled on existing international bodies such as the International Atomic Energy Agency ("IAEA"), adapting its inspection and information-sharing mechanisms to the maritime domain. Key features of the IUIMO could include:

i. A mandate to conduct regular inspections of undersea infrastructure in international waters and, with coastal state consent, in territorial seas and exclusive economic zones.
ii. Authority to collect and analyze data on potential threats to undersea infrastructure.
iii. A mechanism for sharing intelligence and best practices among member states.
iv. The power to issue recommendations for enhancing the security of undersea infrastructure.

The need for such an organization is underscored by recent incidents, such as the January 2024 damage to multiple undersea cables connecting Taiwan, which disrupted internet connectivity and raised suspicions of

intentional sabotage.[81] An IUIMO could help prevent such incidents by improving threat detection and response capabilities. Implementing this proposal would require careful consideration of several legal issues:

i. The scope of the organization's authority in different maritime zones, particularly in light of coastal state sovereignty concerns.
ii. Procedures for ensuring the confidentiality of sensitive information while promoting effective information sharing.
iii. Mechanisms for resolving disputes between the organization and member states or between member states.

The establishment of the IUIMO could draw inspiration from recent developments in international maritime security cooperation. For example, NATO's establishment of the Maritime Centre for the Security of Critical Undersea Infrastructure in May 2024 demonstrates growing recognition of the need for coordinated action in this area.[82] The IUIMO could build on this momentum, expanding the scope of cooperation beyond NATO member states to create a truly global monitoring and security regime.

2. Legal Framework for AUV Deployment

Developing a legal framework for the deployment of AUVs for infrastructure monitoring is essential to harness the potential of these technologies while addressing potential conflicts with the freedom of navigation. AUVs offer significant advantages for undersea infrastructure monitoring, including the ability to operate for extended periods in harsh environments and access areas that are difficult or dangerous for human divers.[83] Key elements of this legal framework could include:

i. Clear definitions of the types of AUVs covered and their permissible uses for infrastructure monitoring.
ii. Rules governing the operation of AUVs in different maritime zones, including provisions for coastal state consent where necessary.
iii. Mechanisms for ensuring that AUV operations do not interfere with legitimate maritime activities or infringe on the rights of other states.
iv. Provisions for the collection, use, and sharing of data gathered by AUVs during monitoring operations.

---

81. Joyu Wang, *Chinese Vessel Cuts Taiwan Internet Cable in Apparent Sabotage*, WALL ST. J. (Jan. 6, 2025), https://www.wsj.com/world/asia/chinese-vessel-cuts-taiwan-internet-cable-in-apparent-sabotage-81e0d3b1 [https://perma.cc/62YV-A4YD].

82. *See NATO Officially Launches New Maritime Centre for Security of Critical Undersea Infrastructure*, NATO (May 28, 2024), https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui [https://perma.cc/8TD5-8B8D].

83. *What is an AUV?*, NOAA OCEAN EXPL., https://oceanexplorer.noaa.gov/facts/auv.html [https://perma.cc/DW3G-Q9MT] (last visited Apr. 4, 2025).

Recent jurisprudence, such as the South China Sea Arbitration, has recognized the importance of protecting submarine communications cables, which could provide a basis for expanding legal protections to include AUV-based monitoring activities.[84] However, the tribunal's emphasis on the duty of states to exercise due diligence in protecting the marine environment would need to be balanced against concerns about potential interference with navigation rights. Therefore, implementing this legal framework would face several challenges:

i. Defining the threshold for activities requiring coastal state consent, balancing the need for effective monitoring with respect for coastal state sovereignty.
ii. Addressing potential conflicts between AUV operations and other maritime activities, such as fishing or scientific research.
iii. Ensuring that AUV deployment does not become a cover for unauthorized intelligence gathering or other activities that could threaten international security.

The development of this legal framework could build on existing initiatives, such as the IMO's ongoing work on Maritime Autonomous Surface Ships ("MASS").[85] While focused on surface vessels, the MASS regulatory scoping exercise provides valuable insights into the challenges of integrating autonomous systems into the existing maritime legal regime.

In conclusion, establishing an IUIMO and developing a legal framework for AUV deployment offer promising approaches to improving the monitoring and security of undersea infrastructure. While significant challenges remain in implementing these proposals, the growing threats to undersea cables and pipelines underscore the urgent need for enhanced international cooperation and legal innovation in this critical area.

E. Update Regulatory Frameworks

The protection of undersea cables and pipelines requires a comprehensive update to existing regulatory frameworks at both the international and national levels. Proposing amendments to the International Telecommunication Regulations ("ITRs") and advocating for a UN General Assembly resolution on harmonizing national laws could significantly enhance the legal protections for this critical infrastructure.

84. *See* S. China Sea Arbitration Award (Phil. v. China), PCA Case Repository 2013-19 (2016).

85. *Autonomous Shipping*, INT'L MARITIME ORG., https://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx [https://perma.cc/TF2M-4E5N] (last visited Apr. 4, 2025).

1. Amending the International Telecommunication Regulations

The ITRs, last revised in 2012, provide a global framework for international telecommunications. However, these regulations do not adequately address the security challenges facing undersea cables in the modern era.[86] Proposed amendments to the ITRs could include:

i. Specific provisions on the physical and cybersecurity of undersea cables, including requirements for risk assessments and security measures.
ii. Obligations for states to cooperate in protecting undersea infrastructure, including information sharing and joint response mechanisms.
iii. Guidelines for the resilience and redundancy of cable networks to ensure continuity of global communications.
iv. Provisions addressing emerging technologies, such as quantum communications, that may impact undersea cable security.

The need for such amendments is underscored by recent incidents and initiatives. For instance, the Joint Statement on the security and resilience of undersea cables, welcomed by the European Commission in September 2024, demonstrates growing international recognition of the need for coordinated action in this area. The statement, proposed by the U.S., lays out principles to ensure undersea cable infrastructure is "secure, reliable, sustainable and resilient."[87] Incorporating these principles into the ITRs would provide them with greater legal weight and global applicability. However, implementing these amendments would face several challenges:

i. Balancing security requirements with the principle of free flow of information, as enshrined in existing international telecommunications law.
ii. Addressing potential conflicts with national sovereignty, particularly regarding security measures in territorial waters.
iii. Ensuring that new regulations do not unduly burden developing countries or impede their access to global telecommunications networks.

86. *See Final Acts of the World Conference on International Communications*, INT'L TELECOMM. UNION (2012), https://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf [https://perma.cc/6JTT-K9M3].

87. *Commission Welcomes Joint Statement on the Security and Resilience of Undersea Cables at UN General Assembly in New York*, EUR. COMM'N (Sept. 26, 2024), https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-joint-statement-security-and-resilience-undersea-cables-un-general-assembly-new [https://perma.cc/M6MY-C2UB].

2. UN General Assembly Resolution on Harmonization of National Laws

Advocating for the adoption of a UN General Assembly resolution calling for the harmonization of national laws regarding the protection of undersea infrastructure could provide a crucial impetus for strengthening legal protections globally. Such a resolution could:

i. Call on member states to review and update their national laws to address modern threats to undersea infrastructure.
ii. Provide guidelines for key elements to be included in national legislation, such as criminal penalties for intentional damage to cables and pipelines.
iii. Encourage the establishment of national focal points for undersea infrastructure protection and international cooperation.
iv. Promote the development of regional cooperation mechanisms for infrastructure protection.

The need for harmonized national laws is evident in the disparate approaches currently taken by different states. For example, while some countries have recently updated their legislation to address undersea cable security, others lack specific legal provisions on this issue. A UN resolution could help bridge these gaps and create a more consistent global legal framework.[88]

Recent developments underscore the timeliness of such an initiative. NATO's establishment of the Maritime Centre for the Security of Critical Undersea Infrastructure in May 2024 demonstrates growing recognition of the need for coordinated action in this area.[89] A UN resolution could build on this momentum, expanding the scope of cooperation beyond NATO member states to create a truly global approach to undersea infrastructure protection. Implementing this proposal would require addressing several legal and practical considerations:

i. Respecting the diversity of legal systems and traditions among UN member states while promoting harmonization.
ii. Balancing the need for robust protection measures with concerns about potential infringements on maritime freedoms.
iii. Addressing the challenges of enforcement in areas beyond national jurisdiction.

In conclusion, updating regulatory frameworks through amendments to the ITRs and a UN General Assembly resolution on harmonizing national

88. Tara Davenport, *Submarine Communications Cables and Law of the Sea: Problems in Law and Practice*, 43 OCEAN DEV. & INT'L LAW 201, 201 (2012).

89. *See NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure*, NATO (May 28, 2024), https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui [https://perma.cc/8TD5-8B8D].

laws offers a promising approach to enhancing the protection of undersea cables and pipelines. While significant challenges remain in implementing these proposals, the growing threats to this critical infrastructure underscore the urgent need for a comprehensive and coordinated global legal response.

VI. CONCLUSION

The proposed recommendations for enhancing the protection of undersea cables and transoceanic pipelines represent a comprehensive approach to addressing the significant gaps in the current international legal framework. These measures aim to leverage established principles of international law while introducing innovative legal mechanisms to bolster the security and resilience of critical global infrastructure in an era marked by increasing geopolitical tensions and technological vulnerabilities.

The urgency of these reforms is underscored by recent incidents that highlight the vulnerability of undersea infrastructure. The January 2024 damage to multiple undersea cables connecting Taiwan, which disrupted internet connectivity and raised suspicions of intentional sabotage, serves as a stark reminder of the potential consequences of inadequate protection. Similarly, the 2022 explosions that damaged the Nord Stream pipelines in the Baltic Sea demonstrated the vulnerability of transoceanic energy infrastructure and the geopolitical ramifications of such incidents.

The proposed establishment of an International Undersea Infrastructure Monitoring Organization ("IUIMO") and the development of a legal framework for autonomous underwater vehicle ("AUV") deployment address the critical need for enhanced monitoring and security measures. These initiatives build upon existing international cooperation frameworks, such as NATO's Maritime Centre for the Security of Critical Undersea Infrastructure, launched in May 2024, while expanding their scope to create truly global mechanisms for infrastructure protection.

The recommendation to amend the International Telecommunication Regulations (ITRs) to include specific provisions on undersea cable security aligns with growing international recognition of the need for coordinated action in this area.

The proposed development of an international liability and compensation fund for damage to undersea cables and pipelines, modeled on the International Oil Pollution Compensation Funds, addresses a critical gap in the current legal framework. This mechanism would not only provide a means for addressing the financial consequences of infrastructure damage but also serve as a deterrent against intentional acts of sabotage.

The advocacy for a UN General Assembly resolution calling for the harmonization of national laws regarding undersea infrastructure protection recognizes the importance of creating a consistent global legal framework. This approach builds on the principle of common concern for the protection of critical global resources, as articulated in various international environmental instruments and increasingly recognized in the context of cybersecurity and critical infrastructure protection.

The proposed expansion of jurisdiction through a new treaty complementing UNCLOS and the potential inclusion of serious damage to undersea infrastructure as a crime under the Rome Statute of the International Criminal Court represent bold steps towards addressing the transnational nature of threats to this infrastructure. These measures draw inspiration from evolving concepts of universal jurisdiction and the recognition of certain crimes as being of concern to the international community.

While these recommendations face significant challenges in implementation, including potential conflicts with established principles of maritime law and concerns about national sovereignty, they offer a path forward for addressing the critical vulnerabilities in the current legal framework. As the International Law Commission noted in its 2023 report on sea-level rise in relation to international law, the law of the sea must evolve to address emerging challenges that were not contemplated when UNCLOS was drafted.

In conclusion, the proposed recommendations represent a comprehensive and forward-looking approach to enhancing the protection of undersea cables and transoceanic pipelines. By combining established legal principles with innovative mechanisms, these measures seek to create a robust international legal framework capable of addressing the complex challenges posed by threats to critical global infrastructure in the 21st century. As the international community continues to grapple with these issues, the implementation of these recommendations could play a crucial role in ensuring the security and resilience of the global communications and energy networks that underpin modern society.

Vox Populi In Camera: Reforming the Foreign Intelligence Surveillance Act to Preserve Civil Liberties Through Adversarial Proceedings

Arjun Singh*

TABLE OF CONTENTS

* Arjun Singh is a third-year Juris Doctor candidate at The George Washington University Law School. He is an Associate of the Federal Communications Law Journal as well as a member of the Moot Court Board and the GW Law Federalist Society. He holds a Bachelor of Arts with Honors from the University of Toronto, from which he graduated with High Distinction in 2021, specializing in political science and international relations. He is a part-time law student and works as a political journalist reporting on the U.S. Congress and national politics. His email address is arjun.singh@law.gwu.edu.

I. INTRODUCTION

Nowadays, there are few things in American politics upon which progressives and conservatives agree. An even fewer number of subjects unite them against the federal bureaucracy. One such controversy, at present, concerns the Foreign Intelligence Surveillance Act ("FISA"). This Act has made strange bedfellows—bringing together members of the House Freedom Caucus and the American Civil Liberties Union, on one side, against the U.S. intelligence community, on the other.[1] As of writing, Congress is embroiled in a controversy over reauthorizing a key provision of the law, with reports indicating a lack of consensus to do so.[2]

The concern with FISA is regarding its apparent erosion of civil liberties. In 1978, Congress enacted FISA to provide the first statutory framework for gathering foreign intelligence inside and outside the United States.[3] Ordinarily, under Supreme Court precedent in *Katz v. United States*, the Fourth Amendment restrains the government from surveillance where a person has a reasonable expectation of privacy, except on issuance of a warrant by a federal court, based on probable cause.[4] *Katz*, however, noted an exception for cases involving national security, where normal proceedings are not always feasible.[5] The evidence of probable cause may be highly classified, and the facts may necessitate secrecy of proceedings to protect the sources and methods of surveillance.[6] FISA remedied this problem by creating a new court—the U.S. Foreign Intelligence Surveillance Court ("FISC")—which hears applications for such warrants, *in camera* and *ex parte* (i.e., a classified proceeding involving only the government pleading before the judge), and where the government may, under special procedures, request warrants for

1. *Warrantless Surveillance Under Section 702 of FISA*, ACLU (Sept. 28, 2023, 9:43 PM), https://www.aclu.org/issues/national-security/warrantless-surveillance-under-section-702-fisa [https://perma.cc/L7UM-X65E]; *Chairs of Progressive and Freedom Caucus Agree – The FBI Is Out of Control*, PROJECT FOR PRIV. AND SURVEILLANCE ACCOUNTABILITY (Feb. 16, 2023), https://www.protectprivacynow.org/news/chairs-of-progressive-and-freedom-caucus-agree-the-fbi-is-out-of-control [https://perma.cc/D7BR-SAET].

2. Arjun Singh, *Here's The Unfinished Work Congress Is Leaving Behind As It Breaks For Thanksgiving*, THE DAILY CALLER (Nov. 16, 2023, 8:24 PM), https://dailycaller.com/2023/11/16/unfinished-work-congress-thanksgiving/ [https://perma.cc/C27T-9GJC].

3. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801-85(c)).

4. Katz v. United States, 389 U.S. 347, 358-59 (1967).

5. *Id.* at 358.

6. *Foreign Intelligence Surveillance Court (FISC)*, ELEC. PRIV. INFO. CTR. (Nov. 25, 2021, 10:17 AM), https://epic.org/foreign-intelligence-surveillance-court-fisc/ [https://perma.cc/P4E8-R7SM].

surveillance.[7] The arrangements under FISA, purportedly, balance national security with constitutional rights.[8]

Crucially, FISA applies to "foreign" intelligence. It limits the government to conducting surveillance of individuals and entities who are agents of a foreign power, terrorists, or saboteurs.[9] "U.S. persons"—or U.S. citizens, lawful permanent residents, associations of such persons, and companies incorporated in the United States and their data—as well as collections primarily taking place inside the United States are subject to strict "minimization" procedures to prevent U.S. persons' data from being collected and, if inadvertently collected, to prevent it from being used against them.[10] The size, scope, and permanence of the federal government's electronic surveillance programs, which collect massive amounts of data, invariably mean that some U.S. persons' data will be collected.[11] This makes both the minimization procedures under the FISA and the FISC's judicial oversight critical to protecting U.S. persons from unauthorized surveillance.[12]

Therein lies the basis for controversy. Critics have attacked FISA, specifically its Section 702, for its purported use to target U.S. persons using information gathered through FISA warrants. Progressive opponents, such as the Brennan Center for Justice, have claimed that FISA has been "routinely abused . . . to gain warrantless access to the communications of tens of thousands of protesters, racial justice activists, 19,000 donors to a congressional campaign, journalists, and members of the U.S. Congress."[13] Conservative opponents claim that FISA has been used to target conservative politicians, specifically Donald Trump during the 2016 presidential election.[14] Whether such information, once gathered, has been abused by the federal government to thwart the efforts of these groups is unclear, though the very existence of a constitutional rights violation against these groups is enough to merit aggrievement and injury.[15] Moreover, that these organizations may be

---

7. FISA Ct. Rev. 7(j).

8. *The Foreign Intelligence Surveillance Act of 1978 (FISA)*, U.S. DEP'T OF JUST. BUREAU OF JUST. ASSISTANCE (Mar. 27, 2021, 10:13 PM), https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286#vf4tzl [https://perma.cc/8N6A-CKEP].

9. 50 U.S.C. § 1801(e)(1).

10. *See id.* at § 1801(h); *see also* 50 U.S.C. § 1873(g)(4).

11. *See* William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633, 1641 (2010).

12. *Id.* at 1635 (programmatic surveillance approved by the FISC, by statute, requires minimization procedures).

13. *Coalition Statement Urges Senator Schumer to Keep Reauthorization of Section 702 Out of Continuing Resolution*, BRENNAN CTR. FOR JUST. AT N.Y.U. L. SCH. (Nov. 13, 2023), https://www.brennancenter.org/our-work/research-reports/coalition-statement-urges-senator-schumer-keep-reauthorization-section [https://perma.cc/FRA4-BQUU].

14. *See* Karoun Demirjian, *G.O.P. Threatens Spy Agencies' Surveillance Tool*, N.Y. TIMES (July 3, 2023), https://www.nytimes.com/2023/07/03/us/section-702-spying.html [https://perma.cc/5XV5-LVN5].

15. *See* 42 U.S.C. § 1983 ("Every person who . . . [causes] deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law . . .").

surveilled by a government whose actions they oppose is considered to have a "chilling effect" on free speech.[16]

Nevertheless, since its enactment, FISA has been regarded as instrumental by the federal government in protecting the United States against security threats.[17] The intelligence community has warned of grave consequences for national security if the baby is thrown out with the bathwater and Section 702 is repealed.[18]

The opposition to FISA is not recent, and efforts have been made to address demands for greater protections of U.S. persons in the FISA process. Enacted in 2015, the USA FREEDOM Act included several reforms to FISA, among them the creation of a panel of amici curiae, who would brief the FISC with their expertise when a "novel or significant interpretation of the law" arose during a warrant application.[19] The FISA process would remain non-adversarial, but the amici would provide an independent voice on matters to inform the FISC's decision.[20]

The reform, while welcome, does not appear to have been sufficient—either to dampen criticism of FISA's programmatic surveillance programs or meaningfully prevent abuses of the system since 2015.[21] Adversarial hearings at the FISC, whereby special advocates with requisite security clearances appear before the court to oppose government warrant applications, have been proposed previously, though these proposals have never been adopted by Congress.[22] It is possible, however, to reconcile adversarial hearings with reforms to FISA in 2015 under the USA FREEDOM Act by empowering authorized amici curiae to intervene in FISA proceedings. A novel solution such as this one would rely on established legal processes of intervention in a proceeding, in this case for warrant applications, to allow an expanded panel of amici to participate and oppose the granting of a FISA warrant. Because the amici would have the discretion to intervene in warrant applications, the proposal is distinct from previous attempts that propose the creation of a new office to constantly oppose the government during FISC proceedings. The adversarial nature—placing their subject matter expertise in an adversarial position against government claims of necessity—is especially useful to

16. *Warrantless Surveillance Under Section 702 of FISA*, ACLU (Sept. 28, 2023, 9:43 PM), https://www.aclu.org/issues/national-security/warrantless-surveillance-under-section-702-fisa [https://perma.cc/L7UM-X65E].

17. Merrick Garland & Avril Haines, *Joint Letter from Attorney General Garland and Director of National Intelligence Haines to Congressional Leadership Regarding Reauthorization of Title VII of FISA*, U.S. DEP'T OF JUST. NAT'L SEC. DIV. (Feb. 28, 2023), https://www.justice.gov/media/1276406/dl?inline= [https://perma.cc/H338-6MU7].

18. *Id.*

19. Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268, 279 (2015) (codified as amended at 50 U.S.C. § 1803(i)) [hereinafter USA FREEDOM Act].

20. Chris Baumohl, *Reforming Section 702: Strengthening FISA Amici*, ELEC. PRIV. INFO. CTR. (Mar. 2, 2023, 10:00 PM), https://epic.org/reforming-702-strengthening-fisa-amici/ [https://perma.cc/5PG3-529V].

21. *Id.*

22. ANDREW NOLAN, RICHARD M. THOMPSON II & VIVIAN S. CHU, CONG. RSCH. SERV., R43260, REFORMING OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS: INTRODUCING A PUBLIC ADVOCATE 2 (2014).

ensuring greater and competitive scrutiny of the government's representations to the FISC. Thus, by providing an adversarial element in the FISA process, the proposal would make the process less prone to abuse and ensure accountability at the FISC.

To that end, this Note will propose a framework for amending FISA to empower the panel of amici curiae, created under 50 U.S.C. § 1803(i), to intervene as a matter of statutory right in proceedings for a surveillance warrant under FISA, i.e., 50 U.S.C. § 1805. Section II will explain the non-adversarial nature of the FISC and resulting controversy, as well as discuss past efforts to reform the act. Section III, proposing the framework, will analyze how amici curiae might exercise their right of intervention and will argue for their suitability for the role. It will argue that empowering amici to intervene will improve the FISC's review of surveillance applications, hold the government accountable for any abuse of FISA authority, and compel the adoption of stricter standards to protect U.S. persons from unconstitutional surveillance.

II. BACKGROUND

A. The Origins of FISA and its Reforms

Before FISA's enactment in 1978, there was no statutory framework to regulate the federal government's surveillance activities for national security-related reasons.[23] The footnote in *Katz* that appeared to exempt such conduct from Fourth Amendment procedures was, perhaps, the only case law on the matter.[24] Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("OCC Act"), meanwhile, provided the procedure under the Fourth Amendment to seek warrants for electronic surveillance.[25] Two events, whereby much controversy was elicited over surveillance, compelled the government to action.

The first event was the 'Keith Case,' known formally as *United States v. United States District Court*, where the Supreme Court ruled that the government was required to obtain a warrant before beginning electronic surveillance within the United States, even in cases of national security.[26] In that case, the government had relied on a provision in the OCC Act—giving the government discretion to act to protect national security—to claim that a warrant was not required.[27] The Court rejected the argument. "The freedoms of the Fourth Amendment cannot properly be guaranteed if domestic security

23. United States v. U.S. Dist. Ct. for E. Dist. of Mich., 407 U.S. 297, 299 (1972) ("Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees, without guidance from the Congress or a definitive decision of this Court. This case brings the issue here for the first time.").

24. *Katz*, 389 U.S. at 358.

25. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 212 (1968) (codified at 18 U.S.C. § 2516, *et. seq.*).

26. *U.S. Dist. Ct. for E. Dist. of Mich.*, 407 U.S. at 297-99.

27. *Id.*; Omnibus Crime Control, *supra* note 25, at 214 (current version at 18 U.S.C. § 2511(3)).

surveillances are conducted solely within the discretion of the executive branch, without the detached judgment of a neutral magistrate," wrote Justice Lewis F. Powell, Jr. for the unanimous court.[28] Powell's opinion also urged Congress to create standards for situations involving national security that would be compatible with the Fourth Amendment.[29]

The second event was the "Church Committee," known formally as the "Senate Select Committee to Study Government Operations with Respect to Intelligence Activities." Following the Watergate scandal and several press revelations of covert activity by the executive branch,[30] both houses of Congress convened select committees to study intelligence collection by the government.[31] The Senate committee, chaired by Democratic Sen. Frank Church of Idaho, in 1976 produced a report six books in length,[32] uncovering widespread abuses of surveillance power by the government to monitor the behavior and communications of U.S. persons, "who engaged in no criminal activity and who posed no genuine threat to the [*sic*] national security."[33] Much of the activity reported the Church Committee was pursued despite doubts about its constitutionality with legal considerations simply being ignored by officials.[34] "The root cause of the excesses which our record amply demonstrates has been failure to apply the wisdom of the constitutional system of checks and balances to intelligence activities," wrote Church in his preface to Book II of the committee's report, which detailed intelligence activities and the rights of Americans.[35] "I believe they make a compelling case for substantial reform."[36]

At the urging of the Supreme Court and the Senate, combined with public outrage at the nature of warrantless surveillance, Congress proceeded to enact FISA two years later.[37] The principal reform of FISA was its creation

---

28. *U.S. Dist. Ct. for E. Dist. of Mich.*, 407 U.S. at 298.

29. *Id.* at 322-23.

30. *See* Seymour Hersh, *Huge C.I.A. Operation Reported In U.S. Against Antiwar Forces, Other Dissidents In Nixon Years*, N.Y. TIMES (Dec. 22, 1974), https://www.nytimes.com/1974/12/22/archives/huge-cia-operation-reported-in-u-s-against-antiwar-forces-other.html [https://perma.cc/T3G4-VQ2R].

31. The Senate's counterpart committee in the House was known as the "Pike Committee," after its chairman, Democratic Rep. Otis G. Pike of New York, and conducted a similar investigation. *See The Unexpurgated Pike Report*, INTERNET ARCHIVE, https://archive.org/details/PikeCommitteeReportFull/page/n1/mode/2up [https://perma.cc/9YA5-L4K9]. .

32. *Intelligence Related Commissions, Other Select or Special Committees and Special Reports*, U.S. S. SELECT COMM. ON INTEL., https://www.intelligence.senate.gov/resources/intelligence-related-commissions (last visited Apr. 10, 2025) [https://perma.cc/KWZ7-L3ER].

33. S. REP. NO. 94-755, at 12 (1976).

34. *Id.* at 13.

35. *Id.* at III.

36. *Id.*

37. James G. McAdams, III, *Foreign Intelligence Surveillance Act (FISA): An Overview*, U.S. FED. L. ENF'T TRAINING CTRS., https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf [https://perma.cc/WYE3-RV56].

of judicial scrutiny over intelligence collection done within the United States. Should the federal government seek to conduct surveillance within the United States targeted at an agent of a foreign power, it must seek an order from the FISC authorizing such surveillance.[38] While the court reviews such applications *in camera* and *ex parte*, the statute makes the issuance of such an order subject to extensive disclosure requirements as well as "minimization procedures"[39] to prevent the inadvertent gathering of information on U.S. persons.[40] The statute imposes criminal penalties and civil liability for damages upon government personnel who conduct surveillance in violation of the statute,[41] as well as empowers defendants to move to suppress evidence in criminal proceedings if FISA surveillance is gathered unlawfully.[42] Intelligence gathered unintentionally from a U.S. source by FISA-authorized surveillance, which is otherwise protected by the Fourth Amendment, must be destroyed.[43]

B. The Emergence of Section 702

FISA's enactment in 1978 was welcomed by watchdogs of government surveillance,[44] though continued exercise of surveillance authority proved controversial among them.[45] The biggest paradigm shift in the FISA regime, however, occurred following the terrorist attacks of September 11, 2001 against the United States by al-Qa'ida. Surveillance authority claimed and exercised by the executive branch, thereafter, spurred further controversy about government surveillance during the "War on Terrorism," which prompted FISA's significant amendment to meet both the privacy and security demands of the 21st Century.[46]

In diagnosing intelligence failures surrounding the government's inability to detect the attacks in advance, the 9/11 Commission opined about the rigidity of safeguards under FISA to protect the privacy of U.S. persons.[47] In 1995, following concerns about informal exchanges of FISA-gathered intelligence between U.S. Department of Justice ("DOJ") criminal prosecutors and Federal Bureau of Investigation ("FBI") counterintelligence officials, Attorney General Janet Reno implemented procedures to regulate

38. *See* 50 U.S.C. § 1805.
39. *See id.* § 1801(h).
40. *See id.* § 1801(i).
41. *See id.* § 1809-10.
42. *See id.* § 1806(e).
43. *See id.* § 1806(i).
44. *See* David Burnham, *Panel Cites U.S. Compliance With Law Limiting Wiretaps*, N.Y. TIMES (Oct. 19, 1984), at B5, https://www.nytimes.com/1984/10/19/us/panel-cites-us-compliance-with-law-limiting-wiretaps.html [https://perma.cc/QBY5-V33S].
45. *See* Michael Wines, *Panel Criticizes F.B.I. for Scrutiny of U.S. Group*, N.Y. TIMES (July 17, 1989), at A13, https://www.nytimes.com/1989/07/17/us/panel-criticizes-fbi-for-scrutiny-of-us-group.html [https://perma.cc/7ZRG-5RXW].
46. *See* Robert Bloom & William J. Dunn, *The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment*, 15 WM. & MARY BILL RTS. J. 147, 151 (2006).
47. *See* THE 9/11 COMM'N, THE 9/11 COMM'N REPORT: FINAL REPORT OF THE NATIONAL COMM'N ON TERRORIST ATTACKS UPON THE U.S. 78-79 (2004).

transmission of such intelligence between the former and latter.[48] The procedures, known as "the Wall,"[49] effectively discouraged the sharing of intelligence information to criminal investigators and prosecutors, as well as vice versa with respect to grand jury information.[50] The Commission's report concluded that the strict procedures of "the Wall" regarding intelligence gathering and sharing, as well as FISA's own statutory requirements for warrants, precluded the FBI from gathering intelligence about Zacarias Moussaoui—an al-Qa'ida operative connected to 9/11 mastermind Khalid Sheikh Mohammad, and who had suspiciously sought flight school lessons in Minneapolis on a Boeing 747 platform—prior to the attacks.[51] "If Moussaoui had been connected to al Qaeda [*sic*], questions should instantly have arisen about a possible al Qaeda plot that involved airliners, a possibility that had never been seriously analyzed by the intelligence community," the report concluded.[52]

The George W. Bush Administration, meanwhile, took matters into its own hands. Shortly after 9/11, on October 4, President Bush issued the first in a series of executive orders to the National Security Agency ("NSA"), authorizing the creation of the President's Surveillance Program ("PSP").[53] Under the PSP, the NSA was directed to gather massive telephone and Internet metadata regarding communications if there was probable cause regarding a connection to international terrorism. The connection could either involve U.S. persons or information transmitted through the United States, and could be gathered without obtaining a warrant from the FISC.[54] These programs were legally justified by DOJ memoranda, written by John Yoo, a deputy assistant attorney general in the Office of Legal Counsel, who directly challenged FISA's authority to make surveillance conditional on a FISC warrant.[55] Acknowledging that Bush Administration's initial executive order could not satisfy FISA standards,[56] Yoo claimed that FISA's restrictions on surveillance represented an "unconstitutional infringement on the President's Article II authorities"[57] and that the president possessed "inherent constitutional power to conduct warrantless searches for national security

48. *Id.*

49. *Id.*

50. These limitations on communication were statutorily removed by the USA PATRIOT Act of 2001. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 364 (2001) (codified at 50 U.S.C. § 1806(k)(1)).

51. THE 9/11 COMM'N, *supra* note 47, at 273-76.

52. *Id.* at 273.

53. OFF. OF INSPECTORS GEN. OF THE DEP'T OF DEF., DEP'T OF JUST., CENT. INTEL. AGENCY, NAT. SEC. AGENCY, AND DIR. OF NAT'L. INTEL., NO. 2009-0013-AS, (U) UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 7 (2009), https://www.dni.gov/files/documents/424/2009%20Joint%20IG%20Report%20on%20the%20PSP%20Vol.%20I.pdf [https://perma.cc/3KSV-345S].

54. *Id.* at 8.

55. *Id.* at 12.

56. Memorandum from John C. Yoo, Deputy Assistant Att'y Gen. 9-10 (Nov. 2, 2001) (on file with author) https://www.justice.gov/olc/page/file/1154156/dl?inline [https://perma.cc/TU83-DNBB].

57. *Id.* at 9.

purposes."[58] Among other matters, Yoo further opined that foreign intelligence surveillance of communications entering or exiting the United States, contrary to FISA, were instead governed by Fourth Amendment jurisprudence alone, and fell within a "border search exception" that allowed for their collection without a warrant.[59]

The activities under the PSP, which was code-named "STELLARWIND,"[60] continued unbeknownst to the public until 2005, when a front-page article in The New York Times broke the news of the program's existence based on information provided by unnamed government officials amid concerns about its legality.[61] "[The NSA] has monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants," read the article, which the administration had asked the Times to not publish.[62] The program was formally acknowledged by Attorney General Alberto Gonzales in 2007,[63] and, following The New York Times's revelation, aspects of the program were gradually brought into FISA compliance with fresh applications to the FISC for their authorization.[64] Nevertheless, knowledge of the program ignited public opposition to it, which prompted Congress to consider action that might rein in executive conduct and bring it into compliance with FISA.[65]

The result of that effort was the FISA Amendments Act of 2008.[66] This act created a new provision of FISA known as Section 702, which authorizes the executive branch, in one-year increments, to collect intelligence regarding non-U.S. person targets, who are "reasonably believed to be located outside the United States."[67] The government is required, however, to submit a certification to the court—regarding minimization procedures and Fourth Amendment compliance—before implementing any surveillance under Section 702,[68] unless an emergency situation (as defined by the Attorney General and Director of National Intelligence) necessitates immediate surveillance and *ex post facto* certification.[69] The FISC, thereafter, reviews

58. *Id.*

59. *Id.* at 14.

60. *NSA inspector general report on email and internet data collection under Stellar Wind – full document*, THE GUARDIAN (June 27, 2013, 12:01 PM), https://www.theguardian.com/nsa-inspector-general-report-document-data-collection [https://perma.cc/9EYH-S4LU].

61. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html [https://perma.cc/83ZE-GUKR].

62. *Id.*

63. Letter from Alberto R. Gonzales, Att'y Gen., to Hon. Patrick J. Leahy, Chairman, Comm. on Judiciary, U.S. Senate (Aug. 1, 2007) (on file with author), https://irp.fas.org/news/2007/08/ag080107.pdf [https://perma.cc/KXB7-KURX].

64. OFF. OF INSPECTORS GEN., *supra* note 53, at 50-60.

65. *See* H.R. REP. NO. 110-373, pt. I, at 9-10 (2007).

66. *See* Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2009).

67. 50 U.S.C. § 1881a(a), *et. seq.*

68. *See id.* § 1881a(h)(1)(A).

69. *See id.* § 1881a(c)(2), (h)(1)(B).

such certification for compliance with the Act, after which it may modify or prohibit such collections.[70] Importantly, the amendments ensure that the government is not required to submit individual certifications to the court for each person surveilled, but may do so for a class of persons to be surveilled under a program, known as "programmatic" authorization.[71] The law countenances the incidental acquisition of information about U.S. persons under such programs but aims to mitigate them by virtue of judicial review of the certification and FISA's existing provisions preventing their use. Electronic service providers who receive directives from the government pursuant to a FISA order may challenge them by petitioning the FISC, which is the only incidence of adversarial proceedings at the court, on the limited question of whether the directives to them (and not the underlying surveillance programs) violate FISA or are otherwise unlawful.[72]

C. The Current Controversy

Since Section 702 was enacted, programmatic surveillance by the United States government has dramatically expanded. Disclosures to media organizations by former NSA contractor Edward Snowden in 2013 revealed the existence of a program—code-named PRISM—whereby the federal government collected information from electronic communications service providers, such as Google, Meta, and Apple, using Section 702 authority.[73] PRISM reportedly accounted for up to 91% of NSA internet search traffic under FISA authority.[74] Another program, code-named XKeyscore, also conducted programmatic surveillance of foreign targets, though it is unclear whether it operated pursuant to FISC order.[75] The intelligence collected by such surveillance programs is often stored in databases, known colloquially as "Section 702 databases,"[76] to which intelligence officials may submit queries to obtain information about a foreign target.[77]

---

70. *See id.* § 1881a(j)(3)(A)-(B).

71. Banks, *supra* note 11, at 1635.

72. *See* 50 U.S.C. § 1881a(i)(4)(A).

73. *See* Glenn Greenwald & Ewan MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, THE GUARDIAN (June 7, 2013), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [https://perma.cc/4BJ7-WGLF]; Barton Gellman & Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, WASH. POST (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [https://perma.cc/V6ZD-TMLX].

74. *See* JOHN W. ROLLINS & EDWARD C. LIU, CONG. RSCH. SERV., R43134, NSA SURVEILLANCE LEAKS: BACKGROUND AND ISSUES FOR CONGRESS 4 (2013).

75. *See* Glenn Greenwald, *XKeyscore: NSA tool collects 'nearly everything a user does on the internet'*, THE GUARDIAN (July 31, 2013), https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data [https://perma.cc/NE4W-YZZM].

76. *See Section 702 Overview*, OFF. OF THE DIR. OF NAT'L INTEL. (Apr. 17, 2018, 4:37 PM), https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf [https://perma.cc/EH25-GX8S].

77. 50 U.S.C. § 1881a(f), *et. seq.*

Section 702 has been criticized by civil liberties organizations for a variety of reasons. One of the most potent critiques of the law is the phenomenon of "backdoor" searches of information conducted by federal government officials.[78] In the massive collection of incidental intelligence about U.S. persons, critics argue that law enforcement can query and obtain such information, despite the information being unrelated to national security.[79] The only limitation on these searches is that they must be "reasonably likely" to retrieve either foreign intelligence or evidence of a crime, which critics assert is a low standard.[80] In effect, they argue that Section 702's authority, while intended for foreign intelligence collection and national security, is being used for criminal justice purposes and circumvents the Fourth Amendment limitations on their collection,[81] as specified in the Keith Case.[82] They also argue that the prevalence of such large-scale surveillance has a "chilling effect"[83] on speech and expression permitted by the First Amendment, deterring activists and critics of the government from engaging in such activity out of fear of being surveilled.[84]

Opposition to Section 702 has been increasingly bipartisan with both left-wing and right-wing opponents. The latter group, however, has grown hostile to Section 702 primarily following the presidential election of 2016. As part of a counterintelligence investigation, known as Crossfire Hurricane, into whether Donald Trump's 2016 campaign received material assistance from the Russian government, the FBI obtained a FISA warrant to surveil Carter Page, a U.S. citizen and foreign policy advisor to Trump.[85] The FBI's application for the warrant from the FISC was later found to have material defects and false statements.[86] Trump has frequently invoked the FISA warrant on Page to justify claims of a "conspiracy" against him by government intelligence personnel (i.e., the "deep state") due to his political

78. *See* Sarah Taitz, *Five Things to Know About NSA Mass Surveillance and the Coming Fight in Congress*, ACLU (Apr. 11, 2023), https://www.aclu.org/news/national-security/five-things-to-know-about-nsa-mass-surveillance-and-the-coming-fight-in-congress [https://perma.cc/3LRV-LQU2].

79. *Id.*

80. *Id.*

81. *Id.*

82. *U.S. Dist. Ct. for E. Dist. of Mich.*, 407 U.S. at 298.

83. Rainey Reitman, *NSA Internet Surveillance Under Section 702 Violates the First Amendment*, ELEC. FRONTIER FOUND. (Nov. 22, 2017), https://www.eff.org/deeplinks/2017/11/nsa-internet-surveillance-under-section-702-violates-first-amendment [https://perma.cc/24JN-DRNF].

84. *See* Taitz, *supra* note 78.

85. *See FISA Warrant Application for Carter Page*, U.S. S. COMM. ON THE JUDICIARY (Feb. 7, 2020), https://www.judiciary.senate.gov/imo/media/doc/FISA%20Warrant%20Application%20for%20Carter%20Page.pdf [https://perma.cc/MB47-LPV4].

86. *See* OFF. OF THE INSPECTOR GEN. OF THE DEP'T OF JUST., REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION 156 (Dec. 9, 2019), https://www.justice.gov/storage/120919-examination.pdf [https://perma.cc/ZK5G-FQAJ].

views.[87] One of the documents allegedly relied upon by the FBI to support its warrant for surveilling Page was the "Steele Dossier," which was prepared by a former British intelligence officer and claimed the existence of embarrassing sexual material possessed by the Russian government regarding Trump, The dossier was later discredited by DOJ investigators and its production was found to have been sponsored by the supporters of Trump's electoral opponent, Hillary Clinton.[88] While this surveillance does not implicate Section 702 directly, it has created a climate of hostility among conservatives to the expansion of FISA authority, which has resulted in opposition to Section 702 among Republican members of Congress.[89]

When critics have waged legal challenges to programs under Section 702, the results have been largely ineffectual due to procedural hurdles of standing. The Supreme Court ruled in *Clapper v. Amnesty Int'l U.S.A* in 2012 that persons whose communications might be collected, as opposed to being definitively collected, by programs under Section 702 lack standing to sue.[90] Additionally, the government's assertions of the "state secrets privilege"—a privilege that enables the government to withhold evidence that may "expose military matters which, in the interest of national security, should not be divulged"[91]—in lawsuits challenging Section 702 has often led to their dismissal.[92] The result is that no court has ever ruled on the merits of Section 702's legality under the Fourth Amendment.

Consequently, opponents have turned their focus to Congress. In 2008, Section 702's authority was not authorized permanently but, instead, was to expire five years later, at the beginning of 2013.[93] It was then renewed for another five years until 2018,[94] and, renewed again until 2023.[95] Opponents have sought to use the periodic reauthorizations to reform the law, or repeal it, with the 2018 reauthorization including statutory amendments regarding

87. *See* Donald J. Trump, @realDonaldTrump, X (July 22, 2018, 6:28 AM), https://x.com/realDonaldTrump/status/1020978929736265729 [https://perma.cc/UL47-HY2Y].

88. JOHN H. DURHAM, REPORT ON MATTERS RELATED TO INTELLIGENCE ACTIVITIES AND INVESTIGATIONS ARISING OUT OF THE 2016 PRESIDENTIAL CAMPAIGNS 109, 110, 123 (May 12, 2023), https://www.justice.gov/storage/durhamreport.pdf [https://perma.cc/UX54-AS93].

89. *See* H.R. 577, 118th Cong. (2023), https://www.congress.gov/118/bills/hres577/BILLS-118hres577ih.pdf [https://perma.cc/J46L-PMQH]. Several Republican members of Congress have publicly called for Section 702's authority to lapse. *See* Arjun Singh, *House Conservatives Tank FISA Vote In Blow To Speaker Mike Johnson*, THE DAILY CALLER (Apr. 10, 2024, 3:02 PM), https://dailycaller.com/2024/04/10/house-blocks-fisa-reauthorization-bill/ [https://perma.cc/8GT9-A8MS].

90. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013) ("respondents' theory of future injury is too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending'").

91. United States v. Reynolds, 345 U.S. 1, 10 (1953).

92. *See* Wikimedia Found. v. Nat. Sec. Agency, 14 F.4th 276 (4th Cir. 2021) (opinion and order affirming dismissal).

93. FISA Amendments Act of 2008, *supra* note 66, at 2474.

94. *See* FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (2012).

95. *See* FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, 132 Stat. 3 (2018).

querying provisions and FBI access to intelligence collections for criminal justice purposes.[96] Amid continued demands for reform, Congress in December 2023—when Section 702 was set to expire—temporarily reauthorized it until April 19, 2024; it was reauthorized for two years in April, with new limits on the querying of terms.[97]

D. Proposals to Reform FISA for Greater Accountability

Many proposals to reform FISA, to ensure a greater check on the executive branch in its surveillance requests and activities, have previously been published.[98] An exhaustive discussion of all proposals is unnecessary here. Merely, at a juncture where Section 702's reauthorization is under consideration by Congress,[99] it is relevant to review current congressional proposals to amend the law, as well as previous attempts to create an adversarial process in the pre-warrant stage of FISA surveillance. These are relevant because of their ongoing consideration by Congress. They would make FISA adversarial, an idea that is advanced by this Note.

Before Congress's reauthorization of Section 702 in December 2023,[100] several congressional initiatives were undertaken to propose reforms that might gain political support. The Republican majority of the House Permanent Select Committee on Intelligence ("HPSCI"), which has jurisdiction over foreign intelligence collection, proposed 45 ideas for reforming FISA—including DOJ audits of all U.S. person queries, requirements of warrants to seek evidence of a crime before any U.S. person queries are conducted, penalties for "noncompliant querying of U.S. person contents" and criminal charges for intentional leaking information of U.S. persons.[101] The list also includes measures to ensure Congress is periodically informed about non-compliant U.S. person queries and any disciplinary action under them as well as to permit members of Congress and staff to

96. *See id*. at 4-10.

97. *See* National Defense Authorization Act for Fiscal Year 2024, Pub. L. No. 118-31, 137 Stat. 136 (2023); Reforming Intelligence and Securing America Act, Pub. L. No. 118-49, 138 Stat. 862 (2024).Both laws were short-term extensions to give lawmakers more time to consider permanent FISA reauthorization.

98. *See generally* Ensuring Adversarial Process in the FISA Court Act, H.R. 3159, 113th Cong. (2013); PRIV. AND C.L. OVERSIGHT BD., REPORT ON THE TELEPHONE RECORD PROGRAM CONDUCT UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 184 (2014), https://irp.fas.org/offdocs/pclob-215.pdf [https://perma.cc/CH8J-9LHN].

99. Letter from Mike Johnson, Speaker of the House of Representatives, to members of the House of Representatives, (Dec. 7, 2023) (on filed with author), https://www.documentcloud.org/documents/24199528-1272023-speaker-dear-colleague [https://perma.cc/N53X-PNP6].

100. *Id.*

101. MAJORITY FISA WORKING GRP., U.S. H.R. PERMANENT SELECT COMM. ON INTEL., FISA REAUTHORIZATION: HOW AMERICA'S MOST CRITICAL NATIONAL SECURITY TOOL MUST BE REFORMED TO CONTINUE TO SAVE AMERICAN LIVES AND LIBERTY 42-47 (2023), https://intelligence.house.gov/uploadedfiles/hpsci_fisa_reauthorization_2023_report.pdf [https://perma.cc/4P3D-M8JG].

attend FISC hearings.[102] Unfortunately, the HPSCI's proposals only address the issue of accountability for abuse, rather than *ex ante* measures to preclude such abuse.[103] Should its ideas be implemented, they would not directly affect the FISC's tailoring of surveillance programs to minimize incidental collection, which is fundamental to ensuring that U.S. persons are protected from surveillance at the outset. Rather, they merely protect information from being misused after the fact.

A parallel proposal, with support among many civil libertarian groups,[104] was introduced in both the Senate and House, known as the Government Surveillance Reform Act.[105] This proposal would narrow the purposes for which information collected under FISC orders may be used, limit the kind of intelligence that may be collected,[106] and limit "reverse targeting" or the targeting of foreign sources for the purpose of obtaining U.S. person information.[107] This proposal's changes to the law's language, if implemented, would likely affect the FISC's standard of review when considering applications for surveillance. However, it offers no reform to the warrant application process and, thus, leaves in place the *ex parte* dynamic between the court and the government. Tangentially, the bill would make FISC applications reviewable by an Inspector General but merely allows that official to make recommendations to various bodies regarding how those orders might be improved.[108]

Regarding reforms to the *ex parte* system, Congress has previously taken steps to offer the FISC an independent perspective when considering warrant applications. In the USA FREEDOM Act of 2015, Congress created a panel of amici curiae to assist the FISC.[109] The amici are authorized to assist the court with warrant applications that present a "novel or significant interpretation of the law" or to provide "technical expertise" when the court is dealing with difficult questions.[110] The USA FREEDOM Act requires that amici be made eligible for security clearances and grants them access to information regarding the FISC's past decisions as well as the current

102. *Id.* at 42, 46

103. *Id.*

104. *Wyden, Lee, Davidson and Lofgren Introduce Bipartisan Legislation to Reauthorize and Reform Key Surveillance Law, Secure Protections for Americans' Rights*, RON WYDEN, U.S. SENATOR FOR OREGON (Nov. 7, 2023), https://www.wyden.senate.gov/news/press-releases/wyden-lee-davidson-and-lofgren-introduce-bipartisan-legislation-to-reauthorize-and-reform-key-surveillance-law-secure-protections-for-americans-rights/ [https://perma.cc/5378-3LFD].

105. Government Surveillance Reform Act of 2023, H.R. 6262, 118th Cong. (1st Sess. 2023).

106. *Id.* § 103. This limitation pertains to "abouts" collection, a short-hand for queries for all information that simply mentions a target, rather than merely communications between them and another party. *See generally* Julian Sanchez, *All About "About" Collection*, JUST SECURITY (Apr. 28, 2017), https://www.justsecurity.org/40384/ado-about/ [https://perma.cc/6DXL-TEF2].

107. FISA Amendments Reauthorization Act of 2017, *supra* note 95, §§ 101-103.

108. *Id.* § 112.

109. USA FREEDOM Act, *supra* note 19; Pub. L. No. 114-23, § 401 (codified at 50 U.S.C. § 1803(i)).

110. 50 U.S.C. § 1803(i)(2)(A)-(B).

application they have been called to review.[111] The amici are required to be "persons who possess expertise in privacy and civil liberties, intelligence collection, communications technology, or any other area."[112] The FISC has published the list of current amici on its website.[113]

Introducing amici to the FISC process is significant and offers the opportunity for government submissions to the court to be scrutinized by independent experts. However, this opportunity is only afforded subject to the court's discretion.[114] It is entirely plausible that a judge reviewing an application may not grasp the full implications of the proposed surveillance by themselves. The judge may not recognize when proposed methods or minimization procedures may threaten U.S. persons. In a landscape of rapidly changing technologies, particularly involving artificial intelligence, it is difficult to foresee that an Article III judge appointed to the FISC for a limited duration may remain abreast of these changes to adequately know all the issues with an application by themselves. Deference to the government's interpretation and its mere assurances of compliance with FISA would defeat the purpose of holding it accountable. An independent review is required, at the application stage, with sufficient expertise to understand the technical scope of surveillance proposed and its conformity with the law. Indeed, given the government's record of past abuses,[115] the FISC's high rate of approval of requests,[116] and the potential for further constitutional erosion of U.S. persons' rights, nothing short of zealous advocacy in an adversarial setting is appropriate.

To this end, the concept of a special or "public advocate" who would challenge the government's requests for surveillance at the FISC has been previously proposed.[117] Such an individual, or group of individuals, would likely be empowered to argue against the government's warrant applications, make submissions before the court and, if the warrant was granted, appeal the matter to the Foreign Intelligence Surveillance Court of Review ("FISCR")—an appellate court that only hears government appeals from denials of requests

111. *Id.* §§ 1803(i)(3)(B), (6)(A)-(C).

112. *Id.* § 1803(i)(3)(A).

113. *Amici Curiae*, U.S. FOREIGN INTEL. SURVEILLANCE CT., https://www.fisc.uscourts.gov/amici-curiae (last visited Mar. 3, 2025) [https://perma.cc/DLJ5-SGRK].

114. 50 U.S.C. § 1803(i)(2)(A) ("shall appoint [amicus curiae] . . . to assist such court in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate"). The discretion of the court is evinced in the ability to make amicus curiae appointments when it deems necessary in its opinion.

115. UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM, *supra* note 53.

116. The FISC reports data on the number of orders granted, modified, denied in part, and denied; historical assessments of this data have revealed that the court grants applications at a high rate, i.e., above 99% of all requests. *See* Conor Clarke, *Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate*, 66 STAN. L. REV. ONLINE 125, 131 (2014), https://www.stanfordlawreview.org/wp-content/uploads/sites/3/2014/02/66_Stan_L_Rev_Online_125_Clarke.pdf [https://perma.cc/2SYJ-P8MT].

117. Ensuring Adversarial Process in the FISA Court Act, H.R. 3159, 113th Cong. (2013).

by the FISC—and, in extraordinary circumstances, the Supreme Court.[118] The proposals suggest that public advocate[s] be appointed from among individuals who have requisite expertise for such a role.[119] The idea appears to have been seriously considered by the Obama Administration before to the USA FREEDOM Act's passage. President Barack Obama, himself, endorsed the idea in public remarks[120], while the Privacy and Civil Liberties Oversight Board ("PCLOB") recommended the idea in its review of the FISC's operations.[121]

The proposal for a public advocate has, to date, not been adopted by Congress. Objections have been raised about the alleged difficulties that such "public advocates" would create, regarding their constitutional status as government employees and their legal standing to challenge applications on behalf of the general public.[122] It is unclear how much influence the PCLOB report had on Congressional consideration of the proposal. At least two bills were introduced in the 113th Congress to create a public advocate or a similarly-named office that would argue before the FISC, but neither received any action.[123]

III. ANALYSIS

To ensure more accountability in the process of authorizing FISA surveillance, as well as compliance with statutory and constitutional requirements, the current system of *ex parte* hearings before the FISC must be reformed. Accordingly, this section will propose the empowerment of the current group of amici curiae by granting them a statutory right of intervention in proceedings before the FISC. The new group, which may be termed the "Panel of Experts," would be expanded and authorized to challenge applications for a warrant of surveillance, or reauthorization of the same, by the government under any provision of FISA. They would no longer be limited, as are the amici, to questions involving a "novel interpretation" of the law, and would have a statutory right to appeal decisions granting government requests, as well as petition the Supreme Court for certiorari if the FISCR denies relief. The panel, expanded beyond amici, would comprise individuals appointed by the Presiding Judge of the FISCR, with an emphasis upon recommendation of the current amici, i.e., a collegium system. That the panel would be drawn from existing amici, who are granted discretion on when to intervene, distinguishes this proposal from other adversarial reforms previously advanced, where the advocates in question would appear to be

118. *See* Foreign Intelligence Surveillance Act of 1978, *supra* note 3.

119. *See* NOLAN, ET AL., *supra* note 22.

120. Barack Obama, President of the U.S., The White House, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence [https://perma.cc/PK4K-3D8L.

121. PRIV. AND C.L. OVERSIGHT BD., *supra* note 98.

122. *See* Clarke, *supra* note 116.

123. FISA Court Reform Act of 2013, H.R. 3228, 113th Cong. (1st Sess. 2013); Ensuring Adversarial Process in the FISA Court Act, H.R. 3159, 113th Cong. (1st Sess. 2013).

government employees with a duty to oppose applications submitted by the United States. The employment status of such a person under those "public advocate" proposals implicated constitutional questions concerning their executive authority and validity of appointment,[124] which this proposal circumvents by virtue of the amici's private citizen status.

A. Summary of Proposed Statutory Language to Create Panel Of Experts

The full statutory language to create a Panel of Experts has been included in the Appendix to this Note.[125] The language replaces 50 U.S.C. § 1803(i), the provision of law that authorizes amici curiae, with modifications to empower the panel to intervene in proceedings of the FISC and FISCR. A summary of the proposed language's provisions, which are relevant to the creation of adversarial proceedings, follows.

1. Paragraph 1, Appointments of experts:

> This paragraph establishes that the Presiding Judge of the FISCR shall appoint "not fewer than 15 individuals to be eligible to serve as members of a Panel of Experts."[126] The number is an increase from the current statute's composition of amici, which sets the number at "not fewer than 5."[127] The reason for such an increase is to ensure the body has a diversity of opinion and heterogeneity of expertise. To aid the chief judge in the exercise of appointment duties, certain entities are named as empowered to make recommendations regarding individuals to be appointed. The PCLOB is one group, an independent agency of the U.S. government that provides advice on civil liberties issues.[128] The other entity empowered to make recommendations are members of the Panel, whose grasp of issues enables them to opine on the suitability of candidates. The Presiding Judge is not bound to accept their recommendations, but their inclusion in the language is intended to grant their recommendations persuasive authority.

124. *See* NOLAN, ET AL., *supra* note 22.
125. *See infra* Part V, pp. 21-24.
126. *Id.* at 21.
127. 50 U.S.C. § 1803(i).
128. *History and Mission*, PRIV. AND C.L. OVERSIGHT BOARD, https://www.pclob.gov/About/HistoryMission (last visited Mar. 3, 2025) [https://perma.cc/Z5NL-YUZC].

2. Paragraph 3, Expert qualifications:

This paragraph lays out qualifications for the Presiding Judge of the FISCR to consider when making appointments to the panel, namely their "expertise in privacy and civil liberties, intelligence collection, communications technology, or any other area that may lend legal or technical expertise."[129] The qualifications ensure that the panel is authoritative and capable of grasping the issues that may come before the court, as well as challenging their decisions. Additionally, and importantly, the paragraph establishes that at least seven members of the body must be attorneys. This enables the panel to have sufficient legal expertise when either advising the court as amici or challenging applications for warrants as intervenors. It is envisioned that, in the event of an intervention, these attorneys would act as counsel for the panel, as the hiring of outside counsel would be very difficult due to the highly classified nature of the proceedings.

In sub-paragraph (B), the paragraph establishes eligibility for a security clearance as a requirement for membership of the panel. This requirement may serve as a limiting factor for some prospective candidates who could provide zealous advocacy in defense of civil liberties during FISC proceedings. Security clearances are issued according to a rigorous process governed by different legal authorities.[130] Given the subject matter sensitivity, it is likely that members will be required to possess high-level clearances (e.g., TS//SCI, or "Top Secret" clearance with access to "Sensitive Compartmented Information") that will require additional procedures, such as a Single Scope Background Investigation.[131] While a potential limitation, this requirement is inevitable and necessary to ensure the proposal is compatible with the interests of national security.

3. Paragraph 4, Right of intervention:

129. *See infra* p. 21.

130. 50 U.S.C. § 3341.

131. *Investigation Types*, U.S. DEP'T OF THE ARMY DEPUTY CHIEF OF STAFF G-2, https://www.dami.army.pentagon.mil/site/PerSec/InvTypes.aspx (last visited Apr. 11, 2025) [https://perma.cc/BN5N-X6RZ].

This paragraph forms the backbone of the proposal, by granting the Panel the right to "intervene in any proceeding of [the FISC] to challenge any petition, application for an order, or motion presented to the court by the United States or any party before the court." In this respect, the Panel enjoys the general rights of litigants before an Article III court, e.g., to gain access to evidence, file motions and briefs, and request a rehearing. Should the FISC not grant their application, they may appeal to the FISCR and, thereafter, seek a writ of certiorari from the Supreme Court.

For the Panel to intervene in matters before the FISC, a majority of its members must deem it necessary. This provision is designed to ensure that the Panel acts as a collective entity and that its power of intervention may be exercised responsibly. The only statutory standard governing the factors the Panel should consider is whether intervention will "advance the protection of individual privacy and civil liberties," and what is reasonable to that end. More specific standards are not elucidated due to the potentially technical nature of such matters, extending beyond the legal discipline. It is best left to the amici to determine specific standards using their expertise on an ad hoc basis.

Unlike previous "public advocate" proposals, this provision grants the Panel discretion in choosing cases upon which to intervene. Chiefly, it ensures efficiency in the FISA process, whereby uncontroversial requests for surveillance need not be deliberately opposed, enabling the panel to focus its efforts on cases where the public interest is more directly implicated.

4. Paragraph 6, Access to information:

This paragraph enables the Panel to access past precedents of the court and other documents that would otherwise be published, to aid it during litigation initiated by intervention. It also empowers members to consult with third parties regarding their duties, subject to the requirement that classified information is only shared with individuals who have a security clearance and/or are otherwise eligible to access it.

5. Paragraph 11, Exception:

> This paragraph concerns the extraordinary circumstance of when a member of the Panel may, themselves, be the target of an application to the FISC for surveillance by the government. In this situation, the ability of the Panel of experts to intervene is foreclosed, due to the significant national security vulnerability if one member of the Panel communicates about their involvement in the case of a targeted member. In such a situation, the whole subsection is deemed inapplicable, and knowledge of an application for a warrant would be withheld from them in entirety. It is foreseen that the FISC will use its discretion in this situation to adjudicate the matter.

6. Paragraph 6, Access to information:

> This paragraph enables the Panel to access past precedents of the court and other documents that would otherwise be published, to aid it during litigation initiated by intervention. It also empowers members to consult with third parties regarding their duties, subject to the requirement that classified information is only shared with individuals who have a security clearance and/or are otherwise eligible to access it.

7. Paragraph 11, Exception:

> This paragraph concerns the extraordinary circumstance of when a member of the Panel may, themselves, be the target of an application to the FISC for surveillance by the government. In this situation, the ability of the Panel of experts to intervene is foreclosed, due to the significant national security vulnerability if one member of the Panel communicates about their involvement in the case of a targeted member. In such a situation, the whole subsection is deemed inapplicable, and knowledge of an application for a warrant would be withheld from them in entirety. It is foreseen that the FISC will use its discretion in this situation to adjudicate the matter.

B. Statutory Basis and Legality of Intervention

Granting a right of intervention to the proposed Panel of Experts in the FISC would not be a "new" framework. Indeed, other statutes grant parties a statutory right of intervention. For instance, under the Fair Housing Act, individuals who are aggrieved by discriminatory practices may intervene in lawsuits commenced by the U.S. government to challenge that practice.[132] The Federal Rules of Civil Procedure ("FRCP"), in Rule 24, allow a party granted either a conditional or unconditional right of intervention by statute

132. *See e.g.*, 42 U.S.C. § 3612(o)(2) (granting parties the right to intervene in Fair Housing Act cases brought by the government).

to participate in a proceeding.[133] The proposed panel would be granted a conditional right, subject to a majority of members deeming intervention necessary under Paragraph (4)(B) of the proposed text.[134] This would conform to the requirements of existing federal rules under the FRCP to make such a framework within precedent. Because FISC proceedings are, presumptively, not criminal in nature,[135] the applicability of the federal civil rules as a standard is appropriate. It should be noted that granting parties statutory rights to participate in FISC proceedings has already been accomplished in Section 702 in the limited circumstance of electronic communications providers petitioning to set aside government directives for compliance with court orders.[136] Due to this circumstance, the FISC's rules of procedure make allowance for adversarial proceedings, which may be borrowed by the Panel of Experts in seeking relief, as proposed, without the creation of substantially new rules to govern their conduct.[137]

However, the similarity does not resolve the issue. The strongest constitutional objections to adversarial participation in the warrant application process are raised in the Congressional Research Service's ("CRS") 2014 report on the matter.[138] The report raises some objections concerning the Appointments Clause, indicating concern about whether a "public advocate" may be a principal officer of the United States, an inferior officer, or non-officer employee.[139] The status of persons appointed by the government in the performance of their duties is certainly a relevant constitutional question that bears upon the performance of their duties.[140] Yet, it is not a question relevant to the proposed framework for a Panel of Experts, none of whom are intended to be permanent or special government employees who may receive a salary drawn from the U.S. Treasury. The Panel of Experts would remain, akin to amici curiae, private individuals who are empowered by statute to participate in FISC proceedings, and would not be compensated for their service. This characteristic avoids the complicated issue of their status under the Appointments Clause, and their designation by the court and discretion over intervention in a matter is facially distinguishable from appointment to a governmental office with statutory duties. While extensive uncompensated service may be a policy concern, the classified nature of the FISC's past jurisprudence make it difficult to predict just how often the Panel's services may be required.

The most potent objection that the report raises to the concept is the matter of standing. Article III of the Constitution requires that parties seeking

133. FED. R. CIV. P. 24(a)(1), (b)(1)(A).

134. *See infra* p. 22.

135. *Foreign Intelligence Surveillance Act (FISA) Part 2 (MP3)*, FED. L. ENF'T TRAINING CTRS., https://www.fletc.gov/audio/foreign-intelligence-surveillance-act-fisa-part-2-mp3 (last visited Mar. 3, 2025).

136. *See* 50 U.S.C. § 1881a(i)(4)(A), *et seq*. Unlike the Panel of Experts, communications providers are an aggrieved entity seeking relief against government, making the circumstances of intervention substantially different.

137. FISA Ct. R. 7(h)-(k), 8(a).

138. *See* NOLAN, ET AL., *supra* note 22.

139. *Id.* at 10.

140. *See* Selia Law v. CFPB, 591 U.S. 197, 204 (2020).

relief from federal courts have standing to bring a case or controversy before the court.[141] The Supreme Court, in *Lujan v. Defenders of Wildlife*, has resolved that, in general, a party seeking relief from federal courts must have a concretized injury that is particular in fact, with damages being actual and imminent if such relief is not granted.[142] The heightened burden includes requirements that the party seeking relief present a "causal connection" between their injury and the government's conduct that is "fairly traceable," and that any relief by the court will sufficiently resolve the injury.[143] Normally, an *ex parte* non-adversarial proceeding before the FISC is akin to those conducted before district judges in criminal cases, is ancillary to an Article III court's powers in[144] cases and controversies. A hypothetical adversarial challenge by the proposed Panel of Experts likely would transform the situation into a form of controversy between them and the government. The CRS report opines that empowering amici to intervene in proceedings, as this proposal seeks to do, would "make an end-run around Article III standing requirements."[145]

A recent case where the Supreme Court addressed the question of whether statutory intervenors require Article III standing was *Town of Chester v. Laroe Estates*.[146] In that case, which involves a complicated dispute over property and a party's intervention, the Court suggests that an intervenor who makes no different a claim from an existing plaintiff need not satisfy the requirements of Article III standing to make an intervention.[147] Applying this framework to a FISC proceeding is challenging because proceedings are both classified and entirely *in camera*; there is certainly an individual, the target[s] of surveillance, who would satisfy standing requirements if seeking to participate, but cannot do so (e.g., due to a lack of a security clearance and national security imperatives of confidentiality). Based on *Chester* jurisprudence, this fact deprives the Panel of Experts of the necessary plaintiff on whose back they may safely intervene in proceedings to block the issuances of FISA warrants.

There is a doctrine of "third party standing" where a plaintiff, suing on behalf of another entity, is granted standing to pursue their claims. In *Singleton v. Wulff*, the Supreme Court ruled that a party may sue to assert the rights of a third party if they have a close relationship with that party and there are "obstacles" to the assertion of that party's rights.[148] Applying this framework to the Panel of Experts, the second condition of obstacles is satisfied in respect of the limitations imposed by the court's classified

141. *See* U.S. CONST., art. III, § 2; *see also* Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

142. *See Lujan*, 504 U.S. at 560.

143. *Id.* at 560-61.

144. Clarke, *supra* note 116, at 17.

145. *Id.* at 25.

146. *See* Town of Chester v. Laroe Ests., 581 U.S. 433, 439-41 (2017).

147. *See id.* ("If Laroe wants only a money judgment of its own running directly against the Town, then it seeks damages different from those sought by Sherman and must establish its own Article III standing in order to intervene.").

148. Singleton v. Wulff, 428 U.S. 106, 107 (1976).

proceedings. The first condition—a close relationship with the party—is not discretely evinced from this case, and the Court's opinion specifies the confidential nature of a doctor-patient relationship as being the basis for its decision.[149]

However, the issue of standing should not limit the proposed framework, for the intervention of the Panel of Experts in FISC proceedings lies within a fundamentally different paradigm than usual "cases or controversies" heard by federal courts. A Panel of Experts, unlike other entities, would not seek any affirmative relief from the FISC and FISCR in a manner that benefits itself. The Panel's only empowerment under the proposed framework is to challenge applications for orders authorizing surveillance under FISA on others, with the relief sought being limited to a denial or modification of the application. These are powers already exercised by the FISC[150], and the Panel of Experts' intervening challenges would merely ask for their exercise to bring governmental action in conformity with FISA. Thus, it would be improper to consider proceedings at the FISC as akin to regular cases or controversies that the federal courts frequently address, for the purpose of determining standing.

Instead, because controversies at the FISC are of a very different nature than regular cases or controversies, a court (and, ultimately, the Supreme Court) should deem the *Lujan* framework inapplicable to evaluating questions of standing for the Panel of Experts and, instead, rule that it satisfies Article III standing on different grounds, such as the notion that the Panel comprises a subset of U.S. persons writ large who, being affected by a general surveillance program, would have standing. There are plausible reasons for doing so, foremost being the exigencies involved. The concept of the Panel of Experts would exist to ensure that the Constitution's safeguards for persons subject to its jurisdiction (i.e., U.S. persons) may be upheld in the FISA warrant process while ensuring that legitimate national security interests are uncompromised. Indeed, in doing so, as the proposed framework reads, to "advance the protection of individual privacy and civil liberties" the Panel can satisfy most of the *Lujan* requirements for standing. They may certainly show a "concretized" injury of surveillance harming privacy and civil liberties of a target, with the injury of such surveillance being "particular" in fact, which would satisfy standing requirements. It may also show that damages to the targets are actual and imminent if such surveillance is to be undertaken, with causal connections between surveillance actions and the targets' damages, also satisfying standing requirements. The only element of the *Lujan* requirements that the Panel of Experts would miss is readily demonstrating the injury to themselves,[151] a necessary requirement to affect standing in cases of a discrete target being surveilled. Indeed, when it comes to the government's programmatic surveillance on a large scale, members of the Panel of Experts may, themselves, have a claim to standing as a subset of a vast class of persons who may be affected by such surveillance. Regarding

149. *Id.* at 115-16.
150. 50 U.S.C. § 1803(a).
151. *See Lujan*, 504 U.S. at 560.

cases of individual surveillance, the courts may recognize the Panel's interventions as Congress' legitimate effort to provide for representation of the interests of U.S. persons—who, for reasons of secrecy, cannot be permitted to participate—as a narrow exception to *Lujan*.

C. Policy Arguments for the Panel's Right of Intervention

Empowering the Panel of Experts to intervene in applications for warrants from the FISC will yield several policy benefits. It is likely that the Panel would improve the FISA process, considerably, as a result of the newfound adversarial nature of applications before the FISC. The adversarial process would unveil new issues for the FISC to consider and ensure that the government's applications were fully scrutinized with the greatest degree of rigor that may be used, akin to suits challenging the government in civil cases. The government would likely be compelled to adopt similar rigor in its curation of programs to ensure legal compliance while also averring from testing the FISC's willingness to expand the government's surveillance authority due to the scrutiny that an empowered Panel of Experts would offer. Over time, the Panel's cumulative experience at litigating at the FISC would progressively deepen the extent of accountability that could be exacted against the government in its FISA applications. This would have especially great benefits for determining the bounds of proposed surveillance's constitutionality, which remains a subject of prime concern to the public.[152] The Supreme Court has opined that "concrete adverseness . . . sharpens the presentation of issues upon which the court so largely depends for illumination of difficult constitutional questions[.]"[153] It has also observed that a system of *ex parte* proceedings is "likely to be less vigorous."[154] When constitutional questions of such gravity affecting millions of U.S. persons are at stake, regarding programmatic surveillance, a "less vigorous" proceeding is insufficient. An empowered Panel of Experts would fill this gap.

IV. CONCLUSION

The current FISA process leaves U.S. persons vulnerable to unconstitutional and unlawful targeting through surveillance by the federal government. Due to the classified nature of matters before the FISC, there are limited opportunities for the public to play a greater role in asserting rights against the government. Congressional action is appropriate, but even Congress's oversight of a classified system, codified since the statute was enacted,[155] has not been sufficient to prevent governmental abuses as well as check public dissatisfaction. What is not needed is yet another external entity

152. *Warrantless Surveillance Under Section 702 of FISA*, ACLU (Sept. 28, 2023, 9:43 PM), https://www.aclu.org/issues/national-security/warrantless-surveillance-under-section-702-fisa [https://perma.cc/NXM5-G92E].

153. *See* Baker v. Carr, 369 U.S. 186, 205 (1962).

154. Franks v. Delaware, 438 U.S. 154, 169 (1978).

155. Foreign Intelligence Surveillance Act of 1978, *supra* note 3, § 108, 92 Stat. at 1795.

to examine the FISC's conduct but, rather, a novel form of participation in the FISA process that reforms it from within. It will bring scrutiny, internally, for accountability of the government. That scrutiny must be adversarial, given the high stakes of constitutional rights. The Panel of Experts can accomplish that task successfully. It must be created to do so.

V. APPENDIX

The proposed statutory language to create a Panel of Experts empowered to intervene in FISA proceedings may be as follows[156]:

> Section 103(i) of the Foreign Intelligence Surveillance Act of 1978 (Public Law 95-511, 50 U.S.C. 1803) is amended by striking all text and replacing it with the following:
>
> (i) PANEL OF EXPERTS AND AMICUS CURIAE. —
>
> (1) DESIGNATION. — The presiding judge of the court established under subsection (b) shall, no later than 180 days after the enactment of this subsection, jointly designate no fewer than 15 individuals to be eligible to serve as members of a Panel of Experts, who shall serve pursuant to rules the presiding judge may establish. In designating such individuals, the presiding judge may consider individuals recommended by any source, including members of the Privacy and Civil Liberties Oversight Board, the presiding judge determines appropriate. Current members of the Panel may submit recommendations to the presiding judges of individuals they deem suitable for any vacancies on the Panel.
>
> (2) AUTHORIZATION. — A court established under subsection (a) or (b), consistent with the requirement of subsection (c) and any other

156. The proposed language is adapted from the amendment of Section 103 of FISA by Section 401 of the USA FREEDOM ACT that creates amicus curiae, with modifications of the legislative language to enable a Panel of Experts with the right of intervention. *See* USA FREEDOM ACT, *supra* note 19.

statutory requirement that the court act expeditiously or within a stated time —

(A) shall appoint an individual who has been designated under paragraph (1) to serve as amicus curiae to assist such court in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate; and

(B) may appoint any individual or organization to serve as amicus curiae, including to provide technical expertise, in any instance as such court deems appropriate or, upon motion, permit an individual or organization leave to file an amicus curiae brief.

(3) QUALIFICATIONS OF EXPERTS. —

(A) EXPERTISE. — Individuals designated under paragraph (1) shall be persons who possess expertise in privacy and civil liberties, intelligence collection, communications technology, or any other area that may lend legal or technical expertise to a court established under subsection (a) or (b). No fewer than seven members of the Panel shall be attorneys and members in good standing of a bar association of a state or territory of the United States.

(B) SECURITY CLEARANCE. — Individuals designated pursuant to paragraph (1) shall be persons who are determined to be eligible for access to classified information necessary to participate in matters before the courts. Amicus curiae appointed by the court pursuant to paragraph (2)(B) shall be persons who are determined to be eligible for access to classified information, if such access is

necessary to participate in the matters in which they may be appointed.

(4) DUTIES. —

(A) If a court established under subsection (a) or (b) appoints an amicus curia under paragraph (2)(A), the amicus curiae shall provide and present to the court—

(i) legal arguments that advance the protection of individual privacy and civil liberties;

(ii) information related to intelligence collection or communications technology; and

(iii) legal arguments or information regarding any other area relevant to the issue presented to the court.

(B) The individuals named in paragraph (1)(A), when a majority of them may deem it necessary, shall have the right to intervene in any proceeding of a court established under subsection (a) to challenge any petition, application for an order, or motion presented to the court by the United States or any party before the court as they deem appropriate to advance the protection of individual privacy and civil liberties. In doing so, they shall[157] —

(i) have the right to participate fully in proceedings of the court, with the same rights and privileges as the Government;

(ii) shall have access to all relevant evidence in such matter and may petition the court to order the

157. The provisions of sub-paragraph (B) are modelled on provisions of the Ensuring Adversarial Process in the FISA Court Act. *See* H.R. 3159, supra note 117, § 2(b).

Government to produce documents, materials, or other evidence necessary to perform their duties;

(iii) may file timely motions and briefs, in accordance with the procedures of the court, and shall be given the opportunity by the court to respond to motions or filings made by the Federal Government in accordance with such procedures; and

(iv) may request a rehearing or en banc consideration of a decision of the court.

(C) Subject to the provisions of paragraph (4)(B), the individuals named in paragraph (1)(A) shall have the right to appeal any decision of a court established under subsection (a) to a court established under subsection (b) after having exercised their right of intervention under paragraph (4)(B).

(D) Subject to the provisions of paragraph (4)(C), if an appeal made under paragraph (4)(C) is denied, the individuals named in paragraph (1)(A) may petition for a writ of certiorari to the Supreme Court, where the record shall be transmitted shall under seal, and which shall have jurisdiction to review such decision and grant relief as it may deem appropriate.

(5) ASSISTANCE. — An amicus curiae appointed under paragraph (2)(A) may request that the court designate or appoint additional amici curiae pursuant to paragraph (1) or paragraph (2), to be available to assist the amicus curiae.

(6) ACCESS TO INFORMATION. —

(A) IN GENERAL. — The individuals named in paragraph (1)(A) —

(i) shall have access to any legal precedent, application, certification, petition, motion of the court and such other materials that the court determines are relevant to the duties of the Panel of Experts; and

(ii) may, if the court determines that it is relevant to the duties of the Panel of Experts, consult with any other individual regarding information relevant to any proceeding, provided that classified information may only be disclosed to other individuals as described in sub-paragraph (C).

(B) BRIEFINGS. — The Attorney General shall brief or provide relevant materials to individuals designated pursuant to paragraph (1) regarding constructions and interpretations of this Act and legal, technological, and other issues related to actions authorized by this Act.

(C) CLASSIFIED INFORMATION. — Individuals designated pursuant to paragraph (1) or amicus curiae designated or appointed by the court may have access to classified documents, information, and other materials or proceedings only if that individual is eligible for access to classified information and to the extent consistent with the national security of the United States.

(D) RULE OF CONSTRUCTION. — Nothing in this section shall be construed to require the Government to provide information to the Panel of Experts or amici curiae appointed by the court that is privileged from disclosure.

(7) NOTIFICATION. — A presiding judge of a court established under subsection (b) shall notify the Attorney General of each exercise of the authority to appoint an individual to serve as amicus curiae under paragraph (2).

(8) ASSISTANCE. — A court established under subsection (a) or (b) may request and receive

(including on a non-reimbursable basis) the assistance of the executive branch in the implementation of this subsection.

(9) ADMINISTRATION. — A court established under subsection (b) may provide for the designation, appointment, removal, training, or other support for an individual designated to serve a member of the Panel of Experts under paragraph (1) or appointed to serve as amicus curiae under paragraph (2) in a manner that is not inconsistent with this subsection.

(10) RECEIPT OF INFORMATION. — Nothing in this subsection shall limit the ability of a court established under subsection (a) or (b) to request or receive information or materials from, or otherwise communicate with, the Government, the Panel of Experts appointed under paragraph (1), or amicus curiae appointed under paragraph (2) on an ex parte basis, nor limit any special or heightened obligation in any ex parte communication or proceeding.

(11) EXCEPTION. — The provisions of this subsection shall not apply to any proceeding where any of the individuals named in paragraph (1)(A) are individually named as targets in an application for an order presented to the court under section 104, and the courts established under subsection (a) or (b) shall withhold information from the individuals in paragraph (1)(A) so long as they are so named."

Striking the Right Enforcement Balance in BIPA-Style Legislation

Lenni Elias*

TABLE OF CONTENTS

* J.D., expected May 2025, The George Washington University Law School; B.A. 2022, Journalism and International Relations, Lehigh University. I extend my utmost appreciation to Professor April Jones, Emily Bernhard and the entire FCLJ editorial board for their guidance throughout the research process. I would also like to thank my close friends, family and long-time boyfriend, Ryan, for their continued support. Your encouragement is responsible for my success.

I. INTRODUCTION

The once futuristic idea of using body parts (biometrics) as a securing mechanism for locked areas or accounts is no longer science fiction, but reality. Industries including finance, information technology, software services, retail, and even government have rushed to adopt biometric capture technologies in recent years.[1] "Biometrics" entails using processes and automated methods to identify and authenticate an individual's identity through measurable behavioral activities and human biological characteristics.[2] Examples of readily used biometric data include iris scans, fingerprint scans, and voice prints.[3]

Biometric data is collected and used for several identifiable reasons.[4] Specifically, companies are keen to implement these technologies because it can augment the consumer retail experience,[5] allow for secure mobile banking,[6] and facilitate convenient air travel.[7] Employers have also rushed to adopt biometric technologies in the workplace to remedy time and attendance issues, ensuring that employees only get paid for the time they actually spend working,[8] and to secure confidential internal systems.[9] Governments use biometrics to identify crime suspects and those crossing national borders.[10]

Inevitably, the popularity and proliferation of biometric capture technologies presents certain dangers.[11] For example, despite great advances in the accuracy of biometric identification technology, there is a heightened risk members of minority groups using these tools will be misidentified, stemming from training issues that can inject systemic bias into biometric systems.[12] In response to increased use of biometric technologies, the general public is concerned that widespread use of these systems will lead to an always-present surveillance state, eroding traditional notions of privacy.[13] Further, if biometric data is compromised, the impacted individual could experience devastating consequences.[14] The victim is unable to remedy the breach in the same way an ordinary victim of a data compromise would be

---

1. *See* Rachel German & K. Suzanne Barber, *Current Biometric Adoption and Trends*, U, TEX. AUSTIN CTR. FOR IDENTITY 2 (Sept. 2017), https://identity.utexas.edu/sites/default/files/2020-09/Current%20Biometric%20Adoption%20and%20Trends.pdf [https://perma.cc/P45T-EYG3].
2. DAVID OBERLY, BIOMETRIC DATA PRIVACY COMPLIANCE AND BEST PRACTICES § 1.01(1) (Matthew Bender ed., 2025).
3. *See, e.g.*, VA. CODE ANN. § 59.1-575 (2021).
4. *See* OBERLY, *supra* note 3 at § 1.03.
5. *Id.* at § 1.03(5).
6. *Id.* at § 1.03(2)).
7. *Id.* at § 1.03(3).
8. *Id.* at § 1.03(6).
9. OBERLY, *supra* note 3, at § 1.03(6).
10. *Biometrics*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/biometrics [https://perma.cc/HZB2-DA89] (last visited Jan. 16, 2024).
11. *See* OBERLY, *supra* note 3, at § 1.02(8).
12. *Id.*
13. *See id.* at § 1.02(9)(a).
14. *Id.* at § 1.02(10).

able to, such as by changing a credit card number or password.[15] The risk of compromise is only exacerbated by the fact that biometrics are intrinsically public as they are a part of you, and you interact with the world at large.[16]

In response to the mass adoption of biometric capture technologies, there has been a development in legislation regulating how biometric data from such technologies is used, collected, retained, and disposed of.[17] Legislation seeks to find a balance between protecting an individual's biometric data while not overburdening companies with compliance requirements, and not forcing companies and courts to handle considerable increases in costly litigation.[18]

This Note explores how states seeking to enact biometric data protection legislation can obtain optimal harmony between vehement enforcement of statutory rights and other practical considerations. It does not inquire into the content of such legislation but rather assumes the statute will include some reasonable means to effectuate the legislative purpose of protecting the biometric data of all of the respective state's citizens. This argument builds on the one set forth by Gabrielle Neace in her Student Note, "Biometric Privacy: Blending Employment Law with the Growth of Technology."[19] In her Note, Neace surveys the intersection between Illinois' Biometric Information Privacy Act ("BIPA") and employment law, and proposes various steps legislative bodies, courts, and employers can take to change the country's biometric data protection scheme for the better.[20] One such suggestion is maintaining BIPA's private right of action, and encouraging newly enacted statutes to include the enforcement mechanism as well.[21] This Note concurs with her assessment of the need for a private right of action in the employment context, but recognizes that implementing a privacy statute with a private right of action is reasonably concerning for states.[22] In other words, BIPA is not perfect and aspects of the law should be changed in newly enacted schemes. Thus, this Note proposes statutory changes to Illinois' scheme that other states can enact to lessen concerns regarding large damage awards and increased litigation while still protecting vulnerable groups. This scheme preserves the importance of a private right of action in the employment context, while making the proposed legal solution more tolerable and efficient for other states.

---

15. *Id.*

16. Andrew Zarkowsky, *Biometrics: An Evolving Industry with Unique Risks*, THE HARTFORD (May 20, 2021), https://www.thehartford.com/insights/technology/biometrics [https://perma.cc/6U4H-W9Q2].

17. *See Updates on Biometrics in the Workplace: Scanning the Legal Landscape in New York and Beyond*, EPSTEIN, BECKER & GREEN, P.C. (Aug. 19, 2021), https://www.ebglaw.com/insights/publications/updates-on-biometrics-in-the-workplace-scanning-the-legal-landscape-in-new-york-and-beyond [https://perma.cc/F6MP-FC2P].

18. *See* Hannah Harper, *Your Body, Your Data, But Not Your Right of Action: Seeking Balance in Federal Biometric Privacy Legislation*, 8 NAT'L SEC. L.J. 85, 112 (2021).

19. Gabrielle Neace, *Biometric Privacy: Blending Employment with the Growth of Technology*, 53 UIC J. MARSHALL L. REV. 73 (2020).

20. *See id.* at 76.

21. *Id.* at 110.

22. *See id.* at 109-110.

The Note proceeds as follows: Section II provides an overview of the current state of affairs pertaining to biometric data in the United States, with Part A surveying the current legislative landscape and Part B outlining how employers use biometric data. Section III supplies an analysis of the proposed legal solution. Section A explains the necessity of the private right of action in the employer-employee relationship, followed by subsections 1 and 2, which analyze how the proposed private right of action will interact with the current employment law landscape and standing requirements, respectively. Section B outlines BIPA's problems and proposes possible solutions. Subsection 1 addresses the concerns regarding class actions brought under BIPA and demonstrates how subjecting consumer harm suits to public enforcement will alleviate accompanying concerns. Subsection 2 describes strategies states can employ to lessen litigation and resulting damages for non-compliant parties. Subsection 3 then compares the legal solution advocated by this Note to other existing proposals.

II. CURRENT STATE OF BIOMETRIC DATA IN AMERICAN LAW AND SOCIETY

A. Current Biometric Data Regulation Legislative Landscape

States have chosen to regulate biometric data through two schemes: biometric data protection-specific legislation and comprehensive privacy legislation.[23] This section will first examine the states that have enacted specific legislation, followed by a description of the states regulating through comprehensive privacy laws.

To date, Washington, Texas, and Illinois have successfully passed legislation protecting only biometric data.[24] While not governing all uses of biometric data, New York, Maryland, and California have laws pertaining to the use of biometric data in the employment context.[25] Certain municipalities have also enacted regulations impacting biometric data.[26] Portland, Oregon prohibits the use of "face recognition technologies in places of public accommodation by private entities within the boundaries of the city of Portland."[27] New York City requires that "any commercial establishment that collects, retains, converts, stores or shares biometric identifier information of customers must disclose such collection, retention, conversion, storage or sharing, as applicable, by placing a clear and conspicuous sign near all of the

23. *Is Biometric Information Protected by Privacy Laws?*, BLOOMBERG L. (May 3, 2023), https://pro.bloomberglaw.com/insights/privacy/biometric-data-privacy-laws/ [https://perma.cc/9RGJ-5AM7].

24. TEX. BUS. & COM. § 503.001 (West 2023); 740 ILL. COMP. STAT. 14/1-14/99 (2024); WASH. REV. CODE §§ 19.375.010-19.375.900 (2024).

25. MD. CODE ANN., LAB. & EMPL. § 3-717 (LexisNexis 2024); N.Y. LAB. LAW § 201-a (LexisNexis 2025); CAL. LAB. CODE § 1051 (Deering 2024).

26. *U.S. Biometric Laws & Pending Legislation Tracker*, BRYAN CAVE LEIGHTON PAISNER LLP (June 2, 2023), https://www.bclplaw.com/en-US/events-insights-news/us-biometric-laws-and-pending-legislation-tracker.html [https://perma.cc/F3ZL-CWD7].

27. *Id.*; PORTLAND, OR., CODE ch. 34.10 (2021).

commercial establishment's customer entrances notifying customers" of such practices.[28] The regulation also makes it unlawful to profit from biometric identifier information.[29]

Other states have chosen to regulate biometric data through comprehensive privacy legislation, regulating biometric data in addition to other types of information.[30] Comprehensive privacy statutes regulate biometric data as "sensitive data," requiring collecting entities to conduct a data protection assessment before processing the sensitive data, and for the purposes of this Note, biometric data.[31] As of April 21, 2025, California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia, successfully passed and signed comprehensive privacy legislation.[32] Only the California, Colorado, Connecticut, Delaware, Iowa, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Texas, Utah, and Virginia laws are in full effect as of February 2025.[33] Despite their broad scope, every state comprehensive privacy law except California exempts employee data collected by an employer from its scope.[34]

Each statute currently in effect, whether specific to biometric data or comprehensive, regulates biometric data slightly differently.[35] Most laws require informing an individual before a business captures a biometric identifier.[36] Each law requires different standards and processes for the collection, use, retention, and destruction of biometric data, the intricacies of which are not necessary to discuss.[37] However, it is important to note that Illinois is widely regarded as having the model law.[38]

---

28. *U.S. Biometric Laws & Pending Legislation Tracker, supra* note 27; N.Y.C. ADMIN. CODE, tit. 22, ch. 12, §§ 22-1201, 22-1202.

29. N.Y.C. ADMIN. CODE, tit. 22, ch. 12, § 22-1202.

30. *See Is Biometric Information Protected by Privacy Laws?*, *supra* note 24.

31. *E.g.*, VA. CODE ANN. § 59.1-575 (2024); VA. CODE ANN. § 59.1-580 (2024.; s*ee also* Benjamin W. Perry et al., *U.S. Continues Patchwork of Comprehensive Data Privacy Requirements: New Laws Set to Take Effect Over Next 2 Years*, OGLETREE DEAKINS (Aug. 6, 2024), https://ogletree.com/insights-resources/blog-posts/u-s-continues-patchwork-of-comprehensive-data-privacy-requirements-new-laws-set-to-take-effect-over-next-2-years/ [https://perma.cc/QCS2-5YD5].

32. Andrew Folks, *US State Privacy Legislation Tracker*, IAPP (Apr. 21, 2025), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/DRP4-YCZ9].

33. *Id.*

34. Müge Fazlioglu, *Workplace Privacy in US Laws and Policies*, IAPP (Oct. 8, 2024), https://iapp.org/news/a/workplace-privacy-in-us-laws-and-policies [https://perma.cc/YT34-D2HU].

35. *Compare* CAL. CIV. CODE § 1798.100(a) (Deering 2024), *with* 740 ILL. COMP. STAT. 14/15 (2024).

36. *E.g.*, TEX. BUS. & COM. § 503.001(b) (2023); COLO. REV. STAT. § 6-1-1308(7) (2024); VA. CODE ANN. § 59.1-578(A)(5) (2024).

37. *Compare* CAL. CIV. CODE § 1798.100(a) (Deering 2024), *with* 740 ILL. COMP. STAT. 14/15 (2024).

38. *See* Joseph Duball, *The rise of US state-level BIPA: Illinois leads, others catching up*, IAPP (Mar. 28, 2023), https://iapp.org/news/a/the-rise-of-us-state-level-bipa- illinois-leads-others-catching-up/ [https://perma.cc/R4LT-UJT5].

The relevant statutes also vary in how the rights granted by the statute are enforced.[39] California and Illinois enforce their statutes through a private right of action.[40] A private right of action is found when a law allows those who have had their statutory rights violated to bring suit directly.[41] California provides a private right of action only to those subject to a data breach involving certain types of personal information, specifically "non encrypted and non redacted personal information" or an "email address in combination with a password or security question and answer that would permit access to the account."[42] An individual may sue if a business fails to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information" resulting in "unauthorized access and exfiltration, theft or disclosure" of the data.[43] Further, an individual can only sue "if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated."[44] If a cure is possible and executed by the offending business within 30 days, and the business provides the consumer with a written statement vowing that no further violations are expected, then no action for statutory damages can be initiated.[45] Any other suit alleging a violation of the California Consumer Privacy Act ("CCPA") which does not involve a data breach affecting the personal information specified above is brought through public enforcement.[46] Illinois is remarkable in that it offers a private right of action, thus any person aggrieved by a BIPA violation can sue in a state circuit court or in federal district court as a supplemental claim.[47]

39. *Compare* CAL. CIV. CODE § 1798.150(a)(1) (Deering 2024), *with* TEX. BUS. & COM. § 503.001(d) (2023).

40. CAL. CIV. CODE § 1798.150(a)(1) (Deering 2024); 740 ILL. COMP. STAT. 14/20 (2024); Cheryl Saniuk-Heinig, *Private Rights of Action in US Privacy Legislation*, IAPP (May 2024), https://iapp.org/resources/article/private-rights-of-action-us-privacy-legislation/ [https://perma.cc/8JJV-P29Y]. Washington's "My Health My Data Act" also includes a private right of action as a violation can be enforced through the state's consumer protection laws. *Id*. It is not considered here as the law focuses on protected health data.

41. Saniuk-Heinig, *supra* note 41.

42. CAL. CIV. CODE § 1798.150(a)(1) (Deering 2024).

43. *Id.*

44. *Id.* § 1798.150(b).

45. *Id.* Further details are provided in this section regarding what constitutes a cure and what type of damages can be sought. *Id.* These details are not necessary to discuss for the purposes of this Note.

46. *Id.* § 1798.199.90.

47. 740 ILL. COMP. STAT. 14/20 (2024).

Other states choose to enforce their statutes through a state attorney general.[48] Public enforcement occurs when a law limits those who can bring suit to state officials.[49] Such officials investigate the afflicted individual or entity's allegations and can then bring suit on behalf of the aggrieved.[50] In Texas, Colorado, and Virginia, for example, suits involving violations of their relevant statute can only be brought by its respective state attorney general.[51] Individuals cannot bring suit directly for violations.[52]

B. Biometric Data in an Employment Context

Biometric data is regularly used by employers.[53] As an example, biometric data allows businesses to conveniently restrict access to certain facilities or areas, allowing for increased access control. [54] Because it is harder to steal, hack, or otherwise compromise biometric data compared to traditional security measures such as passwords or keycards, employers consider biometric capture technologies to be a defensive security measure.[55]

Though beneficial in the employment context, biometric capture technologies also present problems. To comply with a relevant biometric data protection statute, businesses must obtain consent or otherwise inform the affected individual before capturing their biometric data.[56] While impacted employers must inform,[57] employers could make consent to collection of

48. *E.g.*, TEX. BUS. & COM. § 503.001(d) (2023); COLO. REV. STAT. § 6-1-1311(1) (2024); VA. CODE ANN. § 59.1-584(A) (2024); CONN. GEN. STAT. § 42-525(a) (2024); UTAH CODE ANN. § 13-61-402(1) (LexisNexis 2024). Similar to the California statute described above, some of the example statutes provide a cure period. VA. CODE ANN. § 59.1-584(B) (2024); CONN. GEN. STAT. § 42-525(b)(1) (2024); UTAH CODE ANN. § 13-61-402(b) (LexisNexis 2024). If the offending entity does not cure the offense within the given period, the attorney general can bring suit. VA. CODE ANN. § 59.1-584(B) (2024); CONN. GEN. STAT. § 42-525(b)(1) (2024); UTAH CODE ANN. § 13-61-402(b) (LexisNexis 2024). Further intricacies of these provisions are not necessary to discuss for the purposes of this Note.

49. Saniuk-Heinig, *supra* note 41.

50. *See* Ryan Strasser et al., *How Approaches in State Attorney General Actions Differ From Typical Litigation*, REUTERS (Feb. 8, 2023, 12:39 PM), https://www.reuters.com/legal/legalindustry/how-approaches-state-attorney-general-actions-differ-typical-litigation-2023-02-08/ [https://perma.cc/9YF2-N43Q] .

51. TEX. BUS. & COM. § 503.001(d) (2023); COLO. REV. STAT. § 6-1-1311(1)(a) (2024); VA. CODE ANN. § 59.1-584(A) (2024).

52. TEX. BUS. & COM. § 503.001(d) (2023); COLO. REV. STAT. § 6-1-1311(1)(a) (2024); VA. CODE ANN. § 59.1-584(A) (2021).

53. OBERLY, *supra* note 3, at § 1.03(6).

54. *Id.* .

55. See i*d.*

56. *E.g.*, 740 ILL. COMP. STAT. 14/15(b) (2024).

57. *E.g.*, COLO. REV. STAT. §§ 6-1-1308(7), § 6-1-1303(7) (2021). The Colorado statute establishes that a controller must obtain a consumer's consent before processing sensitive (biometric) data. *Id.* § 6-1-1308(7). The statute defines a "controller" as "a person that, alone or jointly with others, determines the purposes for and means of processing personal data. *Id.* § 6-1-1303(7). Thus, an employer could fall within this definition.

biometric data a condition of employment.[58] Thus, employees do not have a meaningful choice when consenting to the collection, retention, and use of their biometric data. The only choice a potential employee would have in such a situation would be to forgo the employment, which may not be a viable option for some, if not most, people. If an employer chooses not to comply with the relevant statute beyond consent, individuals will have little recourse to enforce their statutory rights after essentially being forced into having their data processed through these systems if proper enforcement mechanisms are not in place.

Despite the above assertion that an employer can coerce consent, the United States District Court for the Northern District of West Virginia recognized a situation in which an individual would not have to submit themselves to biometric scans required by an employer.[59] In *United States EEOC v. Consol Energy, Inc.*, Beverly R. Butcher Jr.'s employer installed a biometric hand scanner for tracking employee time and attendance, and required employees to use the scanner for these purposes.[60] Butcher, an Evangelical Christian, held a religious belief that he could not allow either of his hands to be scanned as this would make him take on the "Mark of the Beast."[61] Butcher allegedly informed the defendant employer of his religious belief and suggested two alternatives to the scanner, however the defendant only gave him the option of scanning his left hand palm up instead of right hand palm down.[62] The jury found the Defendants discriminated against Butcher in violation of Title VII, which proscribes employment discrimination on the basis of color, religion, race, sex, and national origin.[63] This suit did not go forward as a violation of any of the biometric-regulating legislation spoken of above, but Title VII would protect any employee working within the United States.[64] *EEOC v. Consol Energy* is somewhat of a 'unicorn' situation because most employees will not have a religious objection to the collection of their biometric data. It is likely most employees across the country will have to submit to biometric scans if their employer uses the technology in the workplace.[65]

---

58. *See* Neace, *supra* note 20, at 101. The article states that "employees may rebel against biometric timekeeping practices and risk losing their employment when they refuse to relinquish their biometric data." *Id.* If an employee can lose their employment by refusing to consent to biometric scans, then it is logical to infer employers can make submission of such data a condition of employment. In New York, an employer cannot make an employee provide their fingerprints as a condition of obtaining or retaining employment. N.Y. LAB. LAW § 201-a (LexisNexis 2025).

59. United States EEOC v. Consol Energy, Inc., 151 F.Supp. 3d 699 (N.D.W. Va. 2015).

60. United States EEOC v. Consol Energy, Inc., No. 1:13CV215, 2015 U.S. Dist. LEXIS 1326, at *2-3 (N.D.W.Va. Jan. 7, 2015).

61. *Id.* at *3.

62. *Id.* at *3-4.

63. *Consol Energy*, 151 F.Supp. 3d at 712; 42 U.S.C. § 2000e-2(a).

64. *Consol Energy*, 151 F.Supp. 3d at 699; 42 U.S.C. § 2000e-2(a); Fazlioglu, *supra* note 35. Further, any dispute concerning an employee's data could not be brought under a comprehensive privacy statute, aside from California, as such data is exempt.

65. Employees in New York will not have to provide fingerprint scans as a condition of employment. N.Y. LAB. LAW § 201-a (LexisNexis 2025).

EEOC v. Consol Energy is the first time in which a court allowed an employee to refuse to provide biometric data to an employer requesting such data.[66] The case is a reminder that employers are still required to consider and comply with relevant civil rights statutes as they implement biometric data capture technologies in the workplace. There could be situations presented in the future in which an employee can rightfully refuse to provide an employer with biometric data if providing such data would conflict with the employee's rights provided by another statute.[67]

With this context in mind, the remainder of this Note will address which enforcement mechanism is best equipped to protect an individual's biometric data without overburdening courts and private entities. The Note will specifically demonstrate why a private right of action should be available to employees who are aggrieved by their employer's violations of relevant biometric data protection statutes. It will also suggest strategies other states can employ to lessen litigation and damage concerns stemming from a private right of action and demonstrate why requiring all other biometric data protection statute violation claims to go through public enforcement will help alleviate central criticisms of BIPA.

III. ANALYSIS

While it is not the purpose of this Note to explain why biometric data protection statutes should be adopted generally, the remainder of this Note rests on the notion that states should enact legislation protecting biometric data from collection to destruction. Biometric technologies are already pervasive and a well-accepted securing mechanism in everyday American life.[68] To put it bluntly, American society may have passed the point of no return when it comes to use of biometric capture technologies. At this time, the focus of legislators should not be on outwardly and explicitly limiting the use of such technologies. It is the law's place to articulate policies and procedures making the use of biometric technologies as safe as possible. This involves both compliance procedures, requiring companies to comply with certain procedures before and while using these technologies, as well as appropriate recourse mechanisms when violations inevitably do occur, which is the focus of this Note. A proper balance must be struck between protecting

66. United States EEOC v. Consol Energy, Inc., No. 1:13CV215, 2015 U.S. Dist. LEXIS 1326 (N.D.W.Va. Jan. 7, 2015).

67. *See generally* Mark Gomsak & Fisher Phillips, *Biometrics and "The Mark of The Beast": Dealing With Employee Accommodation Requests*, JD SUPRA (July 18, 2017), https://www.jdsupra.com/legalnews/biometrics-and-the-mark-of-the-beast-47501/ [https://perma.cc/TP7H-75T4].

68. Previous Apple iPhones include fingerprint scanners and updated models come equipped with technology capable of capturing scans of facial geometry. Because Apple's market share is roughly 25% of the smartphone market, it can be inferred that such technologies are pervasive. *See Apple Grabs the Top Spot in the Smartphone Market in 2023 along with Record High Market Share Despite the Overall Market Dropping 3.2%, According to IDC Tracker*, IDC CORP. (Jan. 15, 2024), https://www.idc.com/getdoc.jsp?containerId=prUS51776424 [https://perma.cc/9TEW-EFBW].

an individual's statutory rights through a private right of action and not overburdening courts and businesses with costly litigation. Further, laws regulating biometric data should ensure that employee data is within its scope as such data warrants protection.[69] This analysis proceeds with the assumption that states will enact statutes that regulate employee biometric data.

Much of the following discussion includes heavy references to Illinois' BIPA. This is because BIPA is the only biometric data protection statute with a private right of action.[70] It is rich in evidence and reasoning to support one prong of the proposed legal solution—to encourage state adoption of a private right of action for employees to sue their employers if their rights are violated under the relevant biometric data protection statute.

For the purposes of the following discussion, I will adopt the Merriam-Webster definition of "employer" and "employee." An employer is "a person or company that provides a job paying wages or a salary to one or more people" and an employee is "one employed by another usually for wages or salary and in a position below the executive level."[71]

The remainder of the analysis consists of two sections. Section A articulates the first prong of the proposed legal solution: to encourage states seeking to enact biometric data protection statutes to incorporate a private right of action allowing employees to sue their employers for statutory violations to protect vulnerable individuals who are susceptible to the mishandling of biometric data. Section B explains the shortfalls of BIPA and how states can remedy these issues when enacting their own legislation.

A. Necessity of the Proposed Private Right of Action

A private right of action for employees whose employers violate their statutory biometric data rights is needed because a majority of cases citing BIPA involve employees alleging violations by their employers.[72] A study conducted by the Chamber of Progress found that eighty-eight percent of lawsuits brought under BIPA involve a timekeeping dispute between employer and employee.[73] This finding leads to the logical prediction that violations by employers of their employee's statutory biometric privacy rights are also regularly violated in other states. But, presumably, suits are not

69. *Infra* Section III.A; Fazlioglu, *supra* note 35. Currently, "all comprehensive U.S. state privacy laws, except the California Consumer Privacy Act, provide a data-level exemption for employee data." *Id.*

70. 740 ILL. COMP. STAT 14/20 (2024); Kirk J. Nahra et al., *Biometric Privacy Law Update*, WILMER CUTLER PICKERING HALE & DORR LLP (Feb. 24, 2023), https://www.wilmerhale.com/en/insights/client-alerts/20230224-biometric-privacy-law-update/ [https://perma.cc/5DXV-LTBQ]. Though this article is from 2023, no further biometric-specific legislation has been passed and enacted since.

71. *Employe*r, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/employer [https://perma.cc/H6QM-VBY9] (last visited Mar. 1, 2025); *Employee*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/employee [https://perma.cc/BCA4-N5N8] (last visited Mar. 1, 2025).

72. Kaitlyn Harger, *Who Benefits from BIPA?*, CHAMBER OF PROGRESS 1 (2023).

73. *Id.*

brought because aggrieved employees lack the ability to sue in states that enforce their statute through public enforcement, or because the state does not have a relevant statute at all.[74] While it is true employees could still complain to a state attorney general if a statute employs public enforcement, there is no guarantee the claim goes any further than this as priorities and functions of an attorney general will vary by jurisdiction.[75]

In addition to the findings of this survey,[76] a private right of action in the employment context is necessary because of a lack of meaningful consent combined with the nature of biometric information and the harm posed by its misuse.[77] To begin, the nature of biometric information and the propensity for harm if the information is misused requires a private right of action.[78] Biometrics are substantially different from social security numbers and other personally identifiable information traditionally used to identify an individual.[79] Biometric data is biologically unique to the individual and cannot be changed in the way a typical password or username can.[80] Once biometric data is compromised, the compromised individual has limited options for recourse as facial geometry, fingerprints, and irises cannot be changed.[81] Because of this, the harm suffered by victims of biometric data breaches/compromises are likely to be more devastating than if another form of information was affected.[82] That individual will have permanently lost their ability to use their person as a secure identifying mechanism and will likely have to withdraw from biometric facilitated transactions forever, which will probably only grow in prevalence.[83]

An example is warranted to illustrate the propensity for harm stemming from compromised biometric data. Imagine that a bad actor obtains access to a facial scan, the original purpose for which was to gain access to an Apple iPhone. The bad actor then uses the scan to gain access to a bank account or another account which is secured with the scan. To remedy the situation to the best of the compromised individual's ability, they would likely have to

---

74. *See, e.g.*, *U.S. Cybersecurity and Data Privacy Outlook and Review – 2023*, GIBSON DUNN, 59-60 (Jan. 30, 2023), https://www.gibsondunn.com/wp-content/uploads/2023/01/us-cybersecurity-and-data-privacy-outlook-and-review-2023.pdf [https://perma.cc/3B9Q-GWW7]. This article, released at the beginning of 2023, states that Texas' Capture and Use of Biometric Identifier Act ("CUBI"), enforced by the state attorney general, has not generated "any meaningful precedent or case law discussing or construing CUBI." This supports the assertion made in the Note that suits are not often brought in states where the relevant biometric data protection statute is enforced by the state attorney general. Notably, Texas' CUBI was enacted in 2009, and the first suit was brought under the statute in 2022.

75. Strasser et al., *supra* note 51. Because state attorney generals are motivated by public policy considerations, priorities and functions will vary as public policy concerns do.

76. Harger, *supra* note 73, at 1.

77. *Infra* Section III.A.

78. *See* OBERLY, *supra* note 3, § 1.03(10). The section speaks on how biometric data differs from other types of personally identifiable data, posing certain risks and challenges. Because of its unique nature, a more inclusive enforcement mechanism is warranted.

79. *Id.*

80. *Id.*

81. *Id.*

82. *Id.*

83. *Id.*; German & Barber, *supra* note 2, at 2.

remove facial recognition as a means for entry on any existing accounts and they would likely not be able to use their face as a means for secure protection of an account in the future.[84] The bad actor already has an existing scan and will have continued access to any accounts set up with facial recognition as a securing mechanism because facial geometry cannot be readily changed.[85] If it was a social security number that was compromised, the compromised individual would simply apply for a new number if the situation requires.[86] Once the compromised individual is provided a new number, the bad actor with the previous social security number has useless data. The compromised individual would not have to withdraw from all future transactions which ask for a social security number as an identifying mechanism, but the individual with the compromised biometric data would likely have to refrain from biometrically secured transactions and provide a different securing mechanism.[87]

The threats posed by compromised biometric data are not mere speculations. The fears about the security risks of inadequately protected biometric data have been realized. In 2019, Customs and Border Protection implemented a facial recognition technology pilot for travelers at U.S. ports of entry.[88] Perceptics, LLC was a subcontractor working on the program.[89] Perceptics "downloaded CBP's sensitive PII [Personally Identifiable Information] from an unencrypted device and stored it on their own network," a direct violation of the Department of Homeland Security's privacy and security protocols.[90] Perceptics fell victim to a cyber-attack, which compromised approximately 184,000 traveler images.[91] "At least 19 of these images were posted to the dark web."[92]

Also in 2019, information obtained from Biostar 2, a web-based biometrics lock system using fingerprints and facial scans to identify people attempting to enter secured buildings, was discovered on a publicly accessible database.[93] Some of the exposed data included personal information about employees of the entities using the security service.[94] When investigating the

84. *See* OBERLY, *supra* note 3, § 1.02(10).

85. *See id.*

86. *Can I change my Social Security Number*, SOC. SEC. ADMIN. (Oct. 7, 2022), https://faq.ssa.gov/en-us/Topic/article/KA-02220# [https://perma.cc/ZG2C-DZXG].

87. *See* OBERLY, *supra* note 3, § 1.02(10).

88. U.S. DEP'T OF HOMELAND SEC. OFFICE OF THE INSPECTOR GEN., OIG-20-71 REVIEW OF CBP'S MAJOR CYBERSECURITY INCIDENT DURING A 2019 BIOMETRIC PILOT 5 (2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf. [https://perma.cc/E97M-GEBR].

89. *Id.* at 3.

90. *Id.* at 5.

91. *Id.* at 6.

92. *Id.*

93. Josh Taylor, *Major breach found in biometrics system used by banks, UK police and defence firms*, THE GUARDIAN (Aug. 14, 2019), https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms [https://perma.cc/S4F7-3HDG].

94. *Id.*

matter, researchers found the data on the Biostar 2 database was "unprotected and mostly unencrypted," allowing access to, and manipulation of, the data.[95]

Employers can also require production of biometric data.[96] If an employer requires an individual to consent to the collection, retention, or use of biometric data as a condition of employment,[97] arguably the individual lacks any form of meaningful consent. Employment is necessary for an individual and their family's financial stability, and it is unrealistic to believe the average person can refuse a job because of a company's biometric data policies. When submitting to employment under these circumstances, an employee is relatively powerless, relying on the employer's efforts to comply with a relevant statute. If an employer fails to adequately comply and there is no private right of action, the employee has compromised data and can only hope their respective state's attorney general takes the case, once again, assuming the state has a privacy law in place that does not exempt employee data.[98]

In the likely event an employee must consent to the biometric capture practices of their employer, the employee may try to void the consent to rid themselves of the obligation. One such theory to do so is unconscionability. To adequately allege unconscionability there must be both procedural and substantive unconscionability, assessed on a sliding scale.[99] An unconscionability analysis entails deciding whether the means by which the parties entered into an agreement or the actual terms of the agreement are so unfairly one-sided that it should not be upheld by the courts.[100] There is nothing one-sided about an employer asking an employee to use biometric capture technologies, thus this theory is likely to fail.

The above discussion shows there are few means through which an employee can have any meaningful control and right over their biometric data absent a private right of action. The recommended private right of action will have a dual effect; it will allow individuals to vindicate their rights in court, thus protecting the very information the statute is designed to protect. In turn, the prospect of litigation will likely entice employers to comply with the terms of the relevant statute to avoid litigation.

1. Interaction Between the Proposed Legal Solution and the American Employment Law Landscape

Because the proposed legal solution involves the employer-employee relationship, it is necessary to consider how a private right of action granted to an employee to vindicate biometric data rights against an employer interacts with other aspects of the employment law landscape. States have

95. *Id.*
96. *See infra* note 59.
97. *See* Neace, *supra* note 20, at 101.
98. Fazlioglu, *supra* note 35.
99. Copper Bend Pharm., Inc. v. OptumRx, NO. 5-22-0211, 2023 Ill. App. Unpub. LEXIS 558, at *41 (5th Cir. 2023).
100. *Id.* at *41, *49.

enacted Workers' Compensation Acts ("WCA"), which provide monetary compensation to employees who "become injured or disabled while working at their jobs."[101] In Illinois, the relevant WCA ordinarily "provides the exclusive means by which an employee can recover against an employer for a work-related [sic] injury."[102] However, an employee can recover against an employer outside the bounds of the WCA if the employee can show that the injury suffered by the employee was not compensable under the WCA.[103]

An employee's claims against an employer alleging a violation of BIPA will not be preempted by a WCA.[104] The Illinois Supreme Court considered this question in *McDonald v. Symphony Bronzeville Park, LLC* and held that an employee's loss of privacy rights resulting from a BIPA violation is not a psychological or physical injury compensable under the WCA, thus the exclusive-remedy provisions of the WCA did not preempt the employee's lawsuit.[105] Each state has a WCA which does differ slightly, however, the differences regard which types of employees are covered under the Act, not the type of injuries covered.[106] Thus, any injuries arising from a violation of biometric data protection legislation is unlikely to be preempted by any state WCA.

BIPA has also come into conflict with the Labor Management Relations Act ("LMRA"), specifically Section 301.[107] This section states that "suits for violation of contracts between an employer and a labor organization representing employees in an industry affecting commerce as defined in this chapter, or between any such labor organizations, may be brought in any district court of the United States having jurisdiction of the parties, without respect to the amount in controversy or without regard to the citizenship of the parties."[108]

The Illinois Supreme Court decided whether the LMRA preempted BIPA claims in *Walton v. Roosevelt Univ*.[109] Walton filed a class action suit against his former employer, Roosevelt University, after the school implemented a hand scan system, alleging that the University's biometric data practices violated BIPA.[110] In the complaint Walton disclosed that neither himself nor any similarly situated employee provided consent to or had any knowledge of the University's biometric retention policies, including "the specific purpose or length of time for which his biometric information was

101. *Workers Compensation*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/workers_compensation [https://perma.cc/XM4Q-MC7F] (last visited Jan. 12, 2024); Jeffrey Johnson, *Workers' Compensation Laws By State (2025 Guide)*, FORBES, https://www.forbes.com/advisor/legal/workers-comp /workers-compensation-laws/ [https://perma.cc/3EK5-34BC] (last updated Nov. 21, 2022, 6:03 AM).

102. McDonald v. Symphony Bronzeville Park, LLC, 193 N.E.3d 1253, 1264 (Ill. 2022) (quoting Folta v. Ferro Eng'g, 43 N.E.3d 108, 113 (Ill. 2015)).

103. *Id.*

104. *Id.* at 1267-68.

105. *Id.*

106. Johnson, *supra* note 102.

107. Walton v. Roosevelt Univ., 217 N.E.3d 968, 970 (Ill. 2023).

108. 29 U.S.C. § 185(a) (1947).

109. *Walton*, 217 N.E.3d at 970.

110. *Id.*

being stored."[111] The University responded by alleging Walton's BIPA claims were preempted by Section 301 of the LMRA as Walton was a member of a collective bargaining unit and thus agreed to a collective bargaining agreement between the University and the organization to which he belonged.[112] Roosevelt argued the agreement's broad management-rights clause covered issues regarding the manner in which an employee clocks in or out.[113] The Illinois Supreme Court agreed with Roosevelt and aligned with two Seventh Circuit cases which decided Section 301 of the LMRA preempted BIPA claims, thus Walton's claims could not be brought under BIPA in court.[114]

In practice, Walton prevents unionized employees covered by broad management rights clauses from bringing BIPA claims against their employers in state or federal courts.[115] Instead, they must comply with the grievance process articulated in their collective bargaining agreement.[116] However, the Walton decision is unlikely to hinder the flow of BIPA litigation because of low unionization rates amongst U.S. workers.[117]

2. Interaction Between the Proposed Legal Solution and Standing Requirements in State and Federal Courts

Because the proposed private right of action for employees will generate litigation, it is also necessary to consider how the proposed legal solution fits with standing requirements imposed by state and federal courts. In order for a private right of action to work, the afflicted individual must have standing to sue.[118] The Illinois Supreme Court considered what constitutes an aggrieved party and an actual injury entitled to relief under

111. *Id.*
112. *Id.* at 970-71.
113. *Id.* at 971.
114. *Walton*, 217 N.E.3d at 975.
115. Sang-yul Lee et al., *Biometric Claims by Workers Covered by Collective Bargaining Agreements are Preempted in Illinois*, K&L GATES (Apr. 20, 2023), https://www.klgates.com/Biometric-Claims-by-Workers-Covered-by-Collective-Bargaining-Agreements-are-Preempted-in-Illinois-4-20-2023 [https://perma.cc/Y6UN-MNDV]*; see also* Maveric Searle & Matthew Wolfe, *Walton v. Roosevelt University: An Illinois Supreme Court BIPA Win*, JD SUPRA (Mar. 29, 2023), https://www.jdsupra.com/legalnews/walton-v-roosevelt-university-an-1309661/ [https://perma.cc/CQ6J-D3V3]
116. Searle & Wolfe*, supra* note 116.
117. Daniel Wiessner, *Union workers can't sue under Illinois biometric law, court rules*, REUTERS (Mar. 23, 2023, 1:41 PM), https://www.reuters.com/legal/union-workers-cant-sue-under-illinois-biometric-law-court-rules-2023-03-23/ [https://perma.cc/K3SQ-EJQN]; *see Union Members in Illinois – 2023*, U.S. BUREAU OF LABOR STATISTICS (2023), https://www.bls.gov/regions/midwest/news-release/2024/unionmembership_illinois_20240207.htm [https://perma.cc/3UEP-LD8A]. In Illinois, 12.8% of employed wage and salary workers are members of unions, and 13.6% of employed wage and salary workers are represented by unions in 2023. Illinois has greater union membership than the national average, which lies at 10%. *Id.*
118. *Standing*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/standing (last visited Apr. 9, 2025).

BIPA in *Rosenbach v. Six Flags Entm't Corp*.[119] BIPA articulates that any person who is "aggrieved" by a BIPA violation can sue the offending party in court and "recover for each violation."[120] In this case, the Illinois Supreme Court found that BIPA protects the interests of Illinois residents by "imposing safeguards to insure that individuals' and customers' privacy rights in their biometric identifiers and biometric information are properly honored and protected to begin with, before they are or can be compromised" and "subjecting private entities who fail to follow the statute's requirements to substantial potential liability."[121] The Illinois Supreme Court concluded an individual is aggrieved by a BIPA violation whenever a private entity fails to comply with a BIPA requirement because the violation impairs the statutory rights of the aggrieved individual.[122] Individuals vindicating their rights granted by BIPA do not have to wait for a compensable injury to occur before seeking legal recourse.[123] Thus, BIPA violations, without more, are sufficient to fulfill standing requirements in Illinois state court.[124]

Federal courts rely on Article III standing to determine whether a particular individual can sue.[125] "First, the plaintiff must have suffered an 'injury in fact,' an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not 'conjectural' or 'hypothetical.'"[126] Violations of a biometric data protection law would create an intangible harm because the harm is that the data has been compromised. In deciding whether an intangible harm is enough to attain Article III standing, courts look to both history and the judgment of Congress to determine whether an intangible harm is an injury in fact.[127] Courts turn to history because it is "instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[128] Further, congressional judgment must be considered because Congress may "elevate to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law."[129] However, the plaintiff does not always meet the injury-in-fact requirement just because a "statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right" because "Article III standing requires a concrete injury even in the context of a statutory violation."[130] But, violation of a statutory right that protects against a risk of real harm may nonetheless fulfill the concreteness

119. Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1202 (Ill. 2019).
120. *Id.* at 1199 (quoting 740 ILL COMP. STAT. 14/20 (2024)).
121. *Id.* at 1206-07.
122. *Id.* at 1206.
123. *Id.* at 1207.
124. *Rosenbach*, 129 N.E.3d at 1206-07.
125. *ArtIII.S2.C1.6.1 Overview of Standing*, CONST. ANNOTATED, https://constitution.congress.gov/browse/essay/artIII-S2-C1-6-1/ALDE_00012992/ [https://perma.cc/H8LT-293Z] (last visited Apr. 7, 2024).
126. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).
127. Spokeo, Inc. v. Robins, 578 U.S. 330, 340 (2016).
128. *Id.* at 341.
129. *Id.* (quoting Lujan v. Defs. of Wildlife, 504 U.S. 578 (1992)).
130. *Id.* at 341.

requirement; under these circumstances, the plaintiff "need not allege any additional harm beyond the one Congress has identified."[131]

The Ninth Circuit considered the issue of Article III standing in the context of BIPA violations in *Patel v. Facebook, Inc*.[132] The case was an action brought by Facebook users claiming its facial recognition technology violated BIPA Section 15(a) and 15(b), prompting the court to use a two-step approach to "determine whether the violation of a statute causes a concrete injury."[133] In deciding whether plaintiffs have Article III standing, the court considered whether the statutory provisions at issue were enacted to safeguard the plaintiff's concrete interests or if the provision is purely procedural.[134] If designed to safeguard concrete interests, the court asked "whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests."[135] In regard to the history aspect of the concrete injury analysis, the court declared that privacy rights have long been vindicated in English and American courts, as it is strongly rooted in common law.[136] Turning next to the legislative judgment portion of the analysis, the court looked to *Rosenbach v. Six Flags Entm't Corp* (the details of which are presented above), leading the court to conclude that 'the statutory provisions at issue' in BIPA were established to protect an individual's 'concrete interests' in privacy, not merely procedural rights."[137] For the harm analysis, the Court again looked to *Rosenbach* in which the Supreme Court of Illinois explained BIPA's procedural protections are especially critical because a private entity failing to adhere to BIPA's procedures results in the individual's total loss of the right to maintain their biometric data.[138] The general conclusion of the court was that the "plaintiffs have alleged a concrete injury-in-fact sufficient to confer Article III standing."[139]

The Seventh Circuit came to a similar conclusion in *Bryant v. Compass Grp. USA, Inc*. when it decided a violation of BIPA Section 15(b) created a concrete and particularized invasion of personal rights, conferring Article III standing on the individual whose statutory rights were violated.[140] Though the Bryant court declined to find a violation of BIPA Section 15(a) as Bryant

131. *Id.* at 341-42.
132. Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019).
133. *Id.* at 1268, 1270.
134. *Id.* at 1270.
135. *Id.* at 1270-71 (quoting Robins v. Spokeo, Inc., 867 F.3d 1108, 1113 (2017)).
136. *Id.* at 1271.
137. *Patel,* 982 F.2d at 1274 (quoting *Spokeo*, 867 F.3d at 1113).
138. *Id.*
139. *Id.*
140. Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 619, 626 (7th Cir. 2020). The Seventh Circuit reasoned that Compass's noncompliance with BIPA Section 15(b) when obtaining biometric identifiers, the statute's informed consent provision, "denied Bryant and others like her the opportunity to consider whether the terms of that collection and usage were acceptable given the attendant risks." *Id.* at 626. "Compass withheld substantive information to which Bryant was entitled and thereby deprived her of the ability to give the *informed* consent section 15(b) mandates." *Id.* However, the Court declined to find standing with respect to Bryant's Section 15(a) claims because this provision simply requires a private entity to publicly disclose certain information and Bryant alleged "no particularized harm that resulted from Compass's violation of section 15(a)." *Id.*

alleged no particularized harm stemming from Compass' failure to publicly disclosure biometric retention and destruction schedules, a subsequent Seventh Circuit case found such standing.[141] However, in *Santana v. Take-Two Interactive Software, Inc.*, the Second Circuit held a game developer's BIPA violations did not confer Article III standing on the respective plaintiffs because the procedural violations alleged involved only a slight divergence from BIPA's requirements which did not raise a material risk of harm.[142] While the Second Circuit drew a different conclusion, it is important to note the facts of this case represented only minimal BIPA violations.[143] For example, the facts of *Santana* involve the plaintiff alleging that a facial scan was collected and disclosed without their consent, however it was undisputed that the game required a face scan which would be publicly accessible by other players.[144] Further, even though the captured data was stored in a less-than-secure way, plaintiffs could not show that this may result in an injury.[145] This differs markedly from the facts of *Patel* in which Facebook created and retained face templates of the class members.[146] Nonetheless, a circuit split exists regarding whether a procedural violation of BIPA can confer Article III standing on a plaintiff.[147]

After all of these cases were already decided, the Supreme Court heard *TransUnion LLC v. Ramirez*, which narrowed Article III precedent in the context of privacy and technology cases.[148] TransUnion falsely included an alert on credit reports of at least 8,185 individuals that they were a "'potential match' to a name on the OFAC [U.S. Treasury Department's Office of Foreign Assets Control of terrorists, drug traffickers and other serious criminals] list."[149] This prompted those whose credit reports included the false designation to sue TransUnion under the Fair Credit Reporting Act for failing to implement reasonable mechanisms to ensure the truthfulness of credit reports.[150] The Court held only those who suffered a concrete harm fulfilled the Article III standing requirements, thus those individuals who could show the false credit reports were provided to a third party had standing to sue while individuals who could not provide such evidence could not sue.[151]

The Supreme Court's *TransUnion LLC* decision appears to come into conflict with the aforementioned Seventh and Ninth Circuit decisions. The

141. *Id.* at 626; Fox v. Dakkota Integrated Sys., LLC, 980 F.3d 1146, 1149 (7th Cir. 2020). In *Fox*, the Seventh Circuit found that Dakkota's failure to comply with BIPA Section 15(a) resulted "in the wrongful retention of her biometric data after her employment ended, beyond the time authorized by law," allowing Fox to sufficiently plead an injury in fact. *Id*. at 1149.

142. Santana v. Take-Two Interactive Software, Inc., 717 Fed. Appx. 12, 16 (2d Cir. 2017).

143. *See, e.g.*, *id.* at 15-16.

144. *Id.* at 15.

145. *Id.* at 16.

146. *Patel*, 932 F.3d at 1268.

147. *Id.*, 932 F.3d at 1274; *Santana*, 717 Fed. Appx. at 17; *Bryant*, 958 F.3d at 626.

148. TransUnion LLC v. Ramirez, 594 U.S. 413, 417 (2021).

149 *Id.* at 417, 420.

150. *Id.* at 417.

151. *Id.* at 438-39.

Patel and *Bryant* decisions apply a more permissive interpretation of concrete and particularized harm allowing mere violations of BIPA to establish Article III standing,[152] while TransUnion finds that concrete and particularized harm is only present when there is more than just a risk of future harm.[153] Despite the conflict, the TransUnion decision is not fatal to BIPA claims premised on strict violations. Plaintiffs can bring suits in state court where the *Rosenbach* precedent dictates that allegations of mere violations of BIPA are enough to move forward in the litigation process.[154]

Speaking to other state courts, courts sitting in other states do not have to interpret their state's relevant statute in the same way the Illinois courts have interpreted their own. However, the conclusion drawn by the *Rosenbach* court shows there is a means through which state courts can allow litigation premised on mere violations of a biometric data protection statute to continue.[155] To allow the private right of action to accomplish its purpose, states are encouraged to follow the Illinois approach and allow individuals standing to sue for violations, providing a strong incentive for entities to comply with the state's statute to avoid litigation.

B. Addressing Concerns Stemming from Emulating Illinois' BIPA

1. Concerns Regarding BIPA Class Actions

An all-encompassing private right of action, like in BIPA, may deter the adoption of biometric capture technologies, particularly by smaller companies or organizations, because the risk of litigation resulting from a mistake in the deployment and continuation of its technology is simply too much to bear. It can even be said that a private right of action available to a smaller class of violations could have the same effect. This is not necessarily a bad thing. If a smaller company does not have the resources to deploy compliant biometric capture systems and cannot carry the cost of litigation, then arguably it should not have the system at all. There are risks inherent in using and collecting biometric data, and it is wise for companies that cannot adequately handle such data and its risks to forgo adoption of these technologies. While useful, the services provided by biometric capture technologies can be easily replaced by other systems without sacrificing function, though admittedly such systems are potentially less convenient or less secure.[156]

---

152. *Patel*, 932 F.3d at 1271, 1274; *Bryant*, 958 F.3d at 621.
153. *TransUnion LLC*, 594 U.S. at 434-35.
154. *Rosenbach*, 129 N.E.3d at 1207.
155. *See generally id.*
156. An example of a replacement system is a physical punch card system used for timekeeping, as opposed to a biometric scanner. Though this system would allow 'buddy punching' to continue, the two systems both adequately serve a timekeeping function. Allison Catalani, *From punch cards to biometrics: Exploring different types of time clocks*, TIMECLOCK PLUS, LLC (TCP SOFTWARE) (June 20, 2024), https://tcpsoftware.com/blog/time-clocks/ [https://perma.cc/B8HR-UHJV0].

Further, private rights of action are often viewed with some skepticism because they can read as dollar signs for aggressive plaintiff's lawyers.[157] A study conducted by the Chamber of Progress focusing on BIPA class actions alleging consumer harm found that in "eight BIPA case settlements involving alleged harm to consumers, plaintiffs' lawyers received an average settlement of $11.5 million per firm per case, while individuals received an average payment of just $506 per case."[158] It is important to note that this study focused almost exclusively on BIPA class actions alleging consumer harm, and did not consider similar BIPA class actions involving employer-employee disputes.[159] The study eventually concludes that, based on payment amounts, BIPA benefits plaintiff's lawyers more than it does the aggrieved consumers.[160] The situation presented by the study is likely representative of at least some of the concerns other states have with emulating BIPA's scheme, and rightfully so.

Across all class action suits, there is a 24.44% average attorney fee maximum in federal court and a 32.33% maximum in state court.[161] The attorney fee share maximum of the eight settlements studied range from twenty percent to forty percent, with the average being thirty four percent.[162] While the researcher noted the attorney fee caps are generally higher on average in Illinois state courts than in those cases removed to or filed in federal courts, aligning with the percentage differences seen between attorney's fees awarded in federal and state court, the average presented by the study is higher than that for federal and state courts.[163] Thus, states may fear a private right of action will not truly protect biometric data, but line the pockets of plaintiff's lawyers.

All the suits investigated in this portion of the research project involved consumer harm,[164] and thus these suits would be brought via public enforcement under the second prong of the proposed legal solution. The concerns regarding fee shares for plaintiff's lawyers and settlement amounts are not necessary to discuss further because other states can rest assured the problems identified in these suits would never come to fruition. Such suits would never privately reach the courts if the state's relevant statute only allows a private right of action for violations within the employer-employee relationship.

However, under the proposed legal solution, employees not subject to collective bargaining agreements remain able to bring class action BIPA suits

157. *What Is a Private Right of Action*, U.S. CHAMBER OF COM. INST. OF LEGAL REFORM (May 15, 2024), https://instituteforlegalreform.com/blog/what-is-a-private-right-of-action/ [https://perma.cc/8A8B-6DPM]. "PRAs can lead to litigation abuse because plaintiffs' lawyers are financially incentivized to file as many lawsuits as possible, placing monetary gain over property addressing potential harms." *See* Harger, *supra* note 73.

158. Harger, *supra* note 73at 1.

159. *Id.* at 9.

160. *Id.* at 20-21.

161. *Id.* at 17.

162. Harger, *supra* note 73, at 17.

163. *Id.*

164. *Id.* at 9.

against their employers.[165] That being said, the continuation of employment-related class action litigation should be tolerated by states because of the nature of the employer-employee relationship and the immense harm that can stem from biometric data mishandling and misuse described throughout this Note.[166] Allowing these suits to go forward via a private right of action furthers the legislature's purpose of protecting biometric data as eighty eight percent of BIPA cases involve employees alleging BIPA violations against their employers.[167] If states want to enact laws that allow their citizenry to have greater agency and control over the capture and use of their own biometric data, then it is counterintuitive to construct a law which prohibits the group experiencing the most violations from seeking independent recourse in court. Further, this solution does not intend to eliminate all BIPA class action or other litigation but rather posits a way to lessen the amount of it and strike a more optimal enforcement balance than is currently felt. By channeling an identifiable group of cases (namely, all those suits not involving an employer-employee dispute) through public enforcement, Illinois courts will experience less litigation overall.

2. Lessening Litigation and Resulting Damages

Recognizing that BIPA was generating large damage awards, the Illinois legislature statutorily overruled the Illinois Supreme Court's *Cothron v. White Castle* decision in August 2024.[168] In *Cothron,* the Court held that each time biometric data is collected in violation of BIPA, a separate claim accrues under BIPA.[169] For example, if an individual scanned their palm five times without consent, this would be five BIPA violations under *Cothron*.[170] From the decision in February 2023 until the August 2024 amendment, *Cothron* facilitated large damage awards because each misstep by an offending business could be amplified if data was obtained incorrectly multiple times.[171]

To limit these awards, Illinois amended BIPA Section 15(b).[172] The section now provides "a private entity that, in more than one instance,

---

165. Searle & Wolfe*, supra* note 116. The Walton v. Roosevelt University court held that a collective bargaining agreement containing a broad management rights clause may preempt a BIPA claim, and any dispute should be dealt with in accordance with the collective bargaining agreement. *Id.* Thus, if an employee is not subject to a collective bargaining agreement, they should be able to pursue a BIPA claim in court.

166. *See supra* Section III.A.

167. Harger, *supra* note 73, at 1.

168. *BIPA Update: Illinois Limits Liability and Clarifies Electronic Consent for Biometric Data Collection,* GREENBERG TRAURIG, LLP (Aug. 14, 2024), https://www.gtlaw.com/en/insights/2024/8/bipa-update-illinois-limits-liability-and-clarifies-electronic-consent-for-biometric-data-collection [https://perma.cc/9PGN-XWT4].

169. Cothron v. White Castle Sys., 216 N.E.3d 918, 920 (Ill. 2023).

170. *See id.*

171. *See* Duball, *supra* note 39.

172. David Stauss, *BIPA Amendment Bill Signed into Law*, HUSCH BLACKWELL LLP (Aug. 4, 2024), https://www.bytebacklaw.com/2024/08/bipa-amendment-bill-signed-into-law/ [https://perma.cc/9722-7VEY].

collects, captures, purchases, receives through trade, or otherwise obtains the same biometric identifier or biometric information from the same person using the same method of collection in violation of subsection (b) of Section 15 has committed a single violation of subsection (b) of Section 15 for which the aggrieved person is entitled to, at most, one recovery under this Section."[173] Thus, multiple violative scans of the same biometric information now amounts to one violation of BIPA.[174] States looking to enact biometric data protection legislation should follow suit, including a similar provision in their law. This could reduce the number of suits reaching the courts, and if a suit does get litigated in court, it would reduce the amount of damages the offending company is liable to pay. In terms of specific damages, the court could also be allowed some discretion in determining damages—if violations repeatedly occur, courts can choose to provide the affected individual with higher damages.

Further, as mentioned throughout the Note thus far, to eliminate other state's concerns of purely increased litigation, the statute could mandate that those suits falling outside of the employer-employee relationship are brought via public enforcement.[175] This would lessen the amount of litigation reaching the courts. In practice, the suits litigated by state attorneys general would involve consumer harm.[176] State attorneys general already have a pronounced role in the nation's privacy enforcement landscape, exercising their role as consumer protection advocates.[177] This compromise would allow public enforcement to continue fulfilling this role, lessening private litigation and ensuring that employer-employee violations are able to reach enforcing entities in an expedient manner.

3. Adequacy of This Solution Compared to Other Existing Proposals

Several scholars have already commented on the enforcement balance they believe is adequate in the biometric data privacy realm. A University of Illinois Law Review Student Note authored by Emma Graham argued that BIPA's private right of action should be limited to Section 15(d) of the statute so as to limit the number of lawsuits going forward alleging violations of the Act.[178] Graham argued that the considerable litigation that went forward after

173. *Id.*; 740 ILL COMP. STAT. 14/20 (2024).

174. Stauss, *supra* note 173. BIPA Section 15 is the substantive provision of the law, providing the requirements a private entity must comply with when handling biometric identifiers or information. 740 ILL COMP. STAT. 14/15 (2024).

175. *See supra* Section III.A-III.B.1.

176. Harger, *supra* note 73, at 16. In Harger's study, she states eighty-eight percent of BIPA litigation involves biometric timekeeping disputes between employer and employee, while the remaining twelve percent allege consumer harm. *Id.*

177. *Enforcing U.S. Consumer Data Privacy Laws Part 2: State Attorney General Enforcement*, PIERCE ATWOOD LLP (May 16, 2023), https://www.pierceatwood.com/alerts/enforcing-us-consumer-data-privacy-laws-part-2-state-attorney-general-enforcement [https://perma.cc/R6LA-KTW2].

178. Emma Graham, *Burdened by BIPA: Balancing Consumer Protection and the Economic Concerns of Businesses*, 2022 U. ILL. L. REV. 929, 957 (2022).

2015 burdened companies who were obliged to defend or settle massive lawsuits, resulting in economic and efficiency losses.[179] It is important to note that from 2015 to 2022, when this Note was written, there was an increase in litigation under BIPA.[180] It remains to be seen whether litigation will decrease in coming years.[181]

Further, there is nothing in the literature to suggest that companies against whom suits are brought cannot comply with the terms of BIPA, only that such companies are not complying.[182] As the Court said in *Rosenbach*, "[c]ompliance should not be difficult; whatever expenses a business might incur to meet the law's requirements are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded."[183] Why should companies not have to properly safeguard biometric data, as instructed by BIPA, when they have the resources and ability to comply with the statute? Additionally, if a company does not have the resources to comply, why is it using biometric capture technology?

As has been established throughout this Note, Gabrielle Neace's proposed solution for other states—articulated in her Student Note, "Biometric Privacy: Blending Employment with the Growth of Technology,"—goes too far.[184] We both agree that employees are especially vulnerable to biometric data mishandling, and that a private right of action presents certain advantages.[185] However, a central concern regarding BIPA-style statute adoption elsewhere is that a permissively interpreted privacy statute with a private right of action will lead to more litigation than tolerable.[186] Thus, allowing all violation claims to be brought directly in court through a private right of action is likely not desirable or acceptable for other states. A simple way to lessen litigation stemming from the statute could be to require all BIPA claims falling outside the employer-employee relationship

---

179. *Id.* at 931-33.

180. *Shepard's Comprehensive Report: 740 Ill. Comp. Stat. 14/15*, LEXISNEXIS, https://plus.lexis.com/shepards/shepardspreviewpod/?pdmfid=1530671&crid=b3abb06e-39f3-45f3-8083-61495f6f5d7b&pdshepid=urn%3AcontentItem%3A805P-VC50-Y87G-F45T-00000-00&pdshepcat=citingref&pddoctabclick=true&prid=986d600b-fe6d-479c-b497-53e8ce85e85a&ecomp=2gntk#/citingref [https://perma.cc/E5K2-NEGD] (last visited Apr. 11, 2025 at 8:36 AM). Sixty-three cases citing BIPA Section 15 were decided by courts in 2022, and lower numbers in years before that. *Id.* Fifty-two and sixty-one cases citing BIPA Section 15 were decided by courts in 2023 and 2024, respectively. *Id*. Thus, the amount of BIPA litigation heard by courts could be trending downwards.

181. *Id.*

182. *See generally Employers Take Heed: Follow Illinois Biometric Privacy Rules or Risk a Losing Battle*, EPSTEIN BECKER & GREEN, P.C. (Feb. 16, 2022), https://www.ebglaw.com/insights/publications/employers-take-heed-follow-illinois-biometric-privacy-rules-or-risk-a-losing-battle [https://perma.cc/9ZL2-YYKQ]. Because law firms are offering its services to help impacted companies comply with BIPA's requirements, it can be inferred that compliance is possible.

183. *Rosenbach*, 129 N.E.3d at 1207.

184. Neace, *supra* note 20.

185. *Id.* at 109-10.

186. *A Bad Match: Illinois and the Biometric Information Privacy Act*, ILR BRIEFLY 2 (Oct. 2021), https://instituteforlegalreform.com/wp-content/uploads/2021/10/ILR-BIPA-Briefly-FINAL.pdf [https://perma.cc/9EKU-23WS].

to be brought via public enforcement. While it is not the purpose of the Note to advocate for public enforcement of a biometric data protection statute, it can be said that state attorneys general are well equipped to build substantial and comprehensive cases against other violating parties.[187] Most of these other suits involve allegations of consumer harm.[188] In their public advocacy roles, attorneys general tend to intervene and litigate impactful cases in which the defendant has regularly offended the statute, producing wide-reaching effects.[189] From this observation, it can be understood that suits brought by attorneys general are unlikely to concern potentially low profile and often occurring violations by employers, which are where the majority of the violations occur.[190] The correct balance is struck when employees are able to privately enforce their statutory rights against their employers, and suits alleging consumer harm are channeled through public enforcement.

IV. CONCLUSION

As biometric technologies increase in use, states must enact statutes to ensure the capture, use, retention, and disposal of an individual's biometric data is done in a manner that protects this sensitive data.[191] For a biometric data protection statute to adequately achieve this purpose, proper enforcement mechanisms must accompany the substantive provisions of the statute.

Illinois' unique statute allowing a private right of action to accompany a privacy statute presents an important case study in understanding where and when BIPA violations have occurred. From this experience, it is revealed that most BIPA violations occur within the employer-employee relationship.[192] To allow biometric data protection statutes enacted in the future to adequately protect the interests it is designed to, a private right of action must be available to employees who seek to enforce their statutory rights against their employers whether this provision exists in its own statute or is part of a state's comprehensive privacy statute. Because consent can be coerced, new employees are unable to meaningfully consent to employer biometric privacy practices which may violate the relevant statute.[193] Additionally, existing employees have few, if any, recourse mechanisms against their employer if the employer chooses to enact biometric capture technologies during the employee's employment.[194] Further emphasizing the need for a private right

187. Strasser et al., *supra* note 51.

188. *See* Harger, *supra* note 73, at 16.

189. Terri Gerstein & Marni von Wilpert, *State attorneys general can play key roles in protecting workers' rights*, ECON. POL'Y INST. (May 7, 2018) at 3, https://www.epi.org/publication/state-attorneys-general-can-play-key-roles-in-protecting-workers-rights/ [https://perma.cc/33W9-TAE4]; Strasser et al., *supra* note 51.

190. Gerstein, *supra* note 190; Harger, *supra* note 73, at 1; Strasser et al., *supra* note 51.

191. *See* German & Barber, *supra* note 2.

192. Harger, *supra* note 73, at 1.

193. *See supra* Section III.A.

194. *Id.*

of action in this context, state attorneys general are public employees with limited resources.[195]

However, BIPA is not perfect and should not be copied exactly. It has presented many problems such as large class action suits resulting in millions in settlements.[196] Such shortcomings have been recognized by Illinois, resulting in the August 2024 amendment to overrule the *Cothron* decision which previously allowed for aggregated damages.[197] To adequately effectuate a legislature's intent of protecting its citizens biometric data, a desirable scheme allows a private right of action for employees against their employers, while channeling the remaining litigation through public enforcement, thereby lessening litigation and excessive damages.[198]

Biometric data is here to stay. It is time the law catches up and appropriately protects it.

195. *See* Strasser et al., *supra* note 51; Caitriona Fitzgerald & Matt Schwartz, *A New Model for State Privacy Legislation*, TECH POL'Y PRESS (Jan. 6, 2025), https://www.techpolicy.press/a-new-model-for-state-privacy-legislation/ [https://perma.cc/K27Y-6WZ3].

196. Harger, *supra* note 73, at 18.

197. Stauss, *supra* note 173.

198. *See supra* Section III.

Telecommunication Breakdown: Promoting Competition Through Reform of the Telecommunications Act Of 1996

Nathan Eichten*

TABLE OF CONTENTS

* J.D., May 2025, The George Washington University Law School; B.A. 2021 Political Science, Philosophy, University of Wisconsin-Madison. I am profoundly thankful to the late Professor Ethan Lucarelli, whose enthusiastic mentorship and intellectual rigor was essential to this Note's creation. I also thank the Federal Communications Law Journal Editorial Board for their tireless commitment to excellence and for helping bring this piece to publication. I want specially acknowledgment Professors Richard Pierce and William Kovacic for advancing my curiosity and excitement for the field of Antitrust Law. Finally, to my family and friends—your support, humor, and well-timed distractions make all the difference.

I. INTRODUCTION

The 1996 Telecommunications Act's stated goal was "to promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies."[1]

The success of the 1996 Telecommunications Act is that as of 2021, 97% of Americans own a cell phone capable of communicating long distance to other users, compared to only 36% of households owning a cell phone in 1998, a short two years after the Act was passed.[2] The average monthly cell phone bill is $144, an expensive price that consumers are still willing to pay for the essential role that cell phones play in American life.[3]

However, the Act has partially failed in that competition in the telecommunications industry has massively consolidated. With the successful merger of T-Mobile and Sprint in 2020, the telecommunications industry became dominated by only three major firms: AT&T, Verizon, and the new-look T-Mobile.[4] These three firms account for about 98% of the United States' mobile service revenues.[5] In 1996, there were seven competitive long-distance carrier providers.[6] The investment-heavy nature of the telecommunications industry poses a major barrier to entry for potential new competitors.[7] Due to this barrier to entry, the future of flourishing competition in the telecommunications industry beyond the three giant firms feels like a long shot.

A question that remains alludes to the purpose of the Act's final goal: what will the future of telecommunication competition look like with the development of technology? The landscape of how humans use

---

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

2. *Compare Mobile Fact Sheet*, PEW RSCH. CTR. (Jan. 31, 2024), https://www.pewresearch.org/internet/fact-sheet/mobile/ [https://perma.cc/8Q7V-X8HE], *with Cellphone Ownership Soared Since 1998*, WALL ST. J. (Nov. 27, 2009), https://www.wsj.com/articles/BL-REB-8073 [https://perma.cc/BW9E-GNA5].

3. *See What is the Average Cell Phone Bill per Month?*, ASTOUND BROADBAND (Apr. 28, 2023), https://www.astound.com/learn/mobile/average-cell-phone-.bill/ [https://perma.cc/6URU-3TR9].

4. Edmund Lee, *T-Mobile and Sprint are Cleared to Merge as the Big Get Bigger*, N.Y. TIMES (Feb. 11, 2020), https://www.nytimes.com/2020/02/11/business/media/t-mobile-sprint-merger.html [https://perma.cc/92DJ-KL9Z].

5. *See* 20 FCC WIRELESS COMPETITION ANN. REP. 8 (2017), https://docs.fcc.gov/public/attachments/FCC-17-126A1.pdf [https://perma.cc/9DC8-YTH6] (reporting the market share strength of the three major firms compared to all other service providers).

6. *See* Jason Whalley & Peter Curwen, *Whatever Happened to the Baby Bells? Internationalization and De-internationalization in the Telecommunications Industry*, 8 MINN. J.L. SCI. & TECH. 149, 155 (2007) (outlining the immense long-distance presence that Baby Bells have in the telecommunications market).

7. *See* Pamela Mondliwa, *Policy Brief: Barriers to Entry in Telecoms*, U. JOHANNESBURG (2016), https://static1.squarespace.com/static/52246331e4b0a46e5f1b8ce5/t/578275e7bebafbf781923a46/1468167662832/Telecommunications+100716.pdf [perma.cc/J3MQ-6WMK].

telecommunications as we know it today will surely evolve with the emergence of novel technologies like AI and machine learning, nanotechnology, advanced sensory digitalization, cloud solutions, and edge computing. These sophisticated technologies require immense amounts of capital, infrastructure, and time to progress into practical tools. They are being developed further every day and could transform the status quo of telecommunications industry as we now know it.

This Note asserts that the Telecommunications Act of 1996, particularly Section 251, has failed to fulfill its intended purpose to empower competition because it benefits incumbent interests and does not give new market entrants the opportunities to succeed nor the incentives to invest in competitive infrastructure. Instead, the Act's approach to promoting competition through deregulation and enabling incumbent telecommunication firms to venture into new industries has produced the opposite effect: industry consolidation.[8] This approach encourages firms to consolidate with competitors who offer similar services to increase their market share.[9] The approach also incentivizes firms to merge with competitors that maintain robust presence in industries the firm seeks to enter but does not want to build out from scratch.[10]

To address this shortcoming, this Note argues that the Telecommunications Act of 1996 needs to be amended to ensure that competition in emerging technologies can flourish alongside currently prevalent technologies in the telecommunications industry. Lawmakers must learn from the 1996 Act's mistakes, using historical context to guide how they should amend the Act to account for the present and future. Emerging technologies create an opportunity for industry newcomers to rise to the challenge against the big three. An amended Telecommunications Act of 1996 must encourage this challenge and do so thoughtfully to prevent a recurrence of the backfire that the original Act experienced. Specifically, Section 251 of the Act needs to be amended to redesign how newcomers to the telecommunications industry can meaningfully capitalize on interconnection requirements.[11] Through amendments to Section 251, newcomers will be able to use incumbent carriers' infrastructure to eventually become independent owners of crucial infrastructure themselves to persist in the industry as legitimate industry competitors.

Section II of this Note discusses the history leading up to the passage of the Telecommunications Act of 1996 and describes its unintended consequences after being made into law Section III analyzes the shortcomings of the Act using examples of how it promoted consolidating effects that run counter to its intended purpose. Finally, Section IV will propose amendments to the Act, aiming to ensure newcomers to the telecommunications industry

8. *See* Gene Kimmelman et al., *The Failure of Competition Under the 1996 Telecommunications Act*, 58 FED. COMM. L.J. 511, 513 (2006).

9. *See id.*

10. *See* Whalley & Curwen, *supra* note 6, at 158 (showing the rationale behind the modified final judgment's decision to restrict the newly created baby bells from entering the long-distance service market).

11. *See* 47 U.S.C. § 251.

may emerge as independent operators of telecommunications infrastructure and loosen their reliance on preexisting infrastructure currently dominated by major industry incumbents.

II. BACKGROUND

The first domino leading to the creation of the Telecommunication Act of 1996 fell in 1982 when AT&T's telecommunications monopoly was divested into seven regional Bell Operating Companies (hereinafter "BOCs"), or the "Baby Bells," who subsequently dominated their respective regions.[12] Congress passed the Telecommunications Act of 1996 with the goal to "let anyone enter any communications business – to let any communications business compete in any market against any other[,]" implying Congress' attempt to counterbalance the BOCs' dominance through the introduction of new competition into telecommunication.[13] The 1996 Act attempts to accomplish this goal through the removal of stringent regulations that had previously restricted businesses from expanding into a diverse range of markets.[14] The passage of the 1996 Act instead produced an opposite consolidating effect, and the BOCs subsequently merged with one another to capitalize on each other's presence in complementary markets.[15] Today, the telecommunications industry is dominated by three major firms after the 2020 merger of T-Mobile and Sprint: AT&T, Verizon, and T-Mobile.[16] Boost Mobile, a previous subsidiary of Sprint, was organized by the Department of Justice (DOJ) and Federal Communications Commission (FCC) to be purchased by Dish Network in hopes of them emerging as a fourth competitor in the telecommunications industry.[17] However, Dish has been unable to pose a legitimate threat to the big three firms due to their major losses in subscribers regardless of their steadfast support from the DOJ and FCC.[18] It appears that no firm will be able to threaten the triopoly of AT&T, Verizon,

12. *See* Michael Meyerson, *Ideas of a Marketplace: A Guide to the 1996 Telecommunications Act*, 49 FED. COMM. L.J. 251, 254 (1997) (detailing the root cause of the local rate increase that was diluting the benefits of the competitive long-distance market).

13. *Telecommunication Act of 1996*, FCC, https://www.fcc.gov/general/telecommunications-act-1996 [https://perma.cc/5A5X-39P7].

14. *See* Whalley & Curwen, *supra* note 6, at 153, 156.

15. *See id.* at 158.

16. *See* David Lumb, *T-Mobile's Merger with Sprint: Everything That's Changed 3 Years Later*, CNET (Apr. 22, 2023, 11:27 AM), https://www.cnet.com/tech/mobile/t-mobiles-merger-with-sprint-everything-thats-changed-3-years-later/ [perma.cc/XH5A-6VQ9].

17. *See* Press Release, U.S. Dep't of Just., Justice Department Settles with T-Mobile and Sprint in Their Proposed Merger by Requiring a Package of Divestitures to DISH (July 26, 2019) (on file with Dep't of Justice), https://www.justice.gov/opa/pr/justice-department-settles-t-mobile-and-sprint-their-proposed-merger-requiring-package [perma.cc/8L6F-6Q8T] (detailing the agreed upon settlement between the DOJ, FCC, T-Mobile, and Sprint).

18. *See* Linda Hardesty, *Dish Loses 225,000 Wireless Subs in Q3 2023*, FIERCE NETWORK (Nov. 6, 2023, 6:30 PM), https://www.fiercewireless.com/wireless/dish-loses-225000-wireless-subs-q3-2023 [perma.cc/QUS6-4NM4] (outlining Dish's competitiveness compared in the 5G industry).

and T-Mobile unless significant changes are made to the governing doctrines of the telecommunications industry.

A. Pre-Telecommunications Act of 1996

1. The 1982 AT&T Divestiture

In 1974, the DOJ filed a lawsuit against AT&T.[19] This lawsuit was based on antitrust grounds under Section 2 of the Sherman Act alleging that AT&T had used its dominant position in the telecommunications market to further progress its already existing monopoly position in the market.[20] The two sides reached a settlement in 1982, when a consent decree was agreed to divest AT&T from the BOCs, often referred to as the "Baby Bells," which were smaller companies spread out on a regional basis that provided strictly local telecommunications services to the region in which they were located.[21] The BOCs no longer exist as a result of their mergers with one another that occurred shortly after the passage of the Telecommunications Act of 1996.[22]

The United States District Court for the District of Columbia described the main ways that AT&T had used its monopoly in local telephone services to harm competitors through its control of the BOCs.[23] First, the court noted that AT&T had prevented or severely delayed competing long-distance carriers to access their local networks, which is essential to compete in the long-distance market.[24] Second, the court found that AT&T had used profits obtained through these monopolistic local practices to fund its long-distance enterprise, thus maintaining an unfair advantage against its competitors.[25] According to the court, divestiture was necessary because of AT&T's "substantial domination of the telecommunications industry in general."[26]

Further, the court assumed that the BOCs would want to expand their business into wider markets to grow, including the lucrative long-distance market.[27] The modified final judgment ("MFJ") predicted this and prohibited

---

19. *See* Ben M. Enis & E. Thomas Sullivan, *The AT&T Settlement: Legal Summary, Economic Analysis, and Marketing Implications*, 49 J. MKTG. 127 (1985) (describing the timeline of the Department of Justice's action against AT&T).

20. *See* John Pinheiro, *AT&T Divestiture & the Telecommunications Market*, 2 HIGH TECH. L.J. 303, 303 (1988) ("It charged that AT&T had used its dominant position in the telecommunications market to suppress competition and enhance its monopoly power."); *see also* 15 U.S.C. § 2.

21. *See id.* (detailing the effects of the agreed-upon settlement between the DOJ and AT&T in 1982).

22. *See* Whalley & Curwen, *supra* note 6, at 155 (outlining the effects of the consolidation of the Baby Bells shortly after the passage of the Telecommunications Act of 1996).

23. *See* United States v. Am. Tel. & Tel. Co., 552 F. Supp. 131, 223 (D.D.C. 1982) (indicating the practices of AT&T that led to the court's decision for its divestiture).

24. *See id.*

25. *See id.*

26. *Id.* at 163 (showing the court's agreement as to the scale of AT&T's control of the telecommunications industry before the 1984 divestiture).

27. *See* Whalley & Curwen, *supra* note 6, at 151 (outlining the broader business goals of the Baby Bells).

them from providing long-distance services and manufacturing products or customer premises equipment.[28]

2. The Aftermath of the 1982 AT&T Divestiture

While the AT&T divestment resulted in seven different BOCs, each were massive enterprises on their own. The BOCs—Ameritech, Bell Atlantic, BellSouth, Nynex, Pacific Telesis, Southwestern Bell, and US West—had average assets of $15.8 billion (equivalent to $47 billion today), and an average of 84,000 employees each.[29] Instead of having monopoly control over the local market on a nationwide basis, the large BOCs instead now controlled a virtual monopoly over their specifically delegated service area.[30]

The competition for the local telephone market thus faced the same problem the D.C. Circuit Court faced regarding AT&T: the expense of creating a local infrastructure as robust as the BOCs was massive, and a new local entity being introduced would require access to a BOC's own network and services to challenge it.[31] In this way, the BOCs had a government-sponsored natural monopoly on the local telephone market. Therefore, a new firm attempting to compete for the local market requires collaboration and help from the same entity which that new firm seeks to compete with.[32] This relationship parallels the reliance that Dish's telecommunications brand Boost Mobile has on its former owner T-Mobile's infrastructure, which will be discussed thoroughly later in this Note.[33]

Though the BOCs were restricted by the D.C. Circuit Court's MFJ from expanding into the long-distance market, they could operate in new lines of business through a waiver process if they successfully showed that they would not abuse their monopoly powers.[34] The BOCs were able to enter new realms of business beyond their local specialty through this waiver process.[35]

---

28. *Id.* at 152 (showing the rationale behind the modified final judgment's decision to restrict the newly created Baby Bells from entering the long-distance service market).

29. *See id.* (showing that though the Baby Bells were spawned from a shared entity their scale remained massive).

30. *See* Meyerson, *supra* note 12, at 254 (detailing the root cause of the local rate increase that was diluting the benefits of the competitive long-distance market).

31. *See id.* (showing the central issue of the 1984 divestiture and a parallel concern that this Note seeks to remedy).

32. *See id.* (displaying the paradoxical nature of the Baby Bell monopoly problem).

33. *See* Jacob Kastrenakes, *Dish Now Owns Boost Mobile, Following Sale from T-Mobile*, VERGE (July 1, 2020, 11:46 AM), https://www.theverge.com/2020/7/1/21309968/dish-boost-sprint-tmobile-acquisition-spinoff-closes-prepaid [https://perma.cc/F6EV-QUHZ].

34. *See* Meyerson, *supra* note 12, at 259-63 (detailing the ability, though limited, for Baby Bells to enter other lines of business with a proper showing they would not abuse their monopoly power).

35. *See id.* (outlining a diverse set of business the Baby Bells entered).

B. The Telecommunications Act of 1996: Scope and Application

As noted earlier, the stated purpose of the Telecommunications Act of 1996 is "[t]o promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies."[36] This Act eliminated the AT&T consent decree and the restrictions that it imposed on the BOCs and replaced them with new duties and regulations.[37]

The Act defines "telecommunications carriers" as "any provider of telecommunications services offering telecommunications for a fee directly to the public to be effectively available directly to the public."[38] One of the duties of telecommunications carriers imposed by the Act centers around interconnection, which is found in Section 251 of the Act.[39] This means that all carriers must allow any other carrier to interconnect with their network fairly and equally.[40] Section 201(a) of the Act broadly affirms this duty, and states that "[i]t shall be the duty of every common carrier engaged in interstate or foreign communication by wire or radio to furnish such communication service upon reasonable request therefor; and . . . to establish through routes . . . to establish and provide facilities and regulations for operating such through routes."[41]

Preexisting telecommunications carriers are one of such entities that has a duty to interconnect their infrastructure with other carriers.[42] The Act defines "Incumbent Local Exchange Carriers," or "ILECs," to be those carriers that already offer telephone services on the date the Act was passed, or firms who are later found to maintain operations similar to an incumbent carrier.[43] Congress imposed additional duties on preexisting ILECs because of their significant advantage over potential market newcomers.[44] As noted, one of the most crucial duties imposed upon ILECs is the duty to provide "for

36. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified at 47 U.S.C. §§ 251-271) (noting the original stated purpose for the Act).

37. *See* Jay L. Birnbaum, *M&A Implications of Telecommunications Act of 1996*, 1 FORDHAM J. CORP. & FIN. L. 59, 63 (1996) (explaining the Act's effect on the Baby Bells, which is a central provision of the Act).

38. Telecommunications Act of 1996, 47 U.S.C. § 153(51)-(53) (stating the statutory definition of "telecommunications carriers").

39. See 47 U.S.C. § 251 (detailing a specific provision of the Act that imposes a duty upon incumbent carriers).

40. *See id*. at (a)(1)-(2) (stating what above-defined "telecommunications carriers" are obligated to do under the Act).

41. 47 U.S.C. § 201(a) (detailing the broad duty of common telecommunications carriers to establish physical connection of their communications infrastructure to others).

42. *See* 47 U.S.C. § 251(c)(2) (showing incumbent telecommunications carriers' obligation to interconnect with competing telecommunications carriers).

43. *Id.* at (h)(1)-(2); *see also* Meyerson, *supra* note 12, at 257 (stating the Act's definition of "incumbent local exchange carriers").

44. *See id.* (detailing the reasoning why the Act imposes are additional duties on incumbent LECs).

the facilities and equipment of any requesting telecommunications carrier, interconnection with the local exchange carrier's network."[45]

The Act further contains a section titled "Bell Operating Company entry into interLATA services," which outlines what a BOC may do to enter the long-distance telecommunications market.[46] Following the divestiture of AT&T in 1982, there was a expansion in the amount of service providers that operated in the long-distance service space.[47] Before this Act, the BOCs were severely restricted from entering the long-distance markets even though their assets were well suited to do so.[48] A BOC was allowed to expand their operations into the long-distance market for telecommunications after they adhered to the Act's "competitive checklist," which lawmakers expected would uphold the potential for competition in the local service market.[49] The foremost requirement in the BOC competitive checklist is interconnection with other telecommunications carriers, thus mirroring the interconnection requirements found in Section 251 of the Act.[50]

C. Post-Telecommunications Act of 1996 Act Effects on Competition in the Telecommunications Industry

Sections 201(a) and 251 of the 1996 Telecommunications Act marked the beginning of BOCs having a clearer path to being able to enter the long-distance and equipment manufacturing markets.[51]

The BOCs had begun to consolidate themselves in 1995 through complex corporate arrangements.[52] However, the 1996 Act's enactment opened the door for a rapid flood of mergers largely due to provisions allowing for expansion into a diverse range of markets.[53] For example, the BOCs were immediately permitted to provide "out-of-region" long distance

45. Telecommunications Act of 1996, 47 U.S.C. § 251(c)(2) (stating what the above-defined incumbent local exchange carriers are obligation to do under the Act).

46. 47 U.S.C. § 271(a) (detailing specific requirements BOCs must satisfy to enter the long-distance market).

47. *See* Eli M. Noam, *Assessing the Impacts of Divestiture and Deregulation in Telecommunications*, 59 S. ECON. J. 438, 443 (1993) (detailing AT&T's reduction in market share in inter-LATA long-distance service from 84.2% in 1984 to 62.9% in 1990).

48. *See* Stuart N. Brotman, *Was the 1996 Telecommunications Act Successful in Promoting Competition?*, BROOKINGS (Feb. 8, 2016), https://www.brookings.edu/articles/was-the-1996-telecommunications-act-successful-in-promoting-competition/ [perma.cc/Z7HT-ZW67] (showing a specific change that the passage of the 1996 Act caused).

49. *See* Meyerson, *supra* note 12, at 260.

50. *See* Telecommunications Act of 1996, 47 U.S.C. §§ 251(c)(2), 271(c)(2)(B) (drawing parallel duties between BOCs and ILECs to enter into the long-distance telecommunications market).

51. Meyerson, *supra* note 12, at 254-55 (showing that adherence to the competitive checklist allowed for Baby Bells to enter the long-distance telephone service industry).

52. *See* Whalley & Curwen, *supra* note 6, at 156 (noting that consolidation within the telecommunications industry began slowly before the 1996 Act).

53. *See id.*

service and to manufacture and sell telecommunications network equipment once they received FCC permission to offer in-region long distance service.[54]

The BOCs rapidly restructured themselves through mergers beginning in 1996 following the enactment of the 1996 Act.[55] By 2006, the BOCs had merged with one another, starting from seven entities into three prominent telecommunications companies: Verizon, AT&T, and Qwest.[56] Qwest now operates under the CenturyLink brand and is owned by Lumen Technologies.[57]

D. The Present Day

According to the FCC's latest Mobile Wireless Competition Report released in 2022, AT&T, Verizon Wireless, and T-Mobile accounted for 98.9% of the market share for providers with publicly-traded facilities by the end of 2021.[58] UScellular retains the remaining 1.1%.[59] However, only AT&T, Verizon Wireless, and T-Mobile are facilities-based service providers referred to as "nationwide service providers" because they cover a substantial majority of the country.[60] UScellular is best characterized as a multi-regional service provider because it deploys wireless network operations in portions of 21 states.[61]

Mobile Virtual Network Operators ("MVNOs") are wireless service providers that do not own any network facilities but instead purchase wireless services wholesale from facilities-based providers and resell those services to consumers.[62] Examples of MVNOs include Mint Mobile, Google's Google Fi, and Boost Mobile, which is owned by Dish.[63] However, Dish is a unique hybrid-type MVNO in that it uses T-Mobile's wireless network to provide service to its customers, provides wholesale services to its customers through AT&T's network, and is committed to building its own 5G network infrastructure alongside its usage of another company's infrastructure.[64] This arrangement and Boost Mobile's existence altogether can be attributed to its

54. *See id.* (detailing another key provision that led to BOCs being interested and able to merge with other entities).

55. *See id.* at 155.

56. *See id.* at 155, 158 (showing the massive consolidation effect that the passage of the 1996 Act had on the telecommunications industry).

57. *See* Aldo Svaldi, *CenturyLink Rebrands Itself as Lumen Technologies*, DENVER POST (Sept. 14, 2020), https://www.denverpost.com/2020/09/14/centurylink-rebrands-itself-as-lumen-technologies/ [perma.cc/8VGX-8VPZ] (detailing the transaction that transformed Qwest's business branding).

58. *See* 2022 Communication Marketplace Report, *Report*, 37 FCC Rcd 15514, 58 (2022) [hereinafter FCC 2022 Communications Marketplace Report].

59. *See id.*

60. *Id.* at 51.

61. *See id.*

62. *See id.* at 52.

63. *See id.* at 52-53.

64. *See* FCC 2022 Communications Marketplace Report, *supra* note 58, at 62.

divestiture from Sprint, which was a result of the pledge agreement approving the massive merger between T-Mobile and Sprint.[65]

1. The T-Mobile/Sprint Merger

Note that according to the 2023 Merger Guidelines released by the FTC and DOJ, a market is presumed to be highly concentrated and subject to stricter antitrust scrutiny when the calculated Herfindahl-Hirschman Index ("HHI") exceeds 1,800.[66] According to the FCC's Mobile Wireless Competition Report in 2022, the weighted average HHI for mobile wireless services was 3,596.[67]

The most contemporary example of consolidation within the telecommunications industry is the merger between industry giants T-Mobile and Sprint under the T-Mobile branding, which was finalized in April 2020.[68] This merger transformed the telecommunications industry from four major carriers to three, with any other meaningful competition largely coming from only Verizon and AT&T.[69] In seeking the completion of this deal, T-Mobile and Sprint needed to appease the competition concerns of one of the antitrust enforcement agencies, the DOJ, and the agency with regulatory authority over common carriers, the FCC.[70]

The DOJ and FCC proposed that Sprint hand over its prepaid mobile business Boost and the entirety of its 800MHz spectrum ownership to Dish, a satellite TV company.[71] They further required strict wholesale interconnection agreements between T-Mobile and Dish.[72] T-Mobile and Sprint were also required to make at least 20,000 cell sites and hundreds of retail locations available to Dish.[73]

Though the FCC and DOJ's competition concerns were held at bay as a result of their negotiations, a group of states and the District of Columbia sued to block the merger in federal court in the Southern District of New York.[74] The plaintiffs claimed that "the effect of the merger would substantially lessen competition in the market for retail mobile wireless telecommunication services (the 'RMWTS Market') in violation of Section 7 of the Clayton Act."[75]

---

65. *See* Lumb, *supra* note 16.

66. *See* U.S. DEP'T OF JUST., FED. TRADE COMM'N, MERGER GUIDELINES 5-6 (2023), https://www.justice.gov/d9/2023-12/2023%20Merger%20Guidelines.pdf [https://perma.cc/C43T-WNCV].

67. *See* FCC 2022 Communications Marketplace Report, *supra* note 58, at 60-61.

68. *See* Lumb, *supra* note 16.

69. *See id.* (detailing further consolidation within the telecommunications industry).

70. U.S. Dep't of Justice, *supra* note 17.

71. *See id.* (outlining further demands made by the DOJ to approve the T-Mobile merger).

72. *See id.*

73. *See id.*

74. *See* New York v. Deutsche Telekom AG, 439 F. Supp. 3d 179, 187-88 (S.D.N.Y. 2020) (describing the plaintiffs in the T-Mobile/Sprint merger lawsuit).

75. *Id.* at 186; *see also* 15 U.S.C. § 18 (outlining the central claim made by the plaintiff states).

The court approved the merger between T-Mobile and Sprint.[76] One of the court's foremost reasons for approving the merger was because they found that the FCC and DOJ's agreements with Sprint and Verizon were satisfactory to set up Dish as a fourth competitor in the industry through their spectrum holdings and the Boost brand.[77] The court did not reference the Telecommunications Act of 1996 anywhere in their opinion.[78]

2. Dish's Failure Following the T-Mobile/Sprint Merger

Dish opened its 5G offerings in August of 2022, along with its newly acquired prepaid service, Boost, following the T-Mobile/Sprint merger.[79] However Dish's new acquisition and 5G rollout has failed to present a legitimate challenge to the incumbent market giants.[80]

Dish's attempt at competing with the likes of Verizon, AT&T, and T-Mobile in the 5G space is not going as the FCC and DOJ had hoped.[81] In Quarter Three ("Q3") of 2023 alone, Dish lost 225,000 retail wireless subscribers, adding to the 188,000 subscribers lost in Quarter Two ("Q2") of 2023.[82] Dish closed Quarter Four ("Q4") with a total of 7.5 million retail wireless subscribers.[83] In their Q3 report, they achieved revenue of $3.70 billion, a significant decrease compared to their 2022 Q3 revenue of $4.10 billion.[84] In comparison, for Q4 of 2023, T-Mobile reported 119 million wireless subscribers,[85] Verizon reported 144 million,[86] and AT&T reported 241.5 million.[87]

After the T-Mobile/Sprint merger was affirmed, there were three dominant players in the telecommunications industry, with little resistance from Dish.[88] There appeared to be negligible hope that any new competition would emerge. However, Mint Mobile presented itself as a strong newcomer

76. *See Deutsche Telekom AG*, 439 F. Supp. 3d at 248.

77. *See id.*

78. *See id.* at 179-249.

79. *See* Lumb, *supra* note 16 (indicating a result of the concessions made during the T-Mobile/Sprint negotiations).

80. *See id.*

81. *See* Hardesty, *supra* note 18 (outlining Dish's competitiveness compared to other players in the 5G industry).

82. *See id.* (outlining specific metrics suggesting Dish's lack of accomplishment).

83. *See id.* (showing Dish's macro losses of revenue).

84. *See id.*

85. *See* T-MOBILE, T-MOBILE DELIVERS INDUSTRY-LEADING GROWTH IN CUSTOMERS, SERVICE REVENUES, PROFITABILITY AND CASH FLOW IN 2023, SETTING UP STRONG 2024 OUTLOOK (2023), 2, https://s29.q4cdn.com/310188824/files/doc_financials/2023/q4/Q4-2023-TMUS-Earnings-Release.pdf [perma.cc/F8NR-Z4QY] (showing T-Mobile's success in comparison to Dish).

86. *See* VERIZON, FINANCIAL AND OPERATING INFORMATION, 11 (Dec. 31, 2024), https://web.archive.org/web/20250124153521/https://www.verizon.com/about/file/74377/download?token=aFR5AvZZ [https://perma.cc/9HDT-E47H].

87. *See* AT&T Inc., Current Report (Form 8-K), 6, (Jan. 24, 2024), https://otp.tools.investis.com/clients/us/atnt2/sec/sec-show.aspx?FilingId=17201271&Cik=0000732717&Type=PDF&hasPdf=1 [https://perma.cc/268H-5D4Z] (showing AT&T's success in comparison to Dish).

88. *See* Hardesty, *supra* note 18, at 6.

to the industry.[89] In fact, Mint Mobile was the fastest growing mobile service provider in the United States in 2022, and by a large margin.[90] Mint Mobile had a 45% year over year ("YoY") growth rate in 2022, compared to T-Mobile's 12%, AT&T's 5%, and Verizon's -5% YoY rates.[91] Mint Mobile held only a small piece of the market share pie with their 3.4% share in 2022, compared to Verizon's 24%, T-Mobile's 31%, and AT&T's 41%.[92]

However, T-Mobile announced in March of 2023 that they acquired Mint Mobile.[93] Mint Mobile specialized in affordable wireless access, which T-Mobile cited as being a key reason for its desire to acquire the brand and expand their position with cost-conscious consumers.[94] Outside of this buyout, Mint Mobile was merely an MVNO that does not own its own facilities.[95]

E. Technologies Pre-Telecommunications Act of 1996 vs. Today And Beyond

1. The 1996 Act's Anachronistic Language

There are a total of eleven references to the Internet in the Telecommunications Act of 1996, but these references occur in only two sections of the Act.[96] First, the Act defines "interactive video services or Internet services over facilities to or for elementary and secondary schools . . ." under the definition of interLATA services during its discussion of the interLATA provision by a BOC.[97] The remaining twenty references come from the famous Section 230, which outlines protection for private blocking and screening of offensive material on the Internet.[98] The definition of "Internet" under this section is "the international computer network of both Federal and non-Federal interoperable packet switched data networks."[99] Though Section 230 repeatedly references the rapid development of the Internet, it does not reference any specific details regarding how development of the Internet could look.[100]

---

89. *See* Sneha Pandey, *T-Mobile Acquires Mint Mobile – 2022's Fastest-Growing US Mobile Service Provider*, SIMILARWEB BLOG (Sept. 6, 2023), https://www.similarweb.com/blog/insights/software-tech-news/t-mobile-aquires-mint-mobile/ [perma.cc/B4GX-KJE8].

90. *See id.*

91. *See id.* (detailing a central reason behind Mint Mobile's presence in the industry).

92. *See id.* (placing Mint Mobile's location in the industry in the context of market power).

93. *See id.*

94. *See id.* (describing Mint Mobile's general consumer base and target).

95. *See* FCC 2022 Communications Marketplace Report, *supra* note 58, at 65.

96. *See* Telecommunications Act of 1996, 47 U.S.C. §§ 230, 271(g)(2).

97. *Id.* § 271(g)(2) (showing the first location of reference to the Internet in the 1996 Act).

98. *See id.* § 230 (detailing the second and more prominent location of references to the 1996 Act).

99. *Id.* § 230(f)(1) (noting the specific definition of "Internet" as defined by the Act).

100. *Id.* (showing how the Act defines the Internet's rapid development).

Importantly, the 1996 Act makes no reference to the current global wireless standard: 5G broadband.[101] In telecommunications, broadband refers to a wide bandwidth that is capable of transporting multiple signals over a wide range of frequencies that supports numerous Internet traffic types, thus allowing multiple data streams to be sent at once.[102] Put simply, mobile broadband technology allows today's phones to connect to the Internet.[103] 5G, or the fifth generation mobile network, is the most prevalent vehicle for broadband support in the telecommunications industry today.[104] 5G allows telecommunications users to leverage the Internet with the highest speed capabilities to date as compared to 4G and 3G, and was specifically designed to flexibly support future telecommunications services that are currently unknown.[105]

2. Telecommunications' Technological Future

As mentioned, there are numerous technologies widely used today and predicted to be the major keystones for future technologies that are not addressed by the 1996 Telecommunications Act. Examples include 3G, which allowed for video calling and Internet access on mobile devices, 4G, that opened the doors to even higher quality video calls and streaming, and the newest development, 5G, which allows for advancements like self-driving vehicles, 4K mobile streaming, and enhanced security.[106] North America alone experienced 22 million new 5G connections in Q3 2024, which adds to a total of 264 million 5G connections in the region.[107] North America leads all continents in 5G adoption.[108]

In addition, new cutting-edge technologies are emerging rapidly that seek to impact the way telecommunications are used. Examples include artificial intelligence, cloud computing, virtual reality, Internet of Things

101. *See Everything You Need to Know about 5G*, QUALCOMM, https://www.qualcomm.com/5g/what-is-5g#:~:text=5G%20will%20bring%20wider%20bandwidths,Gbps%20throughput%2C%20and%20low%20latency [https://perma.cc/QRQ5-Z3K4]; *see also* 47 U.S.C. § 251.

102. *See* NAT'L TELECOMM. & INFO. ADMIN., U.S. DEP'T COM., INTRODUCTION TO BROADBAND AND HIGH SPEED INTERNET 4 (2022), https://broadbandusa.ntia.doc.gov/sites/default/files/2022-12/Introduction_to_Broadband_and_High_Speed_Internet_FINAL_0.pdf [perma.cc/WV5N-UZT8].

103. *See id.*

104. *See* QUALCOMM, *supra* note 101.

105. *See* NAT'L TELECOMM. & INFO. ADMIN., U.S. DEP'T COM., *supra* note 102.

106. *See 3G vs. 4G vs. 5G: What's the Difference?*, ACKERMAN SEC., https://www.ackermansecurity.com/blog/home-security-tips/3g-4g-5g (last visited Apr. 14, 2025) [perma.cc/S8RZ-DGZT] (detailing examples of how telecommunications technology has changed since the passage of the Act in 1996).

107. *See Global Connections Pass 2BN*, CSI (Dec. 19, 2024), https://www.csimagazine.com/csi/Global-5G-connections-pass-2BN.php [https://perma.cc/X46X-U9SD].

108. *See id.*

("IoT"), edge computing, and advanced cybersecurity.[109] 5G is the central facilitator to most of these emerging technologies, including IoT and virtual reality.[110] 5G is considered to be the critical enabler to facilitation for a cohesive and operational relationship between broadband-based technology, and was specifically designed to stand the test of time to continue being useful as future innovation surfaces.[111]

III. ANALYSIS

A. The Telecommunications Act of 1996's Failure to Promote Competition

The Telecommunications Act of 1996, particularly Section 251, has failed to fulfill its intended purpose to empower competition because it benefits incumbent interests and does not give new market entrants the opportunities to succeed nor the incentives to invest in competitive infrastructure. The primary goal of the Telecommunications Act of 1996 was to promote competition in the telecommunications industry.[112] Yet almost immediately after the Act's passage the opposite effect began to occur, and the true implications of the Act emerged: consolidation.[113] The Act permitted the BOCs to access a diverse range of markets that were previously restricted to them, including "out-of-region" long distance service and manufacturing and sales of telecommunications network equipment.[114] Vast opportunity for diversification and investment in new business and industry presented itself. Investment in new areas of business is expensive and requires significant capital to become a practical business solution. This need for investment incentivized companies that had presence in unique realms of business from one another to combine forces through merger, creating an even larger market force with its hands in a wider range of industry.[115]

In the present day of the telecommunications industry, the infrastructure and facilities necessary to deliver quality mobile communications solutions that consumers expect are stacked in the hands of Verizon, T-Mobile, and AT&T.[116] The reason for this is found in history. The 1984 divestiture of AT&T resulted in seven BOCs who maintained a government granted monopoly in their respective telephone region.[117] These

109. *See* Susi Wallner, *Discover the Top 10 Telecom Industry Trends in 2024*, STARTUS INSIGHTS (Feb. 21, 2021), https://www.startus-insights.com/innovators-guide/top-10-telecom-industry-trends-innovations-in-2021/#trend-six [perma.cc/S8RZ-DGZT] (showing examples of new technology being released and developed).

110. *See id.*

111. *See* James Dean, *How 5G Technologies Can be Implemented More Efficiently*, TECH RADAR (Dec. 5, 2018), https://www.techradar.com/news/how-5g-technologies-can-be-implemented-more-efficiently [perma.cc/93EV-M7JL].

112. *See* 47 U.S.C. §§ 251-271.

113. *See* Whalley & Curwen, *supra* note 6, at 155.

114. *Id*. at 156.

115. *Id*. at 155, 158.

116. FCC 2022 Communications Marketplace Report, *supra* note 58, at 58.

117. *See* Pinheiro, *supra* note 20, at 303.

seven BOCs held complete domination over their respective regions because of their well-established infrastructure and financial resources stemming from their previous regional monopolies.[118] New competitors struggled to enter the market because of the massive head start that the BOCs had from being mandated as the sole telecommunications presence in a region.[119] When the 1996 Telecommunications Act was passed the merger spree between the seven BOCs began.[120] In 2020, the T-Mobile and Sprint merger created the power triangle that we know today between AT&T, Verizon, and T-Mobile.[121]

This Note finds that the failure of the 1996 Act is largely due to the existing interconnection provisions outlined in Section 201 and Section 251 being ill-suited for the task of promoting competition. This is true for three main reasons. First, the provisions are focused on outdated telecommunications technologies that are not relevant to today's telecommunications landscape. Second, imposing a duty to provide interconnection is alone not sufficient to guaranteeing competition because the massive benefits of incumbency severely outweigh the significant startup cost and barrier to entry in the telecommunications industry. Third, the current interconnection system leads to a strange economic situation where "new entrants" are not legitimate competition at all, but rather weak state-subsidized wholesale customers of the incumbents themselves. As a result, the interconnection provisions of the 1996 Act should be rewritten around a new notion of modern infrastructure sharing that would more effectively drive new competition in the future.

1. Outdated Language in Sections 201 and 251

First, Sections 201 and 251 of the 1996 Act are focused on outdated technologies that are not relevant to today's telecommunications landscape.[122] Specifically, Section 251 is not equipped to address the current or emerging telecommunications industry because it exclusively encompasses telecommunications network realities of the 1980s and 1990s.[123] High-speed mobile broadband networks ubiquitous today were not available at the time of the 1996 Act.[124] Cellular networks have used different standards for data transmission via broadband since 1996, including 3G, 4G LTE, and the incumbent 5G most prevalent today.[125] Today's networks carry traffic of varying types, including video, data, and voice. 2G existed at the time of the

118. *See* Meyerson, *supra* note 12, at 254.
119. *See id*.
120. *See* Whalley & Curwen, *supra* note 6, at 155.
121. *See* FCC 2022 Communications Marketplace Report, *supra* note 58, at 58.
122. *See* 47 U.S.C. §§ 201, 251.
123. *See id*. § 251.
124. *See The History of Cellular Network and Broadband*, CUSTOM TRUCK ONE SOURCE (May 24, 2021), https://www.customtruck.com/blog/the-history-of-cellular-networks-and-broadband/ [https://perma.cc/M8X8-JVWU].
125. *See id.*

1996 Act's passage, which primarily focused on voice calls and text messaging.[126]

Section 251(2) of the Act's language is thus ill equipped to promote meaningful interconnection because it fails to acknowledge the existence of broadband networks altogether.[127] Rather, Section 251(2)'s language strictly uses the words "network," "telephone exchange services," and "exchange access" when discussing what is covered under an incumbent's duty to provide interconnection to.[128] There is no reference to broadband in any definition located in Section 153 of the Act, nor is there any open-ended language in the definitions that accounts for evolution in the industry to impliedly cover future innovations like 5G broadband capabilities.[129] There is a complete lack of reference to the most prevalent means of telecommunications: broadband. This, combined with its lack of open-ended language, opens the door for incumbent telecommunications carriers to argue that they do not need to provide broadband interconnection, which newcomers need to legitimately compete. Instead, incumbents may claim that they need only to provide interconnection to services of the most archaic type: simple telephone communication capabilities that existed during the 1996 Act's passage. For this reason, the Act's language in Section 251(2) needs to be updated to account for these technological realities, or at the very least add open-ended language that implies coverage of such broadband technologies.

2. Weak Interconnection Accessibility and Infrastructure Investment

Second, imposing a duty to provide interconnection alone is not sufficient to guarantee competition because the massive benefits to incumbency severely outweigh the significant startup cost and barrier to entry in the telecommunications industry. While Section 251 on its face seems satisfactory in ensuring that new competitors are able to access crucial facilities and equipment necessary to enter the telecommunications industry, it currently lacks enough direct support for industry newcomers to be able to become legitimate competition. Specifically, Section 251's interconnection provision does not afford industry newcomers the ability to build their own telecommunications infrastructure and become independent from the incumbent firms. Instead, its scope is limited to ensuring access to an incumbent's infrastructure at a reasonable cost.[130] This benefit is inadequate to properly subsidizing newcomers to develop their own infrastructure and reach independence.

---

126. *See id.*; *see also What is Second-Generation (2G)*, LENOVO, https://www.lenovo.com/us/en/glossary/what-is-2g/ (last accessed Apr. 14, 2025) [https://perma.cc/EQK2-RLMV].

127. *See* 47 U.S.C. § 251(2).

128. *Id.*

129. *Id.* § 153.

130. *See* 47 U.S.C. § 251.

Consider the aforementioned 5G broadband technologies. 5G is currently the preeminent mobile network technology deployed by mobile carriers.[131] The dominance of Verizon, T-Mobile, and AT&T in 5G is so massive that the barrier of entry seems to be insurmountable. For an outside firm to attempt to enter the 5G industry, they must invest into a wide variety of infrastructure to even have the capability to producing 5G, nevertheless being able to bring forth satisfactory pricing, service coverage, and speeds to convince consumers to switch to their services.[132] Such infrastructure includes base stations, antennas, sensors, and onboard radios for devices.[133] Further, usage of this type of infrastructure requires a massive real estate portfolio to be able to house crucial infrastructure necessary to maintain 5G around the entire country. Since Verizon, T-Mobile, and AT&T are so far ahead in both infrastructure and real estate, potential competitors need to rely on the big three's preexisting infrastructure and technology to compete with them.

Dish's attempt to enter the telecommunications industry illustrates this point. Dish was championed by the FCC and DOJ during the T-Mobile and Sprint merger negotiations as a new competitor to the big three, and ensuring Dish's ability to compete was a prerequisite for the agencies to approve of T-Mobile and Sprint's merger.[134] T-Mobile made promises that were monitored and requested by these agencies to subsidize Dish into the role as fourth competitor.[135] Even with the conscious backing of two federal agencies, concessions and aid from two of the largest competitors in the industry, and key wireless spectrum assets to create its own 5G network offered to Dish at significant discount, Dish has still failed to pose a legitimate competitive threat to Verizon, AT&T, and the new-look T-Mobile as of mid-2024.[136] This is because they have been unable to establish their own 5G infrastructure to break away from reliance on T-Mobile's infrastructure.[137]

Dish is a multi-billion-dollar company backed by two federal agencies who provided them cheap access to necessary infrastructure to implement 5G. Even so, Dish could not compete with the big three. This suggests that if Dish cannot compete in the 5G industry given these facts, seemingly nobody can as the 1996 Act currently stands. Therefore, the 1996 Act needs to be amended to account for the massive barrier of entry to the telecommunications industry.

---

131. *See* QUALCOMM, *supra* note 101.

132. *See* Lisa Schwartz, *Top 24 Challenges Facing the Telecom Industry Today*, ORACLE NETSUITE (June 11, 2024), https://www.netsuite.com/portal/resource/articles/erp/telecom-industry-challenges.shtml [https://perma.cc/S3FX-4T9R].

133. *See* Chuck Moozakis, *Enterprise 5G: Guide to Planning, Architecture, and Benefits*, TECHTARGET (Dec. 8, 2023), https://www.techtarget.com/searchnetworking/Enterprise-5G-Guide-to-planning-architecture-and-benefits [https://perma.cc/RE44-ZQUX] (detailing necessary infrastructure needed to properly establish 5G).

134. *See* U.S. Dep't of Just., *supra* note 17.

135. *See id*.

136. *See* Hardesty, *supra* note 18.

137. *See* Lumb, *supra* note 16 (describing the shortcomings of the negotiations during the T-Mobile/Sprint merger).

3. The Paradox of Interconnection with Incumbents

Third, amendments to the 1996 Act need to solve the strange economic situation brought by the current interconnection system where "new entrants" are not legitimate competition due to their reliance on incumbent infrastructure. This problem must be solved by balancing the interests of newcomers and incumbents as equally as possible. This situation is best illustrated by Dish's current reliance on T-Mobile's telecommunications infrastructure as a "hybrid" MVNO.[138] This situation also existed with Mint Mobile before it was bought by T-Mobile.[139] While Mint Mobile appeared to be its own independent and fast-growing company, it was essentially T-Mobile in disguise due to Mint Mobile operating entirely on T-Mobile's nationwide infrastructure.[140]

However, it is important to note that Mint Mobile, unlike Dish, is categorized as a "pure MVNO" in that they merely purchase wholesale wireless service, and do not build or maintain their own network infrastructure.[141] This Note's proposed changes to the 1996 Act are not targeted at pure MVNO firms, as these entities may decide their preferred method of business. Instead, this Note proposes reforms to the 1996 Act that specifically impact hybrid MVNOs, like Dish, who are relying on Section 251's interconnection provisions while actively intending to build their own infrastructure.

Current interconnection rates considered fair and reasonable are likely not low enough for industry newcomers to also undertake significant investment to build telecommunications infrastructure alongside their business operations and emerge as legitimate long-lasting competitors.[142] However, an attempt to change the pricing regime in favor of newcomers presents a concerning situation where the Act would essentially be forcing incumbents to subsidize their own potential competitors with absolutely no benefit to themselves, which is analogous to a government taking without fair compensation. This situation presents a unique paradox where seemingly the only means of a newcomer gaining traction in the industry is through the very support of firms they compete directly against.

To solve this paradox, an additional provision must be added to the Act that strikes a balance between ensuring that potential industry newcomers are able to emerge as legitimate competition while offering some level of incentive and benefit to incumbents for funding a newcomer's ability to do so. To attempt to solve this issue is incredibly complex, but clearly requires substantial change from the current 1996 Act's status quo.

---

138. *See* FCC 2022 Communications Marketplace Report, *supra* note 58, at 52-53.
139. *See id.*
140. *See id.*
141. *See id.* at 52.
142. *See* Mondliwa, *supra* note 7.

4. The 1996 Act's Present Shortcomings

The Telecommunications Act of 1996 is clearly outdated and unequipped to address the competition in the current state of the telecommunications industry. Consider again the T-Mobile/Sprint decision.[143] The Act, whose stated purpose was literally to promote competition in the telecommunications industry, *was not mentioned a single time in the entire opinion by the U.S. District Court for the District of Columbia's opinion*.[144] Rather, the court relied entirely on antitrust law guided by Section 7 of the Clayton Act in making their decision.[145] If this complete lack of consideration of the 1996 Act in the most pressing telecommunications competition case of the century does not prove that the Act needs updating to achieve its goal, nothing will.

B. Pro-Competitive Reforms to the 1996 Act

The Telecommunications Act of 1996 failed in promoting competition for telecommunications services as we know it today. Thus, lawmakers must shift their attention to amending the Act to ensure vigorous competition and opportunity for new market entrants while accounting for the massive barriers of entry into the telecommunications industry.

To do this, this Note argues that Section 251's language needs to be amended with specific language that reflects the ubiquitous 5G broadband capabilities currently dominating the telecommunications industry, alongside open-ended flexible language that ensures that the Act is equipped to cover future telecommunications technology that is not yet operational in the market. Further, this Note argues for further provisions to be added that allows for newcomers to use incumbent facilities at a steeply discounted cost for a ten-year period, with the caveat that newcomers must invest in their own infrastructure and pay incumbents back generously in following years. These amendments are to ensure that potential new competitors can enter the industry for feasible investment prices and to restrict even further consolidation and control of the industry into the hands of Verizon, AT&T, and T-Mobile.

This newcomer-favorable provision should be balanced with a provision that offers incentive for incumbents to subsidize their potential future competition, namely by requiring that the newcomers pay the incumbent organization annually for fifteen years after the newcomer operates on their own infrastructure at a steep interest rate, with the incumbent's cost of allowing the newcomer to use their facilities acting as the basis for the accruing interest.

Through these reforms, newcomers will be able to invest their profits during the ten-year period into rapid infrastructure development and emerge

143. *See generally Deutsche Telekom AG*, 439 F. Supp. 3d 179.

144. *See generally* 47 U.S.C. §§ 251-271); *see generally Deutsche Telekom AG*, 439 F. Supp. 3d 179.

145. *See Deutsche Telekom AG*, 439 F. Supp. 3d at 249.

as legitimate long-lasting competitors, all while being required to handsomely reimburse the incumbents for their interconnection services that were provided during the newcomers' building period.

1. Updating Language to Address the Technological Present and Future

Section 251(a) of the Act describes that telecommunications carriers have a general duty to interconnect with the facilities and equipment of other telecommunications carriers.[146] Sections 251(c)(2)(C)-(D) further describe that ILECs have a duty to provide facilities and equipment for any requesting telecommunications carrier equal to the quality provided to the local exchange carrier itself, and on rates, terms, and conditions that are reasonable and nondiscriminatory subject to arbitration by a neutral State commission.[147]

First, I argue that Section 251(c)(2)'s language pertaining to interconnection needs to be changed to require any organization who has "access to infrastructure, networks, facilities, or other equipment necessary for the delivery of broadband capabilities and telecommunications to customers" to provide access to those commodities by "any requesting telecommunications carrier." Other language regarding quality of service and reasonability of pricing of access to these facilities contained in subsections (C) and (D) would be maintained.[148] The goal of this updated language is to encompass present 5G broadband technology that is ubiquitous in the modern telecommunications industry and continues to grow in relevance since its inception in 2019. Further, 5G broadband is considered a flexible technology that is specifically designed to be able to maintain its relevance and usefulness through innovation. Therefore, it is crucial that interconnection for 5G-based infrastructure is ensured to maintain potential for competition in future telecommunications technologies that are not yet in operation.

I would also change the outdated language of Section 251(h) that defines "incumbent local exchange carrier."[149] This "incumbent local exchange carriers" definitional language should be changed to "organizations offering telecommunications and/or broadband services to consumers." This broader term will serve to ensure that the 1996 Act holds jurisdiction over all organizations that provide telecommunications services rather than relying on the anachronistic language of "local exchange carriers" that modern day telecommunications companies could subvert due to the Act's limited language and almost thirty-year-old legislative history.

The 1996 Act should also update its definitions of "telephone exchange services" and "exchange access" located in Section 153 of the Act.[150] Both these terms are found in Section 251(c)(2)'s interconnection requirement, but

146. *See* 47 U.S.C. § 251(2).

147. *See* 47 U.S.C. §§ 251(c)(2)(C)-(D), 252(b)(1) (outlining specific duties telecommunications companies must abide by through the 1996 Act).

148. *See* 47 U.S.C. § 251(c)(2)(C)-(D).

149. *Id.* § 251(h).

150. *Id.* § 153.

none mention the existence of broadband technology, nor do they contain flexible language capable of ensuring that the 1996's Act's jurisdiction is retained over future technologies.[151]

Further, the 1996 Act should be amended to add the term "network" to its definitions located in Section 153 of the Act. There is currently no definition of "network" contained in Section 153, even though Section 251(c)(2) imposes a duty on incumbents to provide "interconnection with the local exchange carrier's *network*."[152] The 1996 Act should amend the language of each of these definitions to cover "infrastructure necessary for high-standard broadband performance, and other infrastructure necessary for contemporary telecommunications usage."

2. Increasing Deterrence through Fines, Transparency, And Consent Decrees

Second, this Note argues that additional provisions and amendments be added to Section 251(g) and Section 251(c)(2) of the Act to ensure incumbents comply with their interconnection duties. To do this, Section 251(g) should be amended to replace the preexisting language to make such restrictions and obligations set forth by Section 251 enforceable by a fine "amounting to five percent of a corporation's revenues for the fiscal year in which the violation occurred." While this penalty could amount to hundreds of millions of dollars and be considered harsh by some, it is simply to ensure that the preexisting provisions of the 1996 Act are followed.

Further, transparency of the prices is crucial to ensure fair dealing and nondiscriminatory rates that Section 251(c)(2)(D) calls for.[153] Therefore, I would add an additional provision to this section codified as Section 251(c)(2)(E), which would require that pricing arrangements between incumbent telecommunications organizations and hopeful competitors are reported to the FCC, who then make the pricing arrangement publicly accessible. This provision hopes to restrict incumbent telecommunications organizations from offering better prices for preferred customers.

Next, I urge Congress to add an additional subsection provision to Section 251(g): Section 251(g)(1). This subsection should specify that if a company violates Section 251(c)(2)'s requirement for interconnection, in addition to the five percent fine of that company's revenues for the fiscal year, the violating entity will be required to negotiate a consent decree with the FCC. This consent decree is required to expire no later than ten years from its established date, requires bi-annual reporting to the FCC regarding facility usage, and establish a heightened fine of ten percent of that company's yearly

151. *See id.* § 251(c)(2).

152. *Id.* §§ 153, 251(c)(2).

153. *See* INFODEV, TELECOMMUNICATIONS REGULATION HANDBOOK MODULE 3: INTERCONNECTION 3-7 (Hank Intven & McCarthy Tétrault, 2000), https://www.itu.int/ITU-D/treg/Documentation/Infodev_handbook/3_Interconnection.pdf [https://perma.cc/V3B3-VNHP] (supporting the need for transparency of prices to ensure fair dealing between incumbents and new market entrants); *see also* 47 U.S.C. § 251(c)(2)(D).

revenue if a second violation is found during the consent decree's controlling period. If additional provisions beyond the minimum described cannot be agreed upon by the FCC and the violating party through voluntary negotiations outlined in Section 252(a)(1) of the 1996 Act, deliberations regarding additional terms of the consent decree should be completed through arbitration as described by Section 252(b)(1) of the Act.[154]

The inspiration behind implementation of a consent decree after a violation of the interconnection standard's new terms comes from FTC and FCC enforcement actions. Consider the FTC's past privacy enforcement actions. The FTC enforces Section 5 of the FTC Act, which grants the FTC the authority to regulate "unfair or deceptive" acts or trade practices.[155] Consent decrees operate similarly to settlements, acting as an agreement between the agency and the party at fault to outline consequences and rules for their required behavior moving forward after their first violation.[156] Consent decrees can add major monetary penalties for a second violation, acting as an impactful deterrence strategy. For example, in 2019 Facebook made a record-breaking settlement with the FTC by agreeing to pay $5 billion for violating the FTC's 2012 order against them after their first privacy violation charge.[157]

FTC consent decrees can also impose monitoring, compliance, and program requirements upon the violating organizations. For example, in 2022 the FTC alleged that Twitter violated its 2011 consent decree with the FTC.[158] Twitter agreed to pay the FTC $150 million and agreed to an updated consent decree that was to last for an added twenty years.[159] The consent decree also requires that Twitter create a "comprehensive privacy and security program," and report to the FTC within thirty days of any occurrence of an incident that was agreed upon in their negotiations.[160]

The purpose of imposing a consent decree requirement unto telecommunication companies if they fail to comply with interconnection mandates is to produce additional non-monetary costs if that company is a repeat offender. While the five percent yearly revenue payment is already costly, increasing the cost of a second offense through even more payment,

---

154. *See* 47 U.S.C. § 252(a)(1), (b)(1).

155. *FTC Consent Decrees are Best Guide to Cybersecurity Policies*, BOIES SCHILLER FLEXNER (Sept. 22, 2015), https://www.bsfllp.com/news-events/ftc-consent-decrees-are-best-guide-to-cybersecurity-policies.html. [https://perma.cc/5URZ-8GAJ] (showing a method the FTC uses to enforce a specific power it holds).

156. *See id.* (analogizing consent decrees with an example).

157. *See* Lesley Fair, *FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making*, FED. TRADE COMM'N (July 24, 2019), https://www.ftc.gov/business-guidance/blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-and-history-making. [https://perma.cc/6V4Z-3KCX] (detailing a specific result of a consent decree).

158. *See* Letter from Cheyenne Hunt, Big Tech Accountability Advocate, Pub. Citizen, to Lina Khan, Fed. Trade Comm'n Chair, and Merrick Garland, Attorney Gen. (Mar. 13, 2023) (on file with the website of Public Citizen) (detailing further example of a consent decree in action).

159. *See id.* (showing an example of a time period used for a consent decree).

160. *Id.* (noting forced creation of programs to satisfy compliance).

along with time-consuming compliance measures, hopes to add another layer of incentive and deterrence to comply with Section 251.

3. Imposing Significantly Discounted Interconnection Access

Further, I argue that the FCC needs to enforce *significantly* discounted access to incumbent organizations' infrastructure for the first ten years, with the accompanying requirement that the newcomer be off the incumbent's infrastructure completely after those ten years. This provision would be added on to Section 251's preexisting interconnection requirement. As exemplified by Dish's attempt to enter the telecommunications industry, it is extremely difficult to gain a foothold in the industry even with fair and reasonable prices negotiated by the FCC and DOJ.[161] Therefore, I believe the FCC should lower the threshold for what price meets its rates, terms, and conditions for access to incumbent facilities.

However, this benefit to newcomers comes at a caveat: they need to operate on their own infrastructure after ten years of discounted usage of the incumbent facilities. Meaning, while they operate on a cheap basis for ten years through the incumbent's infrastructure, the newcomer market entrant needs to offset that cost by investing heavily in their own infrastructure to become *actual* competition after the ten-year period rather than posing as the big three in disguise, like Mint Mobile.[162]

However, the requirement that the new firm be off the incumbent's infrastructure after ten years would apply strictly to hybrid MVNO's, like Dish, whose business plan is to build their own network.[163] This provision is not intended to apply to pure MVNOs, like pre-buyout Mint Mobile, whose goal was to purchase wireless services wholesale from facilities-based provider T-Mobile and resell those services to consumers, without any intention to build their own physical infrastructure.[164] Rather, these reforms are designed to maintain the ability for companies to pursue the pure MVNO business model while providing rules beneficial to those attempting to become independent infrastructure operators. Therefore, these reforms would not change pure MVNOs' interconnection rates that are the current norm, nor would the reforms have a requirement to halt their usage of incumbent infrastructure after ten years.

4. Solving the Paradox of Interconnection With Incumbents

Further, I argue that there needs to be an award to the incumbent for essentially subsidizing an emerging competitor to their telecommunications

161. *See* Hardesty, *supra* note 18; *see also* Schwartz, *supra* note 132.
162. *See* FCC 2022 Communications Marketplace Report, *supra* note 58, at 52-53.
163. *See id.*
164. *See id.*

market through the severely steep discounted interconnection price afforded to newcomers. To address this, this Note proposes that another provision be added alongside the discounted access for the ten-year period in Section 251. This added provision would require the newcomer to *pay back* the incumbent for what it had cost them to support the newcomer's usage of their facilities.

This price cannot simply be paying the incumbent back equally to what it cost them (inflation included) or following interest rate standards set by the Federal Reserve. Rather, the money owed must be calculated at a steep interest rate to account for the fact that because of their support, though legislatively required, a new competitor may emerge. Further, this payment period would last for fifteen years, which is five years longer than the newcomer is able to use their facilities. For the final five years, the industry newcomer would be required to pay the incumbent a certain percentage of their yearly revenue to be determined by the FCC. The goal of these provisions is to add a layer of benefit to the incumbent carriers to make up for the cost incurred from hosting a newcomer on their facilities and having a competitor in the industry afterward.

5. Preventing Reconsolidation

Lastly, there needs to be a preventive measure to ensure that telecommunications newcomers do not simply merge with current incumbents during any point of this new process, as the BOCs did shortly after the passage of the 1996 Act.[165] To prevent reconsolidation, a final provision would be added that restricts telecommunications organizations who utilized the newly implemented Section 251 discount from merging with any other telecommunications organizations who maintain a certain level of infrastructure or facilities. This provision will hopefully result in the addition of more competitors into the telecommunications landscape balanced with the inability to revert to the consolidated industry that these new provisions were created to address.

C. The Purpose of Reform

The central goal of modernizing the language of Section 251, increasing the penalties for incumbent telecommunication carriers that violate it, offering discounted access to the incumbent organizations with the requirement to create their own infrastructure, and restricting mergers involving industry newcomers is to even the playing field for fresh competition in the industry. For competition to thrive, or even exist, in the telecommunication industry, there needs to be an actual potential for new competition in the first place.

AT&T, Verizon, and T-Mobile had a decade-spanning head start to build telecommunications facilities, which originated from the 1984 divestiture of AT&T. The only feasible way that competitors can attempt to enter the modern-day telecommunications industry is through using these big

165. *See* Whalley & Curwen, *supra* note 6, at 158.

three's infrastructure in hopes of eventually amassing enough capital to build and maintain their own crucial infrastructure. Even with government assistance in helping achieve this aim, it's a daunting task. As exemplified by cable giant Dish's miserable progress in attempting to enter the industry through the Boost Mobile brand and discounted access to the big three's 5G capabilities, entering the market is difficult, even with the right tools. Through these proposed amendments to the Telecommunications Act of 1996, some semblance of an opportunity to enter the concentrated telecommunications market will be available for those daring to try.

IV. CONCLUSION

The telecommunications industry is highly complex due to its unique requirement for comprehensive infrastructure and need for massive investment to acquire such infrastructure. Today, that infrastructure and resulting market share is almost exclusively held by three major players: AT&T, Verizon, and T-Mobile. The reason for this can be traced to history. The 1984 divestiture led to government sponsored quasi-monopolies defined by different regions. The 1996 Telecommunications Act then attempted to fix this monopolized industry by lifting regulation to open the door for competition. This legislation backfired.

Changes must be made to the 1996 Telecommunications Act to achieve a competitive telecommunications industry that the 1996 Act had hoped to achieve. The Act's language must be updated to reflect the realities of the current state of telecommunications technology, and the approach to achieving increased competition in the industry must be changed through promoting the ability for newcomers to enter the industry balanced with incentive for incumbent organizations to support them. Through these changes, vast amounts of competitors in the telecommunications industry may be able to emerge and persist, resulting in an even deeper drive for industry players to innovate cutting-edge telecommunications offerings for the benefit of consumers everywhere.

Addressing Gender Bias in Voice Assistants: European Advertising Nondiscrimination Laws as a Framework for Regulation

Ellen Manby*

TABLE OF CONTENTS

* J.D., May 2025, The George Washington University Law School; B.B.A. 2018, The George Washington University. Thank you to the FCLJ Editorial Board for all their help and support with this note. A special thank you to my parents, my sister, and Sam for all your love and encouragement during my law school journey. And to Alexis, Cait, Sierra, and Trish - I am so grateful to have had you by my side for these three years.

I. INTRODUCTION

On November 22, 2019, Ruth George, a sophomore student at the University of Illinois at Chicago, left a meeting with her professional fraternity and used a ride-sharing app to get to her car in a parking garage a few blocks away.[1] Upon arriving at the garage, she was catcalled by a passerby.[2] When she chose to ignore him, rather than engage him or thank him, the catcaller became enraged, followed her into the garage, and choked her to death.[3] Unfortunately, this tragedy is not an outlier.[4] It fits into a catalog of incidents where verbal harassers become enraged and incredulous when women do not respond to unsolicited and unwanted compliments with politeness and gratitude.[5] That catalog illustrates the damaging and sexist societal expectation that women should respond positively, even with gratitude, to these kinds of comments.[6]

Even after societal movements like #MeToo and public reckoning with the continued presence of sexism in society, the issue of sex discrimination persists.[7] The Merriam-Webster Dictionary defines sexism as "1. prejudice or discrimination based on sex, especially against women," and "2. behavior, conditions, or attitudes that foster stereotypes of social roles based on sex."[8] Gender Discrimination is defined in that same dictionary as "discrimination based on sex and especially against women."[9] A 2023 study by MIT Sloan, the School of Business at the Massachusetts Institute of Technology, showed that women experience toxic workplace culture at a rate forty-one percent

1. *See Julie* Bosman, *A College Student Was Killed by a Man Whose Catcalls She Tried to Ignore, Prosecutors Say*, N.Y. TIMES (Nov. 27, 2019), https://www.nytimes.com/2019/11/27/us/chicago-college-student-killed-catcall.html [https://perma.cc/V3E6-CVBV]; *see also* Mike Puccinelli, *Man Accused of Killing Chicago College Student After She Ignored His Catcalls*, CBS NEWS (Nov. 27, 2019), https://www.cbsnews.com/video/man-accused-of-killing-chicago-college-student-after-she-ignored-his-catcalls/ [https://perma.cc/9Z69-YL78].

2. *See* Bosman, *supra* note 1.

3. *See id.*

4. *See* Claretta Bellamy & Uwa Ede-Osifo, *'Brickgate' Revives an Age-old Argument Between Black Men and Women*, NBC NEWS (Sept. 26, 2023), https://www.nbcnews.com/news/nbcblk/brickgate-revives-age-old-argument-black-men-women-rcna104423 [https://perma.cc/B7BM-PHAX].

5. *See id.*; *see also* Ayesha Roscoe, *The Sunday Story: This is What it Feels Like to be Catcalled*, NPR (Oct. 29, 2023), https://www.npr.org/2023/10/29/1198908962/cap-radio-this-is-what-it-feels-like-catcalling [https://perma.cc/54K9-KBQG].

6. *See* Rosa Inocencio Smith, *The Sexism of Telling Women to Smile*, ATLANTIC (Oct. 4, 2016), https://www.theatlantic.com/politics/archive/2016/10/the-sexism-of-telling-women-to-smile/623090/ [https://perma.cc/G6TB-7V32].

7. *See 'Me Too.' Global Movement*, GLOB. FUND WOMEN, https://www.globalfundforwomen.org/movements/me-too/ (last visited Nov. 20, 2023) [https://perma.cc/B28E-BTSW].

8. *Sexism*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/sexism (last visited Mar. 1, 2024) [https://perma.cc/2VW2-8WP3].

9. *Sex Discrimination*, MERRIAM-WEBSTER, https://www.merriam-webster.com/legal/sex%20discrimination (last visited Mar. 1, 2024) [https://perma.cc/H2AX-MSJB].

higher than men.[10] In its 2023 Report on Pay Equity, Visier, a company focused on workforce analytics, reported a reversal in progress towards bridging the gap between genders for compensation, as their research showed a widening pay disparity.[11] In the STEM field alone, women are drastically underrepresented, with only about one in five students being women in the fields of computer sciences, engineering, and technology.[12] A study conducted by Stanford University's Clayman Institute for Gender Research shed light on how gender discrimination comes through in women's performance reviews.[13] The research found that "managers are significantly more likely to critique female employees for coming on too strong," and that women received "2.5 times the amount of feedback men did about aggressive communication styles."[14] Further, women were described as "helpful" at double the frequency that men were.[15] These studies are troubling, as they illustrate how deeply entrenched gender-based biases translate into double standards in the workplace—specifically in the unequal expectation of women to be more polite and helpful coworkers than their male counterparts.[16] In recent years, such gender inequities have been exacerbated by the biases of technology, and will continue to worsen without government intervention in the form of regulatory action.[17]

Beyond the context of the workplace or receiving a compliment in public, women face heightened expectations to be pleasant, polite, and obedient.[18] In recent years, this inequity has been exacerbated by the sexist

---

10. *See* Donald Sull & Charles Sull, *The Toxic Culture Gap Shows Companies Are Failing Women*, MIT SLOAN MGMT. REV. (Mar. 14, 2023), https://sloanreview.mit.edu/article/the-toxic-culture-gap-shows-companies-are-failing-women/ [https://perma.cc/8885-K2MT].

11. *See* VISIER, THE STATE OF PAY EQUITY IN 2023: THE WAGE GAP BETWEEN WOMEN AND MEN WIDENS, at 2 (2023), https://assets.ctfassets.net/lbgy40h4xfb7/2gBq4yKWiG2yOZjTaz1KiW/36401965ad35ce06632580eb05298b2a/VISIER-insights-report-state-of-pay-equity-2023.pdf [https://perma.cc/67DG-USNQ].

12. *See Women in STEM Statistics: Key Statistics*, STEM WOMEN (June 22, 2022), https://www.stemwomen.com/women-in-stem-percentages-of-women-in-stem-statistics [https://perma.cc/J8CX-UDGK].

13. *See* Rachel Emma Silverman, *Gender Bias At Work Turns Up in Feedback*, WALL ST. J., https://www.wsj.com/articles/gender-bias-at-work-turns-up-in-feedback-1443600759 (last updated Sept. 30, 2015, 5:44 AM) [https://perma.cc/7CKQ-M9VF].

14. *Id.*

15. *See id.*

16. *See id.*

17. *See* Sonia Elks, *Hey Siri, You're Sexist, Finds U.N. Report on Gendered Technology*, REUTERS (May 22, 2019), https://www.reuters.com/article/us-global-women-technology/hey-siri-youre-sexist-finds-u-n-report-on-gendered-technology-idUSKCN1SS2C7/ [https://perma.cc/4AHV-9JV6]; *see also* Joan Goodchild, *Gender Bias in AI: 'Where Are All the Women?'*, SC MAG. (Sept. 27, 2023), https://www.scmagazine.com/feature/gender-bias-in-ai-where-are-all-the-women [https://perma.cc/D484-7RG5].

18. *See* Brijana Prooker, *It's Time For Women To Break Up With Politeness*, ELLE (Apr. 14, 2021), https://www.elle.com/culture/a35854625/no-more-politeness-2021/ [https://perma.cc/29PA-4BZE].

biases that are baked into the functions of everyday technology.[19] Many emerging technologies rooted in artificial intelligence are positioned as "assistants," communicating to users with a default female voice that responds to everyday requests and questions in an eager and polite tone.[20] Voice assistant technology is the foremost example of this.[21] While perhaps an unintentional programming effect, voice assistants are carrying forward harmful female behavioral conditioning in the way they have been programmed.[22] When interviewed about the societal expectations that women be polite, Dr. Leela Magavi, a psychiatrist who studied at Johns Hopkins University, said, "[d]uring childhood and adolescence, girls are socialized to respond to individuals' remarks in a courteous manner, irrespective of the content. Over time, young girls evolve into women who prioritize other individuals' comfort and emotions over their own."[23] These behavioral gender biases have infiltrated voice assistant technology, which have quickly come to play a central role in the home, the office, and beyond.[24]

The federal government and its agencies are responsible for creating and implementing regulations that guide the function of voice assistants and protect against implicit reinforcement of harmful gender stereotypes.[25] In crafting this legislation, the government should look to European laws regulating the prevalence of gender stereotypes in media and advertising. The regulatory language of the United Kingdom's Committees of Advertising Practice ("CAP") Harm and Offence Rule 4.9 and Norway's Marketing Control Act both aim to reduce gender bias in advertising.[26] Such language

19. *See* Elks, *supra* note 17.

20. *See* Kinza Yasar & Bridget Botelho, *What is an AI Assistant?*, TECH TARGET, https://www.techtarget.com/searchcustomerexperience/definition/virtual-assistant-AI-assistant (last visited Apr. 9. 2025, 6:29 PM) [https://perma.cc/K6Q6-5W2J]; *see also* Elks, *supra* note 17.

21. *See* Yasar & Botelho, *supra* note 20.

22. *See* Leah Fessler, *We Tested Bots Like Siri and Alexa to See Who Would Stand Up to Sexual Harassment*, QUARTZ (Feb. 22, 2017), https://qz.com/911681/we-tested-apples-siri-amazon-echos-alexa-microsofts-cortana-and-googles-google-home-to-see-which-personal-assistant-bots-stand-up-for-themselves-in-the-face-of-sexual-harassment [https://perma.cc/95VV-38U7].

23. Prooker, *supra* note 18.

24. *See* Max Roser, *Technology Over the Long Run*, OUR WORLD DATA (Feb. 22, 2023), https://ourworldindata.org/technology-long-run [https://perma.cc/ZRV3-H2T3]; *see also* Elks, *supra* note 17; *see also* Larry Hardesty, *Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems*, MIT NEWS (Feb. 11, 2018), https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212 [https://perma.cc/UGT6-85G9].

25. *See* Joshua Meltzer, *The US Government Should Regulate AI if it Wants to Lead on International AI Governance*, BROOKINGS (May 22, 2023), https://www.brookings.edu/articles/the-us-government-should-regulate-ai/ [https://perma.cc/ZN2U-EJFW]; *see also Government Regulation*, POL'Y CIRCLE, https://www.thepolicycircle.org/brief/government-regulation/ (last visited May 12) [https://perma.cc/WH4E-2NNR].

26. *See Guidelines on Sexist Advertising*, NORWEGIAN CONSUMER AUTH. (Apr. 13, 2009), https://www.forbrukertilsynet.no/english/guidelines/guidelines-on-sexist-advertising (last visited Apr. 7, 2024) [https://perma.cc/D34Q-J4E4]; *see also Harm and Offence*, ADVERT. STANDARDS AUTH. (Aug. 7, 2023), https://www.asa.org.uk/type/non_broadcast/code_section/04.html [https://perma.cc/QX72-64B7].

offers a useful framework for the United States to address gender bias in voice assistant technology. This Note will first explore the rules, guidelines, and applications set forth by European regulations and how they can serve as a framework for similar regulations in the United States aimed at curbing the gender-discriminatory effects of voice assistant technology. The language and standards set forth by European regulations can and should be applied directly to voice assistant technology to curb its discriminatory effects in regulation put forth by the United States.

II. BACKGROUND

Voice assistants, like Siri and Alexa, represent one segment of the rapid technological growth our society has experienced in recent years.[27] Forecasts estimate that there are more than 132 million current users of voice assistant technology, with that number only expected to grow in the near future.[28] As of 2019, smart speakers, which utilize built-in voice assistants like Siri and Alexa, have found their way into twenty-five percent of households in America.[29] A more recent study by NPR found that thirty-five percent of Americans own a smart speaker.[30] Voice assistant technology is not immune from gender bias, and in fact has provided some of the most stunning examples of its prevalence in technology.[31]

A. The Problematic and Damaging Nature of Voice Assistants' Default Responses and Female Tone

The default setting of voice assistants to speak in a female tone, as well as the responses they have been programmed with, have combined to create a problematic dynamic between the technology and its users. Since their

27. *See* Vantage Market Research, *Voice Assistants Market Size & Share to Surpass $22.2 Billion by 2030*, GLOBENEWSWIRE (May 31, 2023), https://www.globenewswire.com/news-release/2023/05/31/2679109/0/en/Voice-Assistants-Market-Size-Share-to-Surpass-22-2-Billion-by-2030-Vantage-Market-Research.html [https://perma.cc/7SVD-6RBZ].

28. *See* James Wohr, *Voice Assistants: What They Are and What They Mean For Marketing and Commerce*, INSIDER INTEL. (Oct. 17, 2023), https://www.insiderintelligence.com/insights/voice-assistants/ [https://perma.cc/9WFK-RJ3C].

29. *See* Brooke Auxier, *5 Things to Know About Americans and Their Smart Speakers*, PEW RSCH. CTR. (Nov. 21, 2019), https://www.pewresearch.org/short-reads/2019/11/21/5-things-to-know-about-americans-and-their-smart-speakers/ [https://perma.cc/Z5TN-TYVC]; *see also* Holly Pyne, *What Is A Smart Speaker And How Do They Work?*, RADIO TIMES (Sept. 7, 2020), https://www.radiotimes.com/technology/what-is-a-smart-speaker/ [https://perma.cc/6EDX-4WQH].

30. *See Smart Speaker Ownership Reaches 35% of Americans*, NPR (June 16, 2022), https://www.npr.org/about-npr/1105579648/npr-edison-research-smart-speaker-ownership-reaches-35-of-americans [https://perma.cc/B9U6-JUK8].

31. *See* Elks, *supra* note 17.

launch, voice assistants have had a female voice.[32] Years later, that default for Siri and Alexa remains, although many voice assistants now provide customers the option to adjust the voice to different genders and accents.[33] Three years after its release, Alexa responded with "that's nice of you to say" when told she was hot.[34] In response to being told she was a slut or receiving a request for sexual activity, voice assistant Siri said "I'd blush if I could."[35] That same answer was also given if a user told Siri "you're a b*tch."[36] These responses reinforce expectations that women should be both polite and obedient, even in the face of unwelcome or offensive comments.[37] Voice assistant creators have since re-programmed the technology to provide disengaging statements in response to comments like these, rather than gratuitous replies.[38] However, the effects of voice assistant technology on reinforcing gender stereotypes extend beyond their programmed responses.[39]

Because most voice assistants default to a female tone, the technology subconsciously teaches its users acceptable expectations and communication with female voices, and in turn, female humans.[40] In his book, *Wired for Speech*, Clifford Nass writes that "people tend to perceive female voices as helping us solve our problems by ourselves, while they view male voices as authority figures who tell us the answers to our problems. We want our technology to help us, but we want to be the bosses of it, so we are more likely to opt for a female interface."[41] This demonstrates that users prefer to interact with a female voice, as market research indicates, because of its association with being helpful and subservient.[42]

Research by Calvin Lai, a professor of psychological and brain science who specializes in hidden forms of prejudice and discrimination, has demonstrated that an individual's exposure to a certain gender association is positively correlated with the likelihood that they adopt that association in

---

32. *See* Caitlin Chin-Rothmann & Mishaela Robison, *How AI Bots and Voice Assistants Reinforce Gender Bias*, BROOKINGS (Nov. 23, 2020), https://www.brookings.edu/articles/how-ai-bots-and-voice-assistants-reinforce-gender-bias/ [https://perma.cc/S86U-2SUK].

33. *See id.*

34. Fessler, *supra* note 22; *see also* Brandon Vigliarolo, *Amazon Alexa: Cheat Sheet*, TECH REPUBLIC (Sep. 24, 2020), https://www.techrepublic.com/article/amazon-alexa-the-smart-persons-guide/ [https://perma.cc/A9CZ-VC22].

35. Fessler, *supra* note 22.

36. *Id.*

37. *See id.*

38. *See id.*

39. *See generally* CLIFFORD NASS & SCOTT BRAVE, WIRED FOR SPEECH 29 (2006).

40. *See* Jessi Hempel, *Siri and Cortana Sound Like Ladies Because of Sexism*, WIRED MAG. (Oct. 28, 2015), https://www.wired.com/2015/10/why-siri-cortana-voice-interfaces-sound-female-sexism/ [https://perma.cc/C8ZE-ENSE]; *see also* Calvin Lai & Mahzarin Banaji, *The Psychology of Implicit Intergroup Bias and the Prospect of Change*, *in* DIFFERENCE WITHOUT DOMINATION: PURSUING JUSTICE IN DIVERSE DEMOCRACIES 14-16 (D. Allen & R. Somanathan eds., 2020) (discussing implicit bias research that has shown that environmental stimuli inform and reinforce implicit biases and associations, while stimuli that counters existing associations can help to reduce them); *see also Implicit Bias*, AM. PSYCH. ASS'N, https://www.apa.org/topics/implicit-bias (last visited Oct. 2, 2024) [https://perma.cc/2HAU-6RLJ].

41. NASS & BRAVE, *supra* note 39; *see also* Hempel, *supra* note 40.

42. *See* Hempel, *supra* note 40.

their own minds.[43] Applying this principle to the gender-based responses of voice assistants supports the likelihood that by programming female voices to be pleasant, helpful, and obedient, the technology implicitly teaches its users what they can expect from female voices and females more broadly outside of the technology.[44] Even to everyday requests, voice assistants respond in a default-female tone, with a sense of eagerness and helpfulness, and without any agency to deviate from that pattern.[45] As users are under no obligation to address voice assistants in a polite or conversational manner, a voice assistant's eager and helpful reply is not dependent on having been asked a request in a respectful way.[46] This further engrains users' subconscious associations of women as subservient, polite, and eager to help.[47] As the use of voice assistants continues to expand, its creators, users, and the governmental bodies responsible for its regulation should be deeply concerned about the gendered expectations, assumptions, and stereotypes that the technology reinforces.[48] Thus, the following section will discuss the need for U.S. regulation in this field, specifically exploring European laws against gender discrimination in advertising as a framework for that regulation.

III. ANALYSIS

A. European Laws Against Gender Discrimination in Advertising Should Serve as a Framework for U.S. Regulation of Voice Assistants' Gender Discriminatory Effects.

The previous section laid out the reasons why voice assistant technology is on track to negatively impact society, specifically in terms of perpetuating gender bias, if it is left unregulated. This section will further emphasize the need for regulation while exploring European anti-discrimination laws that can serve as a guiding model for that framework. Major news sources have reported that while the United States is rapidly adopting emerging technologies like artificial intelligence and the devices that leverage it, it is also quickly falling behind its peer countries in regulating their use.[49] Even the countries that are leading the way in artificial intelligence regulation have focused their efforts on accounting for transparency, security,

43. *See* Lai & Banaji, *supra* note 40, at 14-16; *see also* AM. PSYCH. ASS'N, *supra* note 40; *see also* Sigal Samuel, *Alexa*, *Are You Making me Sexist?*, VOX (June 12, 2019), https://www.vox.com/future-perfect/2019/6/12/18660353/siri-alexa-sexism-voice-assistants-un-study [https://perma.cc/SZ2E-P3GJ].

44. *See* Lai & Banaji, *supra* note 40, at 14-16.

45. *See* MARK WEST ET AL., I'D BLUSH IF I COULD: CLOSING GENDER DIVIDES IN DIGITAL SKILLS THROUGH EDUCATION 113-114 (2019), https://unesdoc.unesco.org/ark:/48223/pf0000367416.page=1 [https://perma.cc/EQ5C-T6QA].

46. *See id.*

47. *See* Lai & Banaji 14-16, *supra* note 40; *see also* AM. PSYCH. ASS'N, *supra* note 40.

48. *See* WEST, ET AL., *supra* note 45, at 113-114.

49. *See* Cecilia Kang, *In U.S., A.I. Regulation is in its 'Early Days'*, N.Y. TIMES (July 21, 2023), https://www.nytimes.com/2023/07/21/technology/ai-united-states-regulation.html [https://perma.cc/TE9J-8WQV].

and data privacy, rather than confronting the ways in which the technology can exacerbate discrimination and gender bias.[50] Current U.S. regulations aimed specifically at combatting gender discrimination focus on its presence in the workplace, at school, and at home, and do not lend themselves to instances of discrimination within technology, especially those that are implicit and not targeted at an individual.[51]

Several European countries have led efforts to curb the effects of gender discrimination in the media, evident in the laws they have passed to reduce discrimination in advertising.[52] Voice assistants are the next frontier, requiring the United States to pass regulations aimed at curbing their gender discriminatory effects.[53] The approach taken by European laws in the realm of gender discrimination in advertising can and should be leveraged as a valuable framework from which such domestic regulations can evolve. Two examples of such European laws are described below.

In 2019, the United Kingdom's Advertising Standards Authority introduced Committees of Advertising Practice ("CAP") Rule 4.9, which aims to eliminate the presence of gender stereotypes in advertising.[54] This rule and its accompanying guidance lend themselves to applications beyond advertising, also regulating emerging technologies. Similarly, Norway's Marketing Control Act and its accompanying guidelines also serve as an effective framework for modeling United States regulations focused instead on gender discrimination in voice assistant technology.[55] Both regulations provide useful language and examine cases that illustrate their application, thereby providing a model for voice assistant technology regulation in the United States. The following two sections of this Note will explore these regulations in depth, beginning with the United Kingdom's CAP Rule 4.9 and followed by Norway's Marking Control Act.

---

50. *See* Hiroki Habuka, *Japan's Approach to AI Regulation and its Impact on the 2023 G7 Presidency*, CTR. STRATEGIC & INT'L STUD. (Feb. 14, 2023), https://www.csis.org/analysis/japans-approach-ai-regulation-and-its-impact-2023-g7-presidency [https://perma.cc/2G56-SW46].

51. *See Know Your Rights: Sex Discrimination,* ACLU (2023), https://www.aclu.org/know-your-rights/sex-discrimination [https://perma.cc/F5U2-FW76].

52. *See generally* Public Interest Litigation Project, *Legal Frameworks for Sexism in Advertising*, DUTCH SECTION INT'L COMM'N JOURNALISTS (2015), https://pilp.nu/wp-content/uploads/2023/10/150609-PILP-sexism-comparative-practice-memo1.pdf [https://perma.cc/8Q3E-7ACU]; *see also* CAP Executive, *Offence: Sexual Orientation and Gender Identity*, ADVERT. STANDARDS AUTH. (Aug. 7, 2023), https://www.asa.org.uk/advice-online/offence-sexual-orientation.html [https://perma.cc/YU4B-KGF8].

53. *See* Elizabeth Yin, Mary Moynihan & Alexandra Walsh, *Hey Siri. Are You Regulated?*, REGUL. REV. (Feb. 18, 2023), https://www.theregreview.org/2023/02/18/saturday-seminar-hey-siri-are-you-regulated/ [https://perma.cc/AS72-P496].

54. *See* CAP Executive, *supra* note 52.

55. *See The Marketing Control Act*, NORWEGIAN CONSUMER AUTH. (Apr. 11, 2016), https://www.forbrukertilsynet.no/english/the-marketing-control-act [https://perma.cc/WFH6-LP8S]; *see also* NORWEGIAN CONSUMER AUTH., *supra* note 26.

B. CAP Rule 4.9: The United Kingdom's Regulation Against Gender Discrimination in Advertising and its Potential for Application to Regulation of Voice Assistant Technology.

The United Kingdom's CAP Rule 4.9 states that "marketing communications must not include gender stereotypes that are likely to cause harm, or serious or widespread offense."[56] Alongside the issuance of the rule, the Advertising Standards Authority, which is responsible for the rule's application, explained the overall intent behind the regulation, asserting that the rule is based on the principle that "[m]arketers should take account of the prevailing standards in society and the context in which a marketing communication is likely to appear to minimize the risk of causing harm or serious or widespread offense."[57] The issuing authority provided guidance alongside their statement of the rule and its purpose to offer additional clarity and practical examples of its use.[58] The guidance asserts that advertisements should strive not to indicate that a stereotypical characteristic or role is "always uniquely associated with one gender" or that are the "only options available to one gender."[59] An example of a prohibited advertisement may be one that depicts a husband relaxing, while his children make a mess, and his wife as the individual responsible for tidying that mess.[60] In announcing the implementation of CAP Rule 4.9, Shahriar Coupal, the Director of the Committees of Advertising Practice, declared that "harmful gender stereotypes have no place in UK advertisements. Nearly all advertisers know this, but for those that don't, our new rule calls time on stereotypes that hold back people and society."[61]

Since its creation, CAP Rule 4.9 has been deployed several times to ban advertisements by major companies, including Volkswagen and Philadelphia Cream Cheese, that fell short of its standards.[62] In 2022, a Match.com advertisement was banned for its depiction of a woman eagerly performing helpful household tasks for her male partner, implying that her completion of these tasks increased her value as a partner.[63] Specifically, the advertisement "feature[ed] a woman performing subservient tasks for her partner such as

---

56. ADVERT. STANDARDS AUTH., *supra* note 26.

57. *Id.*

58. *See Advertising Guidance on Depicting Gender Stereotypes Likely to Cause Harm or Serious or Widespread Offence*, ADVERT. STANDARDS AUTH., https://www.asa.org.uk/static/6c98e678-8eb7-4f9f-8e5d99491382c665/guidance-on-depicting-gender-stereotypes.pdf (last visited Apr. 7, 2024) [https://perma.cc/28U3-5WTS].

59. *Id.*

60. *Id.*

61. *Harmful Gender Stereotypes in Ads to be Banned*, ADVERT. STANDARDS AUTH. (Dec. 14, 2018), https://www.asa.org.uk/news/harmful-gender-stereotypes-in-ads-to-be-banned.html [https://perma.cc/7KWT-2DQZ].

62. *See* Nick Breen & Jonathan Andrews, *Harmful Gender Stereotypes in Advertising: The First Rulings*, REEDSMITH (Aug. 21, 2019), https://www.reedsmith.com/es/perspectives/2019/08/harmful-gender-stereotyping-in-advertising [https://perma.cc/KK6S-32DN].

63. *See ASA Ruling on Match.com International Ltd t/a Match.com, Ourtime*, ADVERT. STANDARDS AUTH. (Oct. 5, 2022), https://www.asa.org.uk/rulings/match-com-international-ltd-a22-1160258-match-com-international-ltd.html [https://perma.cc/6GVK-BGPR].

making sure that football is on TV, and ensuring there are a fresh towel and socks ready for after his shower."[64] In its ruling, the United Kingdom's Advertising Standards Authority found that the advertisement depicted a female performing household chores, which is the kind of stereotypical gender role CAP Rule 4.9 seeks to eliminate.[65] The Authority reported that the fact that the domestic tasks portrayed in the advertisement were done to "please her male partner" and "were not reciprocated" supported their finding that a violation occurred.[66]

The regulations and accompanying standards set forth by CAP Rule 4.9, although written to curb the discriminatory effects of certain kinds of advertising, are directly applicable to the regulation of voice assistants. Instances of the rule's application shed further light on the ways in which it can be applied in the context of voice assistants. The United States should look to the language of CAP Rule 4.9 as a model for its own much-needed regulation of voice assistant technology and its gender-discriminatory implications. The exact same standard set forth by Rule 4.9 could be applied to voice assistants, asserting that voice assistants must not perpetuate gender stereotypes that are likely to cause harm or serious or widespread offense, nor perpetuate the proposition that a certain quality is always uniquely associated with one gender.[67] Similarly to how the UK has applied the rule to advertisements perpetuating gender stereotypes, it would be applied to the default setting of voice assistants to female, polite, and pleasant voices, and to programmed responses that perpetuate harmful gender discrimination and stereotypes.

A plain reading of CAP Rule 4.9 in the context of voice assistant technology indicates that the default of voice assistants to polite female tones would be in clear violation of the rule.[68] The female-tone default of voice assistants perpetuates the idea that certain qualities, helpfulness and politeness, are more uniquely associated with women than with men, given that voice assistants are expected by their users to be available, helpful and polite, and those qualities will accompany a female tone a disproportionately higher number of times due to the default setting.[69] As illustrated by Calvin Lai, this association will translate to the real world, where it will perpetuate the expectation that women should be helpful, polite, and readily available for any everyday question.[70] This is deeply harmful and offensive in a real world context, boxing women into limited and stereotypical options for socially acceptable behavior, holding them to an unfair and unequal standard, and

64. Mark Sweney, *Match.com Ad Showing Woman Carrying Out Subservient Tasks Banned for Being Sexist,* THE GUARDIAN (Oct. 4, 2022), https://www.theguardian.com/media/2022/oct/05/matchcom-ad-showing-woman-carrying-out-subservient-tasks-banned-for-being-sexist [https://perma.cc/XU66-WPZG].

65. *See* ADVERT. STANDARDS AUTH., *supra* note 63.

66. *Id.*

67. *See* ADVERT. STANDARDS AUTH., *supra* note 26.

68. *See* CAP Executive, *supra* note 52.

69. *See* Lai & Banaji, *supra* note 40; AM. PSYCH. ASS'N, *supra* note 40; ADVERT. STANDARDS AUTH., *supra* note 26.

70. *See* Lai & Banaji, *supra* note 40; AM. PSYCH. ASS'N, *supra* note 40 (showing that implicit bias is formed through learned associations and environmental stimuli, and can influence and affect behavior).

exposing them to criticism should they deviate from that expectation.[71] Voice assistants' default female tones and the stereotypical ideas they perpetuate about which traits are more associated with females also has potential to reap economic harm, as users will come to see women as more 'available' for petty requests in the real world, which may divert women's attention from more meaningful work and economic productivity.[72]

Looking beyond the default female voice setting of voice assistants to their programmed responses, which answer to rude, offensive, and gendered requests politely and gratefully, it is readily evident that those responses would also be in violation of CAP Rule 4.9.[73] Their harmful effect is glaringly obvious, as normalizing responses to appearance-based comments and remarks in the category of sexual harassment has dangerous ripple effects.[74] If voice assistant users are conditioned to expect that a woman should be grateful or flirtatious in response to a comment on her appearance, that can result in an uptick in that kind of behavior in the real world, an outcome that is deeply condescending and offensive to women, clearly meeting CAP Rule 4.9's standard for unacceptability.[75] Beyond offense, the normalization of appearance-based and sexual command comments, as well as the expectation that women receive them well, has the potential to cause emotional and physical harm to women, as those kinds of comments are emotionally degrading and can quickly escalate to violent and dangerous exchanges.[76]

C. Norway's Marketing Control Act: An Additional European Approach to Regulating Gender Bias in Advertising that is An Effective Framework for U.S. Regulation of Voice Assistants.

This section will explore the standards and application of Norway's Marketing Control Act as a second European legal framework that could prove helpful in regulating voice assistant technology in the United States. Norway has been at the forefront of regulatory efforts to curb gender

71. *See* Silverman, *supra* note 13.

72. *See* Kathleen Davis, *The Imbalance of Labor at Home is Destroying the American Economy*, FAST CO. (Nov. 30, 2020), https://www.fastcompany.com/90578848/the-imbalance-of-labor-at-home-is-destroying-the-american-economy [https://perma.cc/U32D-UGNU]; *see also* Melissa Hogenboom, *The Hidden Load: How 'Thinking of Everything' Holds Mums Back,* BBC (May 18, 2021), https://www.bbc.com/worklife/article/20210518-the-hidden-load-how-thinking-of-everything-holds-mums-back [https://perma.cc/39VP-YWT4] (showing that women already face a substantial burden due to heightened expectations about their home labor obligations, which could worsen further).

73. *See* ADVERT. STANDARDS AUTH., *supra* note 26; *see also* Fessler, *supra* note 22.

74. *See* Silvia Galdi & Francesca Guizzo, *Media-Induced Sexual Harassment: The Routes from Sexually Objectifying Media to Sexual Harassment*, 84 SEX ROLES, 645, 645 (2021), https://doi.org/10.1007/s11199-020-01196-0 [https://perma.cc/7NNE-MPJG].

75. *See* Lai & Banaji, *supra* note 40; *see also* AM. PSYCH. ASS'N, *supra* note 40; *see also* ADVERT. STANDARDS AUTH., *supra* note 26.

76. *See Alisha* Haridasani Gupta, *Misogyny Fuels Violence Against Women. Should It Be a Hate Crime*?, N.Y. TIMES (Mar. 25, 2021), https://www.nytimes.com/2021/03/25/us/misogyny-violence-against-women-hate-crime.html [https://perma.cc/W629-RVV9].

discrimination in marketing and advertising.[77] Norway's Marketing Control Act specifically addresses sexism in advertising.[78] Section 2 of the Act stipulates that marketing efforts in Norway may not "conflict with the equality of the sexes . . . or convey an offensive or derogatory appraisal of women or men."[79] Although the Act was updated as recently as 2018, its ban on gender discrimination in advertising has been in place since 1978, when Norway passed its Gender Equality Act.[80]

To accompany and clarify the Act, Norway's Consumer Authority has provided guidance which clarifies that in order to comply with the Act, advertisements may not go against the principle of gender equality, exploit bodily images of either gender, or depict an "offensive or derogatory" perspective on either gender.[81] The guidelines assert that the stated purpose of the law is to "promote equality between men and women, and in particular to improve the position of women" and that advertisements "shall not be contrary to equality between the sexes."[82]

Following the release of its guidelines, the country's Consumer Authority has reviewed and banned several advertisements found to conflict with the regulations.[83] In its assessment of a national magazine, Cats, the reviewing council determined that the magazine "may be perceived as sexist" and thus in violation of the Consumer Authority's guidelines because it portrayed women "as sexual objects and attention-grabbers in a way that was demeaning to women's general reputation and sense of pride."[84] This review provides a tangible example of the Authority's analysis and indicates that to be in compliance with the law, an advertisement must not be "demeaning to women's general reputation and sense of pride."[85]

Norway's Marketing Control Act and its accompanying guidelines can be directly applied to the regulation of voice assistants, specifically their default settings and sexist responses. The standard set forth by the act—which stipulates that marketing cannot "conflict with the equality of the sexes . . . or convey an offensive or derogatory appraisal of women or men"—is directly applicable to voice assistants.[86] The problematic responses voice assistants originally gave, specifically those that met sexually demeaning and inappropriate comments with gratitude and flirtatiousness, would clearly not

77. *See* Press Release, United Nations Hum. Rts. Off. of the High Comm'r, Comm. on Elimination of Discrimination Against Women, Norway Called a 'Haven for Gender Equality' as Women's Anti-Discrimination Committee Examines Reports on Compliance with Convention (Jan. 20, 2003) (on file with the Office of the High Commisioner, United Nations Human Rights), https://www.ohchr.org/en/press-releases/2009/10/norway-called-haven-gender-equality-womens-anti-discrimination-committee [https://perma.cc//CH7L-9E5H].

78. *See Guidelines on Sexist Advertising*, NORWEGIAN CONSUMER AUTH. (Apr. 13, 2009), https://www.forbrukertilsynet.no/english/guidelines/guidelines-on-sexist-advertising [https://perma.cc/D34Q-J4E4].

79. *The Marketing Control Act*., *supra* note 55.

80. *See* NORWEGIAN CONSUMER AUTH., *supra* note 78.

81. *Id.*

82. *Id.*

83. *See id.*

84. *Id.*

85. *Id.*

86. *See* NORWEGIAN CONSUMER AUTH., *supra* note 78.

meet this standard.[87] Their derogatory nature is more than evident as they further the idea that sexually explicit or appearance-based comments directed towards women should be met with pleasantness.[88]

Applying the same overarching purpose of the Norwegian marketing regulations to domestic regulation of voice assistants would yield a positive result for society. As expressed in the clarifying guidelines, the purpose of the Norway Marketing Control Act's provisions related to gender is to "promote equality between men and women, and in particular to improve the position of women" and to eliminate advertisements that go against the ideal of gender equality.[89] To meet this standard, voice assistant technology would not only need to do no harm to the cause of gender equality, but would also need to actively work to improve it. To comply, answers responding with neutrality or pleasantness to inquiries rooted in sexism or gender-based aggression would need to be eliminated and replaced with responses that seek to actively protest such inquiries and educate the inquirer as to why their inquiry is offensive and problematic. Further, the application of this standard to more basic qualities of the technology, like its default female-tone setting, would yield other positive results, such as preventing further entrenchment of users' implicit associations between a female tone and the traits of voice assistants. Additionally, the Marketing Control Act's broad language regulating gender discriminatory effects will also be helpful in the United States context of artificial intelligence. Due to its flexibility and broad scope, the Act can be applied to future instances of gender discrimination by the technology that are likely to emerge as the technology develops.[90]

The Authority's regulation of the Cats magazine is a useful example of the law's application.[91] In ruling against the magazine's marketing, the Authority further fleshed out the standard behind the law, ruling that advertisements could not be demeaning to "women's general reputation and sense of pride."[92] The sexually offensive and objectifying nature of Cats magazine's advertising methods parallels the nature of the responses voice assistant technology gave to that same kind of stimulus in its original programming, as it responded to degrading and offensive remarks with a sense of acceptance.[93] Under the standard clarified by the Cats case, sexist programmed responses of voice assistants clearly fall outside of the acceptable practices set by Norway's Marketing Control Act.

87. *See id.*; *see also* Fessler, *supra* note 22.

88. *See* Fessler, *supra* note 22.

89. *See* NORWEGIAN CONSUMER AUTH., *supra* note 78.

90. *See id.*; *see also FTC Interprets "Unfair Competition" Broadly in New Section 5 Policy Statement*, DAVIS POLK (Nov. 15, 2022), https://www.davispolk.com/insights/client-update/ftc-interprets-unfair-competition-broadly-new-section-5-policy-statement [https://perma.cc/PG7W-4Z83] (stating FTC Act's broad language has allowed for more expansive interpretation and regulation by the FTC).

91. *See* NORWEGIAN CONSUMER AUTH., *supra* note 78.

92. *Id.*

93. *See id.*; *see also* Fessler, *supra* note 22.

D. A Model for Implementation: How the European Model of Gender Discrimination Regulation in Advertising Can Be Applied to Voice Assistant Regulation in the United States

While the above sections have centered on the gender discriminatory effects of voice assistant's default settings and defined the rules, standards, and applications of European regulations, the next step is to explore how the model set forth by those regulations could be deployed in the United States. As illustrated by the above analysis of CAP Rule 4.9 and Norway's Marketing Act, European laws on sexism in advertising provide an effective framework and language for the regulation of voice assistant technology in the United States, and particularly of its gender discriminatory effects. The following section will further propose the necessary language of such laws, immediate changes necessary for technological compliance with such a regulation, and how and by whom such regulation would be administered and overseen in the United States.

1. Voice Assistant Technology Should be Regulated Nationally to Facilitate Consistency and International Cooperation and to Maximize Effectiveness

A foundational question in exploring proposed regulation of voice assistants is whether it should be regulated at a national or state level.[94] The answer is national regulation. Although states have so far led the way in regulating artificial intelligence, their approach is merely a band-aid, patchwork approach to regulation.[95] Allowing states to lead artificial intelligence regulation will result in burdensome inconsistency for businesses dealing in voice assistant products in the United States, as they will be subject to state-specific regulations that will lack uniformity given the cross-boundary nature of commerce today.[96] Leading technology companies have

94. *See* POL'Y CIRCLE, *supra* note 25.

95. *See* Benjamin Lerude & Lawrence Norden, *States Take the Lead on Regulating Artificial Intelligence*, BRENNAN CTR. JUST. (Nov. 1, 2023), https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-artificial-intelligence [https://perma.cc/S835-VYVR]; *see also* Ian Prasad Philbrick, *The U.S. Regulates Cars, Radio and TV. When Will It Regulate AI?*, N.Y. TIMES (Aug. 24, 2023), https://www.nytimes.com/2023/08/24/upshot/artificial-intelligence-regulation.html [https://perma.cc/ES4F-FNGH].

96. *See* Maureen Bensily & Kathy Donovan, *Regulatory Complexity Calls for a Strategic Approach*, WOLTERS KLUWER (Aug. 15, 2023), https://www.wolterskluwer.com/en/expert-insights/regulatory-complexity-calls-for-a-strategic-approach [https://perma.cc/7GLL-QRVC].

echoed this concern, voicing their support for national regulation rather than a patchwork of state regulation.[97]

Further, the regulation of artificial intelligence, like voice assistants, will stretch beyond national borders and require international cooperation.[98] Accomplishing effective international cooperation will be challenging, but the national government is accustomed to international compromise and partnership, as well as communicating updates to states and cities within the country to keep them in the loop.[99] In order to ensure the effectiveness of any proposed regulations, they should be made at the national level.

Further, the need for a societal shift towards more balanced and equitable gender ideals is at the root of the need for this regulation. If each state takes its own regulatory view on the matter, regulation will be piecemeal and conflicting, thereby thwarting the larger, necessary societal shift. To support that evolution, regulation must be both national and cohesive. The need for national regulation to reinforce accountability measures during times of societal shifts has been illustrated at numerous points in history, specifically in relation to discrimination and civil rights issues.[100] Title VII and the Equal Pay Act of 1963 are two of the foremost examples of this, as the national government confronted and outlawed gender discrimination and aimed to remedy pay disparities for women.[101] These acts served as a powerful force in outlawing discrimination in the workplace and advanced a

97. *See* David Zapolsky, *Advancing U.S. Regulatory Leadership for AI in 2024*, AMAZON (Feb. 6, 2024), https://www.aboutamazon.com/news/policy-news-views/advancing-us-regulatory-leadership-for-ai-in-2024 [https://perma.cc/34K6-5BB7]; *see also* Greg Bensinger, *Big Tech Wants AI to be Regulated. Why do They Oppose a California AI Bill?*, REUTERS (Aug. 27, 2024), https://www.reuters.com/technology/artificial-intelligence/big-tech-wants-ai-be-regulated-why-do-they-oppose-california-ai-bill-2024-08-21/ [https://perma.cc/BD87-R5W9].

98. *See* Meltzer, *supra* note 25.

99. *See* Anthonia F. Pipa & Max Bouchet, *Partnership Among Cities, States, and the Federal Government: Creating an Office of Subnational Diplomacy at the U.S. Department of State*, BROOKINGS INST. (Feb. 17, 2021), https://www.brookings.edu/articles/partnership-among-cities-states-and-the-federal-government-creating-an-office-of-subnational-diplomacy-at-the-us-department-of-state/ [https://perma.cc/23BT-BNK2]; *see also* Bureau of Public Affairs, *Diplomacy: The U.S. Department of State at Work*, U.S. DEP'T STATE (June 2008), https://2009-2017.state.gov/r/pa/ei/rls/dos/107330.htm [https://perma.cc/DUU3-426A]; *see also* John Leyden, *EU and US Agree to Chart Common Course on AI Regulation*, CIO (Apr. 4, 2024), https://www.cio.com/article/2083973/eu-and-us-agree-to-chart-common-course-on-ai-regulation.html [https://perma.cc/PR7P-A6EW].

100. *See* Mehrunnisa Walli, *8 Key Laws That Advanced Civil Rights*, HISTORY.COM (Jan. 22, 2024), https://www.history.com/news/civil-rights-legislation [https://perma.cc/T96C-FE43].

101. *See Equal Pay Act of 1963*, U.S. EQUAL EMP. OPPORTUNITY COMM'N., https://www.eeoc.gov/statutes/equal-pay-act-1963 (last visited Mar. 5, 2025) [https://perma.cc/V5N2-EHZE]; *see also Title VII of the Civil Rights Act of 1964*, U.S. EQUAL EMP. OPPORTUNITY COMM'N., https://www.eeoc.gov/statutes/title-vii-civil-rights-act-1964 (last visited Apr. 9, 2025) [https://perma.cc/T7TG-VQ5T].

long overdue change in behavior and understanding.[102] It is time for the government to do the same with gender discrimination in voice assistant technology.

Congress should focus on the regulation of voice assistants specifically, rather than another segment of artificial intelligence technology, because of the unique positioning and attributes of voice assistants that heighten its potential harm to users. Chief among these attributes is the placement of voice assistant technology—voice assistants are on the kitchen counters and in the jean pockets of millions of Congress' constituents.[103] This breadth of adoption has led these technologies to become fully integrated with the day-to-day lives of Americans who are not always cognizant of the ways the technology can exacerbate their own biases and influence their perspectives.[104] This subtle integration comes without any warning message to put its users on notice, leaving its users more vulnerable to its effect, which is the opposite of a more extreme example of artificial intelligence use, such as artificial intelligence weapons, where the public and the technology user understand its high level of risk.[105] This added vulnerability is exactly why Congress should focus first on voice assistants, which have been allowed to fly under the radar. Additionally, Congress' regulation of voice assistants would serve as a necessary and overdue first step in taking on the regulation of artificial intelligence more broadly. [106] Given the scale of voice assistants' integration into the day-to-day lives of Americans, regulating the technology would allow for feedback and iteration as Congress begins to develop its regulation of the novel technology that is artificial intelligence.

---

102. *See* Deborah Vagins & Georgeanne Usova, *The Equal Pay Act: You've Come a Long Way Baby (But Not All The Way)*, ACLU (June 10, 2011), https://www.aclu.org/news/womens-rights/equal-pay-act-youve-come-long-way-baby-not-all-way [https://perma.cc/Q29N-D2UR]; *see also* Tamara Lytle, *Title VII Changed the Face of the American Workplace*, SHRM (May 21, 2014), https://www.shrm.org/topics-tools/news/hr-magazine/title-vii-changed-face-american-workplace [https://perma.cc/A4SN-ATT2].

103. *See* Bergur Thormundsson, *Number of Voice Assistant Users in the U.S. 2022-2026*, STATISTA (Dec. 5, 2023), https://www.statista.com/statistics/1299985/voice-assistant-users-us/ [https://perma.cc/P4TT-NBYT**]**.

104. *See* Jesse Jenkins, *Voice Assistants 'Like Us' Affect How Users Process Misinformation, Study Suggests*, N.J. INST. TECH. (Dec. 21, 2023), https://news.njit.edu/voice-assistants-us-affect-how-users-process-misinformation-study-suggests [https://perma.cc/9SQ7-PK36].

105. *See* Chloe Wittenberg, et al., *Labeling AI-Generated Content: Promises, Perils, and Future Directions*, MITOPS (Mar. 27, 2024), https://mit-genai.pubpub.org/pub/hu71se89/release/1 [https://perma.cc/755L-MHB5]; *see also* Eric Lipton, *From Land Mines to Drones, Tech Has Driven Fears About Autonomous Arms*, N.Y. TIMES (Nov. 21, 2023), https://www.nytimes.com/2023/11/21/us/politics/drones-ai-weapons-war.html [https://perma.cc/F3VU-7SRQ].

106. *See* Claudia Grisales, *Congress Wants to Regulate AI, but It Has a Lot of Catching Up to Do*, NPR (May 15, 2023), https://www.npr.org/2023/05/15/1175776384/congress-wants-regulate-ai-artificial-intelligence-lot-of-catching-up-to-do [https://perma.cc/LN7M-6FGL].

2. The Federal Trade Commission Should be Given Responsibility for Leading and Overseeing Regulation Voice Assistant Technology Regulation

In enacting regulation, the legislature should grant responsibility to an existing government agency, or to a combination of such agencies, to lead the development of regulation on artificial intelligence. National regulation of artificial intelligence voice assistant technology is clearly within the regulatory powers and scope of Congress under the Commerce Clause.[107] Voice assistant technology travels across state borders and has a substantial effect on national commerce given the popularity of the technology in the national market.[108] As artificial intelligence technology expands, its uses and role in the market will only increase.[109] Further, the growing appetite for legislation regulating artificial intelligence has led people to urge that 2024 be deemed the "Year of AI Regulation" in the United States.[110] The need for national regulation is further supported by the fact that the United States stands well behind its peers in regulating national privacy and artificial intelligence law, putting it at a further disadvantage as emerging technologies continue to rapidly expand.[111]

As to which government body should be responsible for the regulation of voice assistant technology, there are several options. So far, the federal government agencies that have discussed or proposed regulation of artificial intelligence include the Federal Trade Commission ("FTC"), the Federal Communications Commission ("FCC"), the Department of Defense ("DoD"), the National Institute of Standards and Technology within the Department of Commerce ("NIST"), and the Executive Branch's Office of Management and

107. *See* U.S. CONST. art. 1, § 8, cl. 3.

108. *See id.*; *see also* Asa Johnson, *How Congress Can Foster a Digital Single Market in America*, INFO. TECH. & INNOVATION FOUND. (Feb. 20, 2024), https://itif.org/publications/2024/02/20/how-congress-can-foster-a-digital-single-market-in-america/ [https://perma.cc/8NSW-3TC2].

109. *See Generative AI to Become a $1.3 Trillion Market by 2032*, BLOOMBERG (June 1, 2023), https://www.bloomberg.com/company/press/generative-ai-to-become-a-1-3-trillion-market-by-2032-research-finds/ [https://perma.cc/M9C6-6X9W].

110. Natasha Allen & Louis Lehot, *What to Expect in Evolving U.S. Regulation of Artificial Intelligence in 2024*, FOLEY & LARDNER (Dec. 7, 2023), https://www.foley.com/insights/publications/2023/12/us-regulation-artificial-intelligence-2024/ [https://perma.cc/RK79-L3W5].

111. *See* Philbrick, *supra* note 95; *see also* Jane Wiertel, *U.S. Lags Other Nations in Regulating AI*, PULITZER CTR. (June 29, 2023), https://pulitzercenter.org/stories/us-lags-other-nations-regulating-ai [https://perma.cc/CEG7-5CBR].

Budget ("OMB"), among others.[112] Governmental agencies, like the Equal Employment Opportunity Commission ("EEOC") and the FTC, have released joint statements on the discriminatory impacts of artificial intelligence.[113]

Of the potential agencies, the FTC is best positioned to regulate voice assistant technology for discriminatory practices, as they have already focused their artificial intelligence regulation efforts on addressing bias and discrimination, and thus would be well positioned to address the issue of gender bias in virtual assistant technology.[114]

3. What Should the Regulations Contain and How Can They Leverage European Models as a Framework for Their Design?

As to the content and standards of the much-needed national regulation on artificial intelligence, the language used by European laws in addressing the gender-discriminatory effects of advertising should be applied in the United States to address that same gender-discriminatory potential of voice assistant technology. Language from Norway's Marketing Control Act stipulates that marketing and advertising in the country cannot "conflict with the equality of the sexes . . . or convey an offensive or derogatory appraisal of women or men."[115] The stated purpose of the law is to "promote equality between men and women, and in particular to improve the position of women."[116] That same language can be used as the standard, and purpose,

---

112. *See FTC Authorizes Compulsory Process for AI-related Products and Services*, FED. TRADE COMM'N (Nov. 21, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/11/ftc-authorizes-compulsory-process-ai-related-products-services [https://perma.cc/GV5K-2P6J]; *see also* Joseph Clark, *DOD Committed to Ethical Use of Artificial Intelligence*, DOD NEWS (June 15, 2023), https://www.defense.gov/News/News-Stories/Article/Article/3429864/dod-committed-to-ethical-use-of-artificial-intelligence/ [https://perma.cc/D7HU-EJRQ]; *see also* Press Release, White House, FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence (Oct. 30, 2023) (on file with WH.gov), https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/ [https://perma.cc/BZ9G-6A5V]; *see generally* Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts, *Notice of Inquiry*, 38 FCC Rcd 11675 (2023), https://docs.fcc.gov/public/attachments/FCC-23-101A1_Rcd.pdf [https://perma.cc/TJ8U-ZZWV]; *see also* U.S. DEP'T COM. NAT'L INST. STANDARDS & TECH., NIST AI 100-1, ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK at 1 (2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf [https://perma.cc/Q3ZR-LGB3]; *see also OMB Releases Requirements for Responsible AI Procurement by Federal Agencies,* COVINGTON (Oct. 24, 2024), https://www.cov.com/en/news-and-insights/insights/2024/10/omb-releases-requirements-for-responsible-ai-procurement-by-federal-agencies [https://perma.cc/C8LR-4CEZ].

113. *See* Rohit Chopra, Kristen Clarke, Charlotte Burrows & Lina Khan, *Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems*, FED. TRADE COMM'N (Apr. 25, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf [https://perma.cc/7HUD-PQZQ].

114. *See* Airlie Hilliard, *How is the FTC Regulating AI?*, HOLISTIC AI (Sept. 22, 2023), https://www.holisticai.com/blog/ftc-regulating-ai [https://perma.cc/E392-YVGX].

115. NORWEGIAN CONSUMER AUTH., *supra* note 78.

116. *Id.*

respectively, for laws protecting against gender discrimination by voice assistants. Both examples of problematic instances of gender discrimination by artificial intelligence discussed above, default female-tone settings and problematic responses to objectifying and sexist inquiries, would be found to violate that standard, as they are clearly derogatory and conflict with gender equality.[117] Such clear applicability demonstrates the usefulness of the European regulation language as a framework for domestic regulation in this arena. Further, a broad but clear purpose, such as that put forth by Norwegian regulators above, will perform well with voice assistant regulation in the United States.[118] A purpose to promote gender equality and advance the position of women in society is clear and defensible, while also providing enough flexibility to effectively serve as justification for decisions made under the regulation.

The United Kingdom's CAP Rule 4.9 also serves as a useful model for application to voice assistant technology in the United States, specifically the technology's potential to reinforce problematic gender stereotypes and behaviors.[119] The rule's language stipulates that advertisements must take care to avoid reinforcing the idea that certain traits or behaviors are uniquely associated with, or available to, one gender.[120] Application of this standard to voice assistant technology would also be effective in reducing its tendencies to entrench gender bias. Under the CAP Rule 4.9 standard, both default female-tone settings and problematic responses to sexual inquiries would be unacceptable.[121] Helpfulness, pleasantness, availability and politeness are traits voice assistants portray in answering their customers and they will most frequently be coupled with the female default tone, advancing the idea that they are truly linked. This suggests to users that those traits are uniquely associated with female voices, and thus females in general. This is similar to the Match.com advertisement banned under CAP Rule 4.9, as it portrayed a woman, in an eager and helpful manner, performing household tasks, while the man relaxed on the couch.[122] The advertisement portrayed the same harmful idea that voice assistant settings perpetuate—that females are expected to be pleasant, eager, and the default for helpfulness with small mundane tasks.[123] Rule 4.9's ban of the advertisement demonstrates how its standards can be used to regulate against the same practice and harm in voice assistant technology.

CAP Rule 4.9's stated purpose, which is to regulate advertisers so that they are obligated to take care so as not to cause harm or widespread offense, would be also useful in the context of voice assistants.[124] Regulation in the arenas of emerging technology should not aim to be overly restrictive, but

117. *See* Breen & Andrews, *supra* note 62; *see also* Sweney, *supra* note 64.
118. *See* NORWEGIAN CONSUMER AUTH., *supra* note 78.
119. *See* ADVERT. STANDARDS AUTH., *supra* note 26.
120. CAP Executive, *supra* note 52.
121. *See id.*
122. *See* Sweney, *supra* note 64.
123. *See id.*
124. *See* CAP Executive, *supra* note 52.

rather force producers of such technology to be more thoughtful in their design to prevent harm in their delivery. Domestic voice assistant regulation should incorporate the prevention of harm or offense into its statement of purpose as it provides useful insight and explanation behind the driving goal of the regulation.

4. Why the United States Should Act to Regulate Voice Assistants: A Reiteration of the Public Policy Factors Urging Regulatory Action

Public policy factors weigh heavily in favor of developing rules for voice assistants, as both normative and economic arguments support the regulation of this technology. From a normative lens, the principle of equality, and gender equality specifically, is a core value of society and key to its progress.[125] Allowing gender discrimination to go unchecked in technology that is becoming more and more ingrained in our everyday lives has the potential to derail and undercut the progress society has made towards gender equality in the last century. Beyond derailing that progress, it could yield harmful consequences that could even worsen the status quo. Those consequences may include an increase in violence and derogatory language directed at women as the influence of voice assistant technology creates unequal gender-based expectations.[126]

Studies have shown that gender equality has a positive effect on economic growth and stability.[127] From an economic lens, allowing gender discrimination to persist in voice assistants could lead to a reversal of the progress women have made in the professional sphere in the last several decades.[128] Given this, it is crucial that the U.S. government acts to regulate technologies exacerbating gender discrimination for the good of the economy, in addition to the normative reasons for doing so.

Lastly, the United States is a leading example for other countries looking to navigate and manage emerging technologies and their side

125. *See Americans, Deeply Divided, Yet Share Core Values of Equality, Liberty & Progress,* SIENA COLL. RSCH. INST. (Oct. 25, 2021), https://scri.siena.edu/2021/10/25/americans-deeply-divided-yet-share-core-values-of-equality-liberty-progress/ [https://perma.cc/7875-M7VL]; *see also* Wayne Baker, *United America, Core Value 6: Equal Opportunity*, U. MICH. CTR. POSITIVE ORGS. (Feb. 3, 2014), https://positiveorgs.bus.umich.edu/news/united-america-core-value-6-equal-opportunity/ [https://perma.cc/A5UY-W74Y].

126. *See* Lai & Banaji, *supra* note 40; *see also* AM. PSYCH. ASS'N, *supra* note 40.

127. *See* Gita Gopinath, *Gender Equality Boosts Economic Growth and Stability*, INT'L MONETARY FUND (Sept. 27, 2022), https://www.imf.org/en/News/Articles/2022/09/27/sp092722-ggopinath-kgef-gender-korea [https://perma.cc/6RE6-2GL3].

128. *See* OECD, SOCIAL INSTITUTE AND GENDER INDEX 2019 GLOBAL REPORT (2019), https://www.oecd-ilibrary.org/docserver/bc56d212-en.pdf? [https://perma.cc/54NJ-2CGD] (showing improvements in gender equality over last several decades).

effects.[129] It can leverage that leadership in a positive way by acting to regulate technology for concerning issues like gender discrimination. Leading in the development of voice assistant regulation will further benefit the United States, as it will allow the United States to have full agency over the scope and application of the regulation, rather than having to account for existing laws in the space.[130]

5. Responding to Free Speech Concerns About the Regulation of Artificial Intelligence Voice Assistant Technology

Those who oppose regulating sexism in Nordic advertising have pointed to freedom of expression and freedom of the press as the basis for their concerns.[131] These ideas hold great weight in America as well and would likely be leveraged to oppose the implementation of domestic regulation of voice assistant technology.[132] A threat to freedom of speech is not received lightly in the United States, as the First Amendment is perceived to be the bedrock to so many other fundamental rights that America holds dear.[133] Given this, it is likely that efforts to regulate voice assistants for gender-discriminatory content would face First Amendment concerns and lawsuits.

The most apparent weakness in this argument is that First Amendment rights extend to individuals, not artificial intelligence, as artificial intelligence does not hold personhood.[134] Even the most creative legal arguments advanced in the space of First Amendment rights and artificial intelligence have not gone so far as to say that artificial intelligence is generally entitled

---

129. *See* Robert Kagan & Ivo H. Daalder, *The U.S. Can't End its Global Leadership Role*, BROOKINGS (Apr. 25, 2016), https://www.brookings.edu/articles/the-u-s-cant-afford-to-end-its-global-leadership-role/ [https://perma.cc/EWD7-9TWE]; *see also* David Zopolsky, *Advancing U.S. Regulatory Leadership for AI in 2024*, AMAZON (Feb. 6, 2024), https://www.aboutamazon.com/news/policy-news-views/advancing-us-regulatory-leadership-for-ai-in-2024 [https://perma.cc/Y8JC-V4M8].

130. *See* Shana Lynch, *Analyzing the European AI Act: What Works, What Needs Improvement*, STAN. UNIV. (July 21, 2023), https://hai.stanford.edu/news/analyzing-european-union-ai-act-what-works-what-needs-improvement [https://perma.cc/A465-59ZJ].

131. *See Sexist Advertisement in the Nordic Countries*, SWEDISH WOMEN'S LOBBY (2016), https://sverigeskvinnoorganisationer.se/wp-content/uploads/2020/05/Sexist-advertisement-in-the-Nordic-countries.pdf [https://perma.cc/MM3W-LY9F].

132. *See Freedom of Expression*, ACLU (Mar. 1, 2002), https://www.aclu.org/documents/freedom-expression [https://perma.cc/7VGQ-3PLT].

133. *See* Michael Gonchar, *Why is Freedom of Speech an Important Right? When, if Ever, Can It Be Limited?*, N.Y. TIMES (Sept. 12, 2018), https://www.nytimes.com/2018/09/12/learning/why-is-freedom-of-speech-an-important-right-when-if-ever-can-it-be-limited.html [https://perma.cc//3FM5-ATQK].

134. *See* Lance Eliot, *AI Legal Personhood Distresses AI Ethicists Since People Could Deviously Scapegoat Machines to Avoid Apt Human Responsibility, Including In The Case Of AI-Based Self-Driving Cars*, FORBES (Mar. 4, 2022), https://www.forbes.com/sites/lanceeliot/2022/03/04/ai-legal-personhood-distresses-ai-ethicists-since-people-could-deviously-scapegoat-machines-to-avoid-apt-human-responsibility-including-in-the-case-of-ai-based-self-driving-cars/ [https://perma.cc/3RMU-U3R6].

to First Amendment rights.[135] In a recent lawsuit, Amazon has claimed that conversations between Amazon Echo products and its users should be protected from a search warrant to the extent that those conversations reflect expressive content.[136] As a secondary argument, Amazon has argued that the conversations should be protected under the extension of its own First Amendment rights.[137] These arguments, however, would not apply to the regulation of voice assistant technology's default settings, as it does not involve any human expression or content. Additionally, regulating programmed responses of these products does not implicate any user conversation records, but rather serves to prevent sexist responses by the technology in the first instance.

When faced with challenging and novel First Amendment issues, courts have regularly considered how compelling the societal and government interest is that is provoking First Amendment opposition.[138] Where there is a compelling interest, courts are much more likely to allow regulation.[139] Here, public policy weighs heavily in favor of enabling regulation in this instance.[140] The public interest at stake here, which is reducing society's exposure to both subliminal and blatant gender discrimination from artificial intelligence technology, is grave. There is serious potential for a significant increase in problems of gender bias and discrimination should these issues go unregulated, as use of artificial intelligence-based voice assistants becomes more and more commonplace in society.[141] In weighing the potential First Amendment rights of an emergent technology against the well-being of public and social progress, particularly in the realm of gender equality, the latter should be more important.[142] On a more general level, courts should be very hesitant to grant First Amendment rights to artificial intelligence technology,

135. *See* Eric C. Boughman, Sara Beth Kohut, David E Sella-Villa & Michael V Silvestro, *Alexa Do You Have Rights? Legal Issues Posed by Voice-Controlled Devices and the Data They Create*, AM. BAR ASS'N (July 20, 2017), https://www.americanbar.org/groups/business_law/resources/business-law-today/2017-july/alexa-do-you-have-rights/ [https://perma.cc/33RZ-W8LP].

136. *See* Silvia Sui, *State v. Bates: Amazon Argues that the First Amendment Protects Its Alexa Voice Service*, HARV. JOLT DIG. (Mar. 25. 2017), https://jolt.law.harvard.edu/digest/amazon-first-amendment **[**https://perma.cc/3GSS-2L2K].

137. *See* Boughman, et al., *supra* note 135.

138. *See* Ronald Steiner, *Compelling State Interest*, FREE SPEECH CTR. (Aug. 10, 2023), https://firstamendment.mtsu.edu/article/compelling-state-interest/ [https://perma.cc/UR76-D7VA].

139. *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York, 447 U.S. 557, 566 (1980) (finding that the governmental may regulate commercial speech if such regulation advances a compelling state interest and is narrowly tailored to serve that interest).

140. *See Gender Equality*, UNITED NATIONS (Mar. 1, 2002), https://www.un.org/en/global-issues/gender-equality [https://perma.cc/258Y-EQML]; *see also* Veera Korhonen, *Gender Inequality in the United States – Statistics & Facts,* STATISTA (July 3, 2024), https://www.statista.com/topics/11801/gender-inequality-in-the-united-states/#topicOverview **[**https://perma.cc/85VU-TDFV].

141. *See* Lai & Banaji, *supra* note 40; AM. PSYCH. ASS'N, *supra* note 40.

142. *See* UNITED NATIONS, *supra* note 140; *see also* Korhonen, *supra* note 140.

as that will surely create a barrier to regulating an area of technology that is already dangerously unregulated.[143]

IV. CONCLUSION

As artificial intelligence continues to grow rapidly, so does its potential for gender discriminatory effects. This is especially evident with artificial intelligence voice assistant technology, as interactions with voice assistants have become a seamless part of our everyday customs and commerce. Public policy factors weigh heavily in favor of acting to regulate voice assistant technology, as default female tones and programmed responses serve to worsen and entrench existing gender biases. The United States government should pass broad legislation to regulate voice assistant technology for gender bias. In passing more specific regulations in accordance with that law, its administering agency should look to European laws as a framework and example for how to do so. The United Kingdom's CAP Rule 4.9 and Norway's Marketing Control Act provide language and cases that are directly applicable to the regulation of voice assistant technology in the United States. The government should leverage these European regulations and their guidelines as a framework for its regulation of voice assistant technology. United States regulation should be enacted at the national level by the federal government and should be administered by the FTC. Failing to do so will allow for the expansion of harmful biases and a reversal of the progress regarding gender equality in society.

143. *See* Peter Henderson, *Who Is Liable When Generative AI Says Something Harmful?*, STAN. UNIV. (Oct. 11, 2023), https://hai.stanford.edu/news/who-liable-when-generative-ai-says-something-harmful [https://perma.cc/8VQF-4D2N]; *see also Freedom of speech*, LEGAL INFO. INST. (June 2021), https://www.law.cornell.edu/wex/freedom_of_speech [https://perma.cc/GU4X-8BYF]; *see also* Daron Acemoglu, *Dangers of Unregulated Artificial Intelligence*, CTR. FOR ECON. POL'Y. RSCH. (Nov. 23, 2021), https://cepr.org/voxeu/columns/dangers-unregulated-artificial-intelligence [https://perma.cc/8TB5-R2C5].

Communications Law: Annual Review

Staff of the Federal Communications Law Journal

TABLE OF CONTENTS

Consumers' Research v. Federal Communications Commission

Andrew Hanin

109 F.4TH 743 (5TH CIR. 2024)

In *Consumers' Research v. Federal Communications Commission*, the Fifth Circuit decided en banc that the Federal Communication Commission's ("FCC") methods of funding Congress's goal of affordable and nationwide cell service were unconstitutional.

I. BACKGROUND

Congress's goal in enacting § 254 of the Telecommunications Act of 1996 (codified at 47 U.S.C. § 254) was to promote policy that would lead to "providing 'universal' [telecommunications] service to all residents and businesses in the United States," a goal that persists to the present day.[1] As it stands, the FCC does not decide how much money is necessary to reach the goals set out for Universal Service as prescribed by 47 U.S.C. § 254 (2016).[2] The FCC "instead, . . . relies on a private company called the Universal Service Administrative Company, ("USAC") which "is managed by representatives from 'interest groups affected by and interested in universal service programs.'"[3] The issues presented in this case surround the constitutionality of the FCC's practices in their pursuit of fulfilling their statutory prescription from Congress in 47 U.S.C. § 254.[4] The Fifth Circuit Court of Appeals originally denied petition, but that decision was vacated and the case was reheard en banc.[5] Upon rehearing, the Fifth Circuit Court of Appeals decided en banc that this method of gathering funds for the Universal Service Fund (USF) "violates Article 1, § 1 of the Constitution."[6]

---

[1] Consumer's Rsch. v. FCC, 109 F.4th 743, 748 (5th Cir. 2024) (quoting Ronald J. Krotoszynski, Jr., *Reconsidering the Nondelegation Doctrine: Universal Service, the Power to Tax, and the Ratification Doctrine*, 89 IND. L.J. 239, 279 (2005)).

[2] *See id.* at 750.

[3] *See id.* (quoting *Leadership*, UNIVERSAL SERV. ADMIN. CO., https://www.usac.org/about/leadership/ [https://perma.cc/MG3Q-3K84] (last visited Feb. 1, 2025)).

[4] *See id.* at 756.

[5] *See id.* at 743.

[6] *See id.* at 748.

II. ANALYSIS

The agency action that prompted this challenge was the FCC's proposal of the goal contribution amount for "Q1 2022," which was "derived directly from USAC's proposed contribution amount."[7] The challenge invokes the nondelegation doctrine to assert that the delegation of power from both Congress to the FCC and the FCC to USAC is unconstitutional for three reasons: (1) the collection of fees from telecommunication companies is a tax, (2) there is no intelligible principle in 47 U.S.C. § 254, and (3) the FCC delegated a tax power to a private party.[8] Yet, the court grounds its decision in the proposition that even if the individual delegations of power themselves are constitutional, the combination of the two delegations is not.[9]

A. The Fees Charged to the Regulated Industry Are Taxes

The court began its analysis by first establishing that what the FCC portrayed as "fees" charged to companies in the regulated field is actually a tax levied against those parties. The court defined a fee as "having three characteristics," and asserted that the FCC's fee lacks all three.[10] According to the court, a fee is a charge "incurred 'incident to a voluntary act,'"[11] which can only be imposed on members of the agency's regulated industry,[12] and payment of the fee yields benefits for the paying party, "rather than to the public generally." [13]

The court found that the FCC's fee had none of the three characteristics set out above. First, the fees were not "incident to a voluntary act," but rather "a condition of doing business."[14] Second, the fees were a cost that was permissibly passed onto the consumer.[15] In other words, companies subject to the fee offset the cost of the fee by raising prices and otherwise passing that cost onto consumers so that the company's profits would not be significantly affected.[16] Third, those who benefit from the fee are not members of the

---

[7] *See Consumers' Rsch.*, 109 F.4th at 752 (challenging the constitutionality of USAC being able to propose a goal contribution amount to reach through the taxes at issue, and the FCC's decision to use that amount in its own rulemaking).

[8] *See id.* at 756.

[9] *See id.* at 782 (referencing the "double-layered delegation" being unconstitutional).

[10] *See id.* at 757.

[11] *Id.* (quoting Nat'l Cable Television Ass'n, Inc. v. United States, 415 U.S. 336, 340 (1974)).

[12] *See id.* (quoting Valero Terrestrial Corp. v. Caffrey, 205 F.3d 130, 134 (4th Cir. 2000).

[13] *See* Skinner v. Mid-Am. Pipeline Co., 490 U.S. 212, 223 (1989) (quoting *Nat'l Cable Television Ass'n, Inc.*, 415 U.S. at 343).

[14] *Consumers' Rsch.*, 109 F.4th at 757 (quoting from *Nat'l Cable Television Ass'n, Inc.*, 415 U.S. at 340).

[15] *See id.* (referencing 47 C.F.R. § 54.712(a) (2006)) (allowing the payer of the fee to pass the cost of the fee onto its consumers).

[16] *See id.*

regulated industry. Therefore, the court finds these fees to be taxes, and that Congress delegated its taxing power to the FCC.[17]

B. Congress's Delegation of Power to the FCC Has No Intelligible Principle

With the underpinning of this fee being a tax, the court then more directly addresses the petitioners' challenge.[18] The petitioners' challenge to "the USF's funding mechanism"[19] could be successful if there is no intelligible principle in 47 U.S.C. § 254 to guide the FCC in setting a tax collection goal for supplying the USF.[20] If there is no intelligible principle, then extending this tax power to the FCC could be unconstitutional on nondelegation grounds.

The court finds that the language of 47 U.S.C. § 254 does not establish an intelligible principle that permits the FCC to tax the telecommunication companies.[21] The language of the statute relevant to this inquiry "provides that USF funding should be 'sufficient . . . to preserve and advance universal service,'[22] and § 254(b)(1) suggests that telecommunications services 'should be available at . . . affordable rates.'"[23] The crux of the court's argument is that the clauses in 47 U.S.C. § 254, which are meant to limit the FCC's discretion, are so vague and without clear limitations that they provide no intelligible principle.[24] Additionally, the FCC has no "superior technical knowledge"[25] that would make a more general organic statute permissible,[26] especially where the power delegated is legislative, not executive.[27] All that being said, the court does not rely on this argument alone to deem this agency action unconstitutional.

C. The FCC Impermissibly Delegated Power to a Private Entity

On the issue of delegating this power to a private entity, the court pulled from Supreme Court precedent and from district court cases to establish the conditions that make for a constitutional delegation of power to a private party.[28] According to the Fifth Circuit, for a private delegation to be constitutional, a "government official must have final decision-making

---

[17] *See id.* at 758.
[18] *See id.* at 760.
[19] *Id.*
[20] *See Consumers' Rsch.*, 109 F.4th at 760.
[21] *See id.*
[22] *Id.* (quoting 47 U.S.C. § 254(d) (citations omitted)).
[23] *Id.* (quoting 47 U.S.C. § 254(b)(1) (citations omitted)).
[24] *See id.*
[25] *Id.* at 764.
[26] *See Consumers' Rsch.*, 109 F.4th at 764 (citing to Whitman v. Am. Trucking Ass'ns, Inc., 531 U.S. 457, 472 (2001) (showing that a more general principle that relies on an agency's (the Environmental Protection Agency's) technical expertise may not violate the nondelegation doctrine even though it grants much discretion to the agency)).
[27] *See id.* at 765.
[28] *See id.* at 768-70.

authority," that authority must "actual[ly] [be] exercise[d]," and "the private actors must always remain subject to the 'pervasive surveillance and authority' of some person or entity lawfully vested with government power."[29]

The court found that because the approval of the tax doesn't require affirmative approval from the FCC, and because the FCC "never made a single substantive change to the contribution amounts proposed by USAC," the tax is an unconstitutional delegation to a private entity.[30] Additionally, because 47 U.S.C. § 254 does not explicitly prescribe delegation of this duty to a private entity, the court sees this delegation as likely unconstitutional.[31]

D. The Combination of the Delegation and Subdelegation is Unconstitutional

The court then finally decides that the combination of the two delegations violates the Vesting Clause in Article 1 § 1, making the Q1 2022 USF Tax unconstitutional.[32] The court presents the opinion that even if the delegation from Congress to the FCC is constitutional, and the sub-delegation of power from the FCC to USAC is also constitutional, the combination of the two is not.[33]

First, the court emphasizes the unprecedented nature of double-layered delegation.[34] While there are some similar cases, the court finds that none are similar enough to provide a relevant means of comparison to the structure of the FCC's delegation.[35] The court also distinguishes historical precedent by comparing the present regulatory scheme to a similar one used by the Framers of the Constitution.[36] The court found that the 1798 Congress's use of private tax assessors to ascertain the "value [of] real estate for the purpose of administering a" tax was distinguishable from the present facts, and thus provides no justification for the kind of delegation at issue here.[37] The final nail in the coffin for the FCC's practice is a structural argument about accountability.[38] Through the double-layered delegation, it is difficult for the public to know who is accountable for the taxes and extra costs passed onto

---

[29] *See id.* at 769-70 (quoting Sunshine Anthracite Coal Co. v. Adkins, 310 U.S. 381, 388 (1940).

[30] *Id.* at 771.

[31] *See id.*

[32] *See Consumers' Rsch.*, 109 F.4th at 778.

[33] *See id.*

[34] *See id.* at 779.

[35] *See id.* at 780 (finding that *Sunshine Anthracite Coal Co.* is distinguishable from the present case because the recommendations for coal prices in that case did not de facto decide minimum coal prices, whereas here the court found the USAC recommended contribution goal de facto decided the contribution goal).

[36] *See id.* at 779-780.

[37] *See id.* at 780-81 (distinguishing the present facts from the historical precedent regarding tax assessors because in 1798, "Congress itself decided the amount of revenue the Government would levy from the American citizens", "Congress made all relevant tax policy decisions," and the tax assessor's role was "to discern between falsity and truth").

[38] *See Consumers' Rsch.*, 109 F.4th at 782-83.

consumers, and difficult to voice their frustrations through the democratic process.[39]

In all, the court roots its decision in the double-layered delegation being unprecedented and unsupported by law, and contrary to the structure of the executive branch as prescribed by the Framers.[40]

III. CONCURRENCE (J. ELROD JOINED BY J. HO, J. ENGELHARDT)

This concurrence is in full accord with the majority's opinion, only concurring to add that the court should rule each level of this delegation to be unconstitutional for the same reasons the majority presented.[41]

IV. CONCURRENCE (J. HO)

Similarly, this concurrence agrees wholeheartedly with the majority, but writes separately to drive home the structural argument the majority makes.

V. DISSENT (J. STEWART JOINED BY J. SOUTHWICK, J. HAYNES, J. GRAVES, J. HIGGINSON, J. DOUGLAS)

Judge Stewart's dissent concludes that both levels of delegation are permissible. First, the dissent disagrees with the majority in asserting the existence of an intelligible principle in 47 U.S.C. § 254, arguing that the "duty to weigh the enumerated universal service principles is reminiscent of constitutional statutory delegations that provided an intelligible principle."[42] The dissent finds that the statute provides adequate guidance for the FCC when taking into account the entirety of the statute and the "context, purpose, and history" of 47 U.S.C. § 254.[43]

Next, the dissent addresses the constitutionality of the FCC's delegation to the USAC.[44] For the FCC's delegation to the USAC to be constitutional, the USAC must be subordinate to the FCC.[45] Here, the USAC is subordinate because there is a long process before the "public notice announcing USAC projections,"[46] where there are opportunities for the FCC to review the USAC's processes and conclusions.[47] The dissent concludes that the private-nondelegation doctrine is not violated because the USAC is subordinate to the FCC.[48]

---

[39] *See id.* at 783.
[40] *See id.* at 783-84.
[41] *See id.* at 786 (Elrod, J., concurring).
[42] *Id.* at 790 (Stewart, J., dissenting)..
[43] *See id.* at 792-93.
[44] *See Consumers' Rsch.*, 109 F.4th at 793-97.
[45] *See id.* at 793 (Stewart, J., dissenting).
[46] *See id.* at 750 (majority opinion).
[47] *See id.* at 793-94 (Stewart, J., dissenting).
[48] *See id.* at 796.

Finally, the dissent refutes the majority's claim that the fees the USAC administers are taxes. The fee is compared to another Fifth Circuit case,[49] where the court held that "a charge by a legislative body is a fee, and not a tax."[50] Specifically, the Fifth Circuit held that if a charge is "levied against a specific industry sector, serves a regulatory purpose, and raises funds for a specific regulatory program," then it is a fee and not a tax.[51] The dissent finds that this fee on the telecommunication companies satisfies all aspects of the above fee characteristics, along with a characteristic forwarded by the majority: that the charged party must also benefit from the fee.[52] For those reasons, the dissent asserts that both layers of delegation are constitutional and that the fee is not a tax.[53]

VI. DISSENT (J. HIGGINSON JOINED BY J. STEWART, J. SOUTHWICK, J. GRAVES)

Judge Higginson's dissent further disagrees with the majority by disputing that the combination of the two delegations of power is what creates the unconstitutional regulatory scheme.[54] This opinion also asserts that more general guidance from Congress to the FCC is necessary for it to effectively regulate such a dynamic and ever-changing industry.[55]

VII. CONCLUSION

Despite the Dissenters' arguments, the Fifth Circuit Court of Appeals held the Q1 2022 USF Tax unconstitutional.[56] Petitioners appealed the decision to the Supreme Court, which granted certiorari on November 22, 2024. The Supreme Court heard oral arguments on March 26, 2025.

[49] *See id.* at 798; Tex. Ent. Ass'n, Inc. v. Hegar, 10 F.4th 495, 502 (5th Cir. 2021).

[50] *See Consumer's Rsch.*, 109 F.4th at 798 (referencing *Hegar*, 10 F.4th at 506-507) (Stewart, J., dissenting).

[51] *See id.* at 798 (referencing *Hegar*, 10 F.4th at 506-507).

[52] *See id.* at 799.

[53] *See id.* at at 801.

[54] *See id.* (Higginson, J., dissenting).

[55] *See id.* at 803-04.

[56] *See Consumer's Rsch.*, 109 F.4th at 786 (majority opinion).

Free Speech Coalition, Inc. v. Paxton

Maya W. Lilly

95 F.4TH 263 (5TH CIR. 2024)

In *Free Speech Coalition, Inc. v. Paxton*, the Fifth Circuit reversed the District Court for the Western District of Texas's judgment to apply strict scrutiny to Texas statute H.B. 1181 and vacated the injunction against the statute's age-verification requirements.[1] The Fifth Circuit found that the statute was subject to rational-basis review under the Supreme Court's decision in *Ginsberg v. New York*, 390 U.S. 629 (1968).[2] According to the Fifth Circuit, *Ginsberg* created a carveout for the application of rational-basis review to content-based restrictions that regulate the distribution of materials obscene *for minors to minors*.[3] Therefore, although H.B. 1181 is a content-based restriction, it only regulates commercial entities' ability to distribute "sexual material *harmful to minors*," *to minors*, placing it within *Ginsberg*'s framework and subject only to rational-basis review.[4]

I. BACKGROUND

The Texas legislature passed Liability for Allowing Children to Access Pornographic Material (H.B. 1181) in 2023.[5] Before the law took effect, Free Speech Coalition, a trade association of the adult entertainment industry, filed suit seeking to enjoin enforcement of the statute, arguing that the statute's provisions requiring age-verification and the display of certain health warnings violated the plaintiff's First Amendment rights.[6] Certain plaintiffs also contended that H.B. 1181 conflicts with Section 230 of the Communications Decency Act, 47 U.S.C. § 230, and is thereby preempted by Section 230.[7] The age-verification requirements are contained in Section 129B.002, titled "Publication of Material Harmful to Minors."[8] Pursuant to Section 129B.002, any "commercial entity that knowingly and intentionally publishes or distributes more than one-third sexual material which is harmful to minors, on an Internet website, including social media platforms, shall use

1. *See* Free Speech Coal., Inc. v. Paxton, 95 F.4th 263 (5th Cir. 2024), *cert. granted*, 144 S. Ct. 2714 (2024) (No. 23-1122).
2. *See id.* at 269.
3. *See id.* at 270, 276.
4. *Id.* at 269 (emphasis added).
5. *See* H.B. 1181, 88th Leg., ch. 676 (Tx. 2023) (codified as TEX. CIV. PRAC. & REM. ANN. § 129B.001 (West 2023)).
6. *See Free Speech Coal.*, 95 F.4th at 266.
7. *See id.*
8. *See* § 129B.002.

reasonable age verification methods to verify that an individual attempting to access the material is at least 18-years-old."[9] The challenged health warnings are contained in Section 129B.004, titled "Sexual Materials Health Warnings."[10] Pursuant to that Section, commercial entities regulated by the statute must display in 14-point font or larger, notices "on the landing page of the Internet website on which sexual material harmful to minors is published or distributed and all advertisements for that Internet website."[11]

After finding that the plaintiffs satisfied Article III's standing requirements, the district court granted the preliminary injunction on three grounds.[12] First, the district court determined that the Supreme Court's decisions in *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997) (*Reno*), and *Ashcroft v. American Civil Liberties Union*, 542 U.S. 656 (2004) (*Ashcroft II*), were controlling on the applicable standard of review to analyze the Texas Statute's age-verification requirements and therefore applied strict scrutiny.[13] The district court found that H.B. 1181's age-verification requirements failed strict scrutiny and would likely be unconstitutional.[14] Second, the district court determined that H.B. 1181's requirements for placement of certain health warnings compelled speech and were therefore subject to strict scrutiny.[15] The court further found that the health warnings would fail strict scrutiny and were likely unconstitutional.[16] Finally, the district court held that certain provisions of H.B. 1181 conflicted with and were therefore preempted by Section 230 of the Communications Decency Act.[17]

The State of Texas filed an emergency appeal, and the Fifth Circuit issued an administrative stay.[18] After argument in the Fifth Circuit, the court granted the State's motion to stay the district court's injunction pending its decision on appeal.[19] The Fifth Circuit vacated the injunction against enforcement of the age-verification requirement, finding that the district court erred by failing to assess H.B. 1181's age-verification provisions under rational-basis review pursuant to *Ginsberg*.[20] Applying rational-basis review, the court found that the age-verification requirements do not violate the First Amendment.[21] Additionally, the Fifth Circuit reversed the district court's judgment that Section 230 preempted H.B. 1181.[22] However, the court upheld the district court's judgement in granting the plaintiff's injunction to H.B.

9. *Id.*
10. *See* § 129B.004.
11. *Id.*
12. *See* Free Speech Coal., Inc. v. Colmenero, 689 F. Supp. 3d 373, 385–87 (W.D. Tex. 2023), *vacated in part*, 95 F.4th 263 (5th Cir. 2024).
13. *See id.* at 390–91.
14. *See id.* at 393.
15. *See id.* at 405.
16. *See id.* at 408.
17. *See id.* at 414.
18. *See* Free Speech Coal., Inc. v. Paxton, 95 F.4th 263, 266 (5th Cir. 2024).
19. *Id.*
20. *See id.* at 267.
21. *See id.* at 267, 278–79.
22. *See id.* at 285–86.

1181's health warning provisions because they unconstitutionally compelled speech.[23]

Free Speech Coalition petitioned the Supreme Court for a writ of certiorari only to address whether the Fifth Circuit properly applied rational-basis review instead of strict scrutiny in assessing the constitutionality of H.B. 1181's age-verification requirements.[24] The Supreme Court granted the petition[25] and held oral arguments on January 15, 2025.[26]

II. ANALYSIS

A. Age Verification Requirements Are Subject to Rational-Basis Review Pursuant to Ginsberg v. New York

According to the Fifth Circuit, since H.B. 1181's age-verification requirements regulate *distributions to minors of materials that are harmful to minors*, it triggers the Supreme Court's framework in *Ginsberg v. New York*, and is therefore subject only to rational-basis review.[27] In *Ginsberg*, the Court held that New York could criminalize the sale of "girlie" magazines *to minors* even though the material in the magazines was *not obscene for adults*, without violating the First Amendment.[28] According to the Fifth Circuit, by upholding the New York statute in *Ginsberg*, the Supreme Court affirmed that criminalizing the sale of materials *to children* is a rational means to protect minors from exposure to material judged by the state to be *harmful to minors*, even where the material is not obscene for adults; the Court determined that rational-basis review is appropriate for regulating materials that the State has found *harmful to minors*.[29] The Fifth Circuit went on to explain that the Supreme Court reaffirmed *Ginsberg*'s framework in *Erznoznik v. City of Jacksonville*, 422 U.S. 205 (1975).[30] In *Erznonznik*, a city ordinance prohibiting the "showing of films containing nudity by a drive-in theater when its screen is visible from a public street or place," was challenged under the First Amendment.[31] The Fifth Circuit highlighted that the Supreme Court in *Erznoznik* did not strike down the ordinance because enforcing its provisions would burden some material available to adults in order to protect children.[32] Rather, in *Erznoznik* the Court noted that the statute also regulated material that was not even harmful to children.[33] According to the Fifth Circuit, H.B.

---

23. *See id.* at 285–86.
24. *See* Petition for Writ of Certiorari, Free Speech Coal., Inc. v. Paxton, 144 S. Ct. 2714 (2024) at i (No. 23-1122).
25. *See* Docket for No. 23-1122, SUP. CT. OF THE U.S., https://www.supremecourt.gov/docket/docketfiles/html/public/23-1122.html [https://perma.cc/SW7K-ZAZ4].
26. *Id.*
27. *See Free Speech Coal.,* 95 F.4th at 269.
28. *See* Ginsberg v. New York, 390 U.S. 629, 637–39 (1968).
29. *See Free Speech Coal.*, 95 F.4th at 269 (emphasis added).
30. *See id.* 269–270.
31. *See* Erznoznik v. City of Jacksonville, 422 U.S. 205, 206–07 (1975).
32. *See Free Speech Coal.*, 95 F.4th at 270 (citing *Erznoznik*, 422 U.S. at 213).
33. *See Erznoznik*, 422 U.S. 205 at 206.

1811 is distinguishable because it only restricts "material obscene *for minors*" and asserted that if the statute in *Erznoznik* regulated only material obscene for minors, the Supreme Court would have upheld it.[34]

1. Ginsberg Remains Good Law After *Reno* and *Ashcroft II* and Binds This Court's Decision

The Fifth Circuit began by establishing that *Ginsberg* remained good law after the Supreme Court's decisions in *Reno and Ashcroft II*.[35] To support this point, the Fifth Circuit pointed to the Supreme Court's opinion in *Brown v. Entertainment Merchants Association*, decided in 2011.[36] According to the Fifth Circuit, *Entertainment Merchants* confirms *Ginsberg* is good law because there, the Supreme Court explained that the statute in *Entertainment Merchants*, was not subject to the lower standard it applied in *Ginsberg* because the challenged material was violent in nature rather than sexual.[37] The Court clarified that *Ginsberg*'s lower standard applies only to types of *sexual* content.[38] According to the Fifth Circuit, the fact that the Court relied on *Ginsberg* to make this distinction in *Entertainment Merchants*, which was decided years after its decisions in *Reno* and *Ashcroft II*, demonstrates that *Ginsberg* remains good law.[39] Moreover, the Supreme Court has cited *Ginsberg* in opinions after it decided *Reno* and *Ashcroft II* for different propositions.[40]

2. Technological Changes Since *Ginsberg* Do Not Sufficiently Distinguish H.B. 1181 From the Statute Upheld in *Ginsberg*

The plaintiffs contended that source-based restrictions on Internet expressions raise "categorically different" concerns than what was at issue in *Ginsberg*, emphasizing that the Supreme Court itself has acknowledged as much.[41] Further, in-person age-verification, upheld in *Ginsberg*, raises fewer privacy concerns than the age-verification methods required under H.B. 1811.[42] This is because, in practice, most people will not have to provide an identification in-person, since their appearance will usually be sufficient.[43] The Fifth Circuit disagreed with these contentions for four reasons.

First, the court noted that the statute at issue in *Ginsberg* "necessarily implicated, and intruded upon," privacy of the adults who sought to purchase "girlie magazines," but that was not a sufficient basis for the Supreme Court

34. *See Free Speech Coal.*, 95 F.4th at 270 (citing *Erznoznik*, 422 U.S. at 212).
35. *See id.*
36. *See id.*
37. *See id.*
38. *See id.*
39. *See id.*
40. *See Free Speech Coal.*, 95 F.4th at 270 n.14 (collecting cases).
41. *See id.* at 270–71.
42. *See id.* at 271.
43. *See id.*

to apply strict scrutiny there.[44] Second, H.B 1811's age-verification methods are not a "categorically different" burden on adults because it provides three methods for age-verification, including the option that an individual provide their government-issued identification.[45] According to the Fifth Circuit, this means that "at least one option will have no more impact on privacy," than the in-person verification that was required by the statute upheld in *Ginsberg*.[46] The Fifth Circuit also noted that H.B. 1811 proscribes commercial entities for retaining identifying information because it will fine any entity $10,000 for each instance of retention of information, which is a heavier penalty than if a commercial entity failed to verify the age of its users.[47] This makes H.B. 1181 more protective of privacy, not less.[48]

Third, there is no precedent that would compel the court to depart from *Ginsberg*'s holding on the grounds of privacy concerns and therefore it declined to do so.[49] Finally, the Fifth Circuit noted that the Supreme Court has not distinguished between source-based restrictions on Internet expressions.[50] According to the Fifth Circuit, in *Reno*, the Supreme Court had an opportunity to distinguish *Ginsberg* based on the premise that "the world of the Internet" and "the world of in-person interaction" are different.[51] However, none of the four key differences the Supreme Court identified between the statute in *Reno* and the one in *Ginsberg* mentioned the Internet at all.[52]

3. The Supreme Court's Decisions in *Reno* and *Ashcroft II* Do Not Control Here Because H.B. 1181 Is Distinguishable

The Fifth Circuit next addressed why *Reno* and *Ashcroft II* do not require the court here to apply strict scrutiny to H.B. 1181's age-verification provisions. Beginning with the statue in *Reno*, the court found H.B. 1181 easily distinguishable.[53] In *Reno*, the Supreme Court distinguished the challenged statute—the Communications Decency Act of 1996 ("CDA") —from the statute in *Ginsberg* in four critical ways.[54] The Fifth Circuit observed that H.B. 1181 is distinguishable in most of the same ways from the CDA.[55] The Fifth Circuit also noted an additional six features which distinguishes H.B. 1181 from the CDA and therefore, places H.B. 1181 outside of *Reno*'s framework.[56] First, the CDA prohibited sexual and non-

44. *See id.*
45. *See id.*
46. *See Free Speech Coal.*, 95 F.4th at 271.
47. *See id.*
48. *See id.* at 271 n.17.
49. *See id.* at 271.
50. *See id.* at 271–72.
51. *See id.* at 271 (citing Reno v. Am. C.L. Union, 521 U.S. 844, 865–66 (1997)).
52. *See Free Speech Coal.*, 95 F.4th at 271.
53. *See id.* at 272.
54. *See id.* (citing *Reno*, 521 U.S. at 865).
55. *Id.*
56. *See id.* at 272.

sexual material while H.B. 1181 does not.[57] Second, parental participation or consent can circumvent H.B. 1181, which was not a feature of the CDA.[58] Third, the CDA failed to specifically define the prohibited material, whereas H.B. 1181 has specific definitions.[59] Fourth, the CDA provided no limitations on commercial activity, while H.B. 1181 only covers commercial entities.[60] Fifth, the Supreme Court in *Reno*, enjoined the CDA in part because it did not have "a viable age verification process," but H.B. 1181 is centered on age-verification requirements.[61] Sixth and finally, in *Reno*, the Court's conclusion "was fundamentally bound up in the rudimentary 'existing' technology," of the past.[62] The Fifth Circuit noted that technology has "dramatically developed," since then.[63]

The Fifth Circuit acknowledged that one distinction between *Ginsberg* and *Reno* points against its analysis: in *Reno*, the Supreme Court distinguished New York's statute in *Ginsberg* based on its definition of a minor as a person under 17-years-old.[64] In contrast, the CDA's definition of a minor was everyone under the age of 18.[65] Like, the CDA, H.B. 1181 defines minors to be those under 18 years of age.[66] However the court did not believe that the Supreme Court decided to apply a rational-basis framework in *Ginsberg* because of the New York statute's definition of minor.[67] It provided three reasons: (1) the Supreme Court only noted this distinction once throughout *Reno*;[68] (2) H.B. 1181 aligns with the rest of the distinctions between the CDA and the *Ginsberg* statute;[69] and (3) the Supreme Court spent more time defending its conclusion by focusing on the overly-sweeping nature of the CDA and its failure to follow the *Miller* standard, rather than the CDA's definition of minor.[70] The Fifth Circuit also addressed what it classified to be "seemingly contradictory" language from *Reno*.[71] Beginning with the fact that in *Reno*, the Supreme Court states that "the interest in protecting children," relying on *Ginsberg*, "'does not justify an unnecessarily broad suppression of speech addressed to adults.'"[72] According to the Fifth Circuit, this was irrelevant to its analysis of H.B. 1181 because the CDA reached far beyond the statutory framework upheld in *Ginsberg* and also regulated non-sexual material.[73]

---

57. *See id.* at 272 (citing *Reno*, 521 U.S. at 873).
58. *See Free Speech Coal.*, 95 F.4th at 272 (citing *Reno*, 521 U.S. at 865).
59. *See id.* (citing *Reno*, 521 U.S. at 873).
60. *See id.* (citing *Reno*, 521 U.S. at 865).
61. *See id.* (citing *Reno*, 521 U.S. at 876).
62. *See id.* (citing *Reno*, 521 U.S. at 876–77).
63. *See id.*
64. *See Free Speech Coal.*, 95 F.4th at 273; *see also Reno*, 521 U.S. at 865–66 (discussing these differences).
65. *See Free Speech Coal.*, 95 F.4th at 273 (quoting *Reno*, 521 U.S. at 865–66).
66. *See* § 129B.001(3).
67. *See Free Speech Coal.*, 95 F.4th at 273.
68. *See id.* (citing *Reno* at 865–66).
69. *See id.*
70. *See id.* (citing *Reno*, 521 U.S. at 873).
71. *See id.* at 273.
72. *See id.* at 273 (quoting *Reno*, 521 U.S. at 875).
73. *See Free Speech Coal.*, 95 F.4th at 273.

Turning to *Ashcroft II*, the Fifth Circuit acknowledged that it provided more support for the plaintiffs' contention that strict scrutiny is the applicable standard here because of the similarities between H.B. 1181 and the Child Online Protection Act ("COPA"), which Court held likely to be unconstitutional in *Ashcroft II*.[74] However, the Fifth Circuit read *Ashcroft II* as the Supreme Court's declaration that COPA would fail strict scrutiny, and did not provide an answer to the question whether strict scrutiny is the appropriate standard of review to analyze statutes like COPA or H.B. 1181.[75] The Fifth Circuit highlighted that the petitioners in *Ashcroft II* only raised two issues: (1) whether COPA passes strict scrutiny; and (2) whether the court of appeals erred in its finding that COPA was not narrowly tailored.[76] Therefore, the petitioners did not challenge the appropriate standard of review nor did the Court have to raise the argument *sua sponte* because it is not jurisdictional.[77]

The Fifth Circuit went on to acknowledge that the Supreme Court in *Ashcroft II* stated in *dicta*, "when plaintiffs challenge a content-based speech restriction, the Government has the burden to prove that the proposed alternatives will not be as effective as the challenged statute."[78] However, it found this inapposite on two grounds.[79] First, taken altogether with the rest of the opinion, this comment explains how strict scrutiny works in general rather than a definitive statement that strict scrutiny is the correct standard to apply to COPA.[80] Second, and more importantly, according to the Fifth Circuit, this comment is inconsistent with the premise that *Ginsberg* is no longer good law.[81] Although the Supreme Court's comment in *Ashcroft II* seems "irreconcilable" with its decision to apply rational-basis to the content-based regulation in *Ginsberg*, according to the Fifth Circuit, the fact that the Supreme Court has made clear that *Ginsberg* remains good law after *Ashcroft II* means that cases which fit into *Ginsberg*'s framework must follow it.[82] For these reasons, the Fifth Circuit found that *Ashcroft II* does not constitute precedent on the question of the appropriate standard of review to apply to COPA.[83]

The Fifth Circuit next addressed the plaintiffs' reliance on *United States v. Playboy Entertainment, Group, Inc.*, 529 U.S. 803 (2000), to rebut the State's argument that *Reno* and *Ashcroft II* do not command the application of strict scrutiny to H.B. 1811.[84] The law at issue in *Playboy* served to protect children, and there, the Supreme Court made clear, "[a]s we consider a content-based regulation, the answer should be clear . . . [t]he standard is strict

74. *See id.*
75. *See id.* at 274.
76. *See id.*
77. *See id.*
78. *See id.* at 274 (quoting Ashcroft v. ACLU, 542 U.S. 656, 657 (2004)).
79. *See Free Speech Coal.*, 95 F.4th at 274.
80. *Id.*
81. *See id.*
82. *See id.* at 275 (citing Brown v. Ent. Merchs. Ass'n, 564 U.S.786, 793 (2011)).
83. *See id.*
84. *See id.*

scrutiny."[85] The Fifth Circuit also noted that the Supreme Court even acknowledged the difference in degree between content-based burdens and content-based bans, yet still concluded that both "must satisfy the same rigorous scrutiny."[86] Yet, as the Fifth Circuit pointed out, even with that language, the Supreme Court has never overturned *Ginsberg*, and therefore its precedent must mean something.[87]

The Fifth Circuit also distinguished H.B. 1181 from the statute challenged in *Playboy* in three ways. First, the court pointed out that unlike the law in *Playboy*, H.B. 1181 permits adults to access as much pornography as they want whenever they please.[88] Second, the burden in *Playboy* was "different in kind" from the burden caused by enforcing H.B. 1181's age-verification requirements.[89] According to the Fifth Circuit, the age-verification requirements are the same as the age-verification requirements that people face when they want to participate in other activities that are restricted to adults.[90] Third, the law at issue in *Playboy* regulated distribution to everyone, whereas H.B. 1181 regulates only minors' ability to access certain materials.[91] The Fifth Circuit explained that once an individual is confirmed to be at least 18 years of age, "H.B. 1181 does nothing further."[92] That is unlike the law in *Playboy*, which imposed burdens on individuals even after establishing that they were not minors.[93]

Moreover, *Playboy* was decided before *Entertainment Merchants* and *Reno* where the Supreme Court dedicated significant space distinguishing the challenged statute in *Reno* from the one in *Ginsberg* to justify its application of strict scrutiny.[94] The Fifth Circuit refused to believe that the Court would have distinguished the statutes in *Reno* and *Entertainment Merchants* so carefully from the one in *Ginsberg* if the Court did not consider *Ginsberg* good law.[95] The court also noted that *Playboy* implicated specific broadcast media considerations, which trigger unique First Amendment concerns, and therefore provided less guidance here in a non-broadcast context.[96]

4. Rational-Basis Is Appropriate Under Ginsberg Even Though H.B. 1181 Is a Content-Based Restriction

In closing its analysis, the Fifth Circuit agreed that H.B. 1181 is a content-based restriction, but found that this alone does not trigger strict scrutiny since the New York statute in *Ginsberg* was also content-based.[97]

85. *See Free Speech Coal.*, 95 F.4th at 275 (quoting United States v. Playboy Ent., Grp., 529 U.S. 803, 814 (2000)).
86. *See id.* at 275 (citing *Playboy*, 529 U.S. at 812).
87. *See id.* at 275.
88. *See id.*
89. *See id.* at 275–76.
90. *See id.* at 276.
91. *See Free Speech Coal.*, 95 F.4th at 276.
92. *Id.*
93. *See id.*
94. *See id.* (citing *Reno*, 521 U.S. at 864–66).
95. *See id.* at 275–76.
96. *See id.* at 276 (citing *Playboy*, 529 U.S. at 806).
97. *See Free Speech Coal.*, 95 F.4th at 276.

According to the court, *Ginsberg* created a narrow carveout for applying rational-basis review to content-based restrictions.[98] Since H.B. 1181 fits into this carveout, it is not subject to strict scrutiny even though it is content-based. The court also shared concerns, in response to the dissent, that applying strict scrutiny to every content-based restriction would make protecting children extraordinarily difficult.[99] In the majority's view, such difficulties are inconsistent with *Ginsberg* and would allow the First Amendment to "strangle" the right and obligation of States to protect their minors by restricting their ability to access pornographic materials.[100]

5. Plaintiffs' Contentions That Strict Scrutiny Must Apply Because H.B. 1181 Is Overbroad and Vague Are Unconvincing

The plaintiffs contend that H.B. 1811's age-verification requirements are being used to regulate more speech than *speech obscene for minors*.[101] This is so because H.B. 1181 is only triggered against a commercial entity where one-third of the material it publishes to an Internet website is "sexual material harmful to minors."[102] Therefore, according to the plaintiffs, under this threshold the statute even regulates content benign for people of any age.[103] In the plaintiffs' view, this makes H.B. 1811 substantially overbroad and therefore facially unconstitutional.[104] The Fifth Circuit provided two reasons for rejecting the argument that H.B. 1181 is substantially overbroad.[105] First, in this context it may be appropriate to analyze the "plaintiffs' websites as a whole."[106] Second, the magazine challenged in *Ginsberg* also had a "substantial amount of content that was non-sexual," therefore, according to the court, *Ginsberg* instructs that "[t]he inclusion of some—or even much—content that is *not* obscene for minors does not end-run *Ginsberg*," so long as the regulation targets a "substantial amount of content that *is* obscene for minors."[107] The plaintiffs also argued that H.B. 1181 was unconstitutionally vague and will chill protected speech.[108] The plaintiffs expressed vagueness concerns over the statute's phrase, "with respect to minors," asserting that it has "no fixed meaning."[109] The Fifth Circuit stated that this phrase presents no constitutional issue here because it did not in *Ginsberg*.[110]

98. *See id.*
99. *See id.*
100. *See id.* at 276–77.
101. *See id.* at 277 (emphasis added).
102. *See id.*; *see also* § 129B.002(a).
103. *See Free Speech Coal.*, 95 F.4th at 277 (internal quotations omitted).
104. *See id.* (citing United States v. Stevens, 559 U.S. 460, 473 (2010)).
105. *See id.* at 277.
106. *See id.*
107. *Id.* (emphasis added).
108. *Id.*
109. *See Free Speech Coal.*, 95 F.4th at 277.
110. *See id.*

6. H.B. 1181 Does Not Discriminate Based on Speaker or Viewpoint

The plaintiffs additionally argued that strict scrutiny must apply because H.B. 1181 discriminates against speaker and viewpoint.[111] The plaintiffs argue that H.B. 1181's under inclusiveness[112] and health warnings requirements provide evidence of this.[113] The Fifth Circuit disagreed, stating that analyzing under-inclusivity in determining speaker/viewpoint discrimination serves only as a "signal that the state *may* be engaged in viewpoint discrimination."[114] However, where under-inclusivity is driven by reasonable policy choices "to avoid legal concerns that accompany attempts to regulate the 'entire universe of cyberspace,'" as are present here, courts have not found states to be engaging in viewpoint discrimination.[115] Furthermore, under-inclusivity presents fewer issues where the state is choosing to regulate a specific medium, as Texas is doing here.[116] Therefore, the plaintiffs' suggestion that *R.A.V. v. City of St. Paul*[117] requires the presumption that H.B. 1181 was unconstitutional because of its under-inclusiveness was incorrect here because, unlike *R.A.V.*, Texas is choosing to regulate a specific kind of medium differently rather than attempting to regulate certain messages.[118] According to the Fifth Circuit, this type of selection "does not necessarily implicate strict scrutiny based on viewpoint discrimination."[119]

B. H.B. 1181's Age-Verification Requirements Satisfy Rational Basis Review

According to the Fifth Circuit, it was not irrational for the Texas State Legislature to determine that access to pornography would be harmful to minors.[120] The court relied on evidence presented in the record showing (1) a correlation between frequent access to online pornography and "distorted gender orientations, insecurities, or dissatisfaction about one's own body image, depression symptoms, assimilation to aggressive models;"[121] and (2) that Internet pornography addiction shares a similar framework and "basic mechanisms" with addiction to other substances.[122] For these reasons, the

111. *See id.*
112. *Id.* (according to the plaintiffs', the statute was underinclusive because it excluded search engines and social media platforms that contain the same content).
113. *Id.* (internal quotations omitted). Plaintiffs contend that the health warnings requirement is evidence that Texas is "really engaged in speaker discrimination to stigmatize the porn industry and deter all patronage of such disfavored speech." *Id.*
114. *See id.* at 277–78 (citing City of Ladue v. Gilleo, 512 U.S. 43, 52 (1994)).
115. *See Free Speech Coal.*, 95 F.4th at 278 (citing *Reno*, 521 U.S. at 868).
116. *See id.*
117. *See generally* R.A.V. v. City of St. Paul, 505 U.S. 377 (1992).
118. *See Free Speech Coal.*, 95 F.4th at 278 (citing *R.A.V.*, 505 U.S. at 394 (1992)).
119. *See id.*
120. *See id.*
121. *Id.*
122. *Id.*

Fifth Circuit found H.B. 1181's age-verification requirements constitutional.[123]

III. CONCLUSION

For the foregoing reasons, the Fifth Circuit reversed the district court's judgment that H.B. 1181's age-verification requirement is subject to strict scrutiny.[124] Instead, the court held that under the Supreme Court's decision in *Ginsberg v. New York*, H.B. 1181 was only subject to rational basis review.[125] The Fifth Circuit found that H.B. 1181 satisfied rational basis review, and therefore, does not violate the First Amendment.[126] The Free Speech Coalition petitioned the Supreme Court of the United States for a writ of certiorari, and the Court granted the petition on July 2, 2024.[127] Oral arguments in the case took place on January 15, 2025.[128]

123. *See id.* at 279.
124. *See Free Speech Coal.*, 95 F.4th at 269, 278.
125. *See id.* at 278.
126. *See id.* at 279.
127. *See* Docket for No. 23-1122, SUP. CT. OF THE U.S., https://www.supremecourt.gov/docket/docketfiles/html/public/23-1122.html [https://perma.cc/SW7K-ZAZ4].
128. *Id.*

Truth Health Chiropractic v. McKesson

Sophia Wang

896 F.3D 923 (9TH CIR. 2023)

In *Truth Health Chiropractic v. McKesson*, the Ninth Circuit affirmed the Northern District of California's grant of summary judgment to Plaintiffs and decertification order pursuant to an order of the Federal Communications Commission ("FCC"), which found that the Telephone Consumer Protection Act ("TCPA") does not apply to online fax services. The U.S. Supreme Court granted certiorari to hear the question regarding whether the Hobbs Act requires district courts to accept the FCC's interpretation that the TCPA does not apply to online fax services. The case was argued before the U.S. Supreme Court on January 21, 2025.

I. BACKGROUND

Defendants McKesson Corporation and McKesson Technologies (collectively "Defendants") are companies that engage in services ranging from the sale of pharmaceuticals to health information technology.[1] Plaintiffs True Health Chiropractic and McLaughlin Chiropractic (collectively "Plaintiffs") are two small medical practices.[2] Between 2009 and 2010, Plaintiffs, as well as many other small medical practices, received various unsolicited advertisements through both stand-alone fax machines and online fax services from Defendants.[3] The advertisements were about certain software products that Defendants were selling.[4] In 2008, McKesson was warned by the FCC that it had "sent one or more unsolicited advertisements" via fax "in violation of the TCPA."[5]

On May 15, 2013, True Health Chiropractic sued McKesson, on behalf of a class of similarly situated small medical practices, on the grounds that Defendants sent unsolicited advertisements by fax in violation of TCPA.[6] Specifically, Plaintiffs contended that the small medical practices never

1. Petition for Writ of Certiorari at 7, McLaughlin Chiropractic Assocs., Inc. v. McKesson Corp., No. 23-1226 (2024) [hereinafter Petition for a Writ of Certiorari].
2. *Id.*
3. *Id.* at 7-8.
4. *Id.* at 8.
5. Brief for Petitioner at 12, McLaughlin Chiropractic Assocs., Inc. v. McKesson Corp., No. 23-1226, 2024 WL 4858625 (U.S. Nov. 18, 2024) [hereinafter Brief for Petitioner].
6. True Health Chiropractic Inc. v. McKesson Corp., No. 13-cv-02219, 2020 WL 7664484, at *1 (N.D. Cal. Dec. 24, 2020).

invited or permitted Defendants to send the faxes, and even assuming there was permission, there was no "opt-out notice," which Defendants were legally required to provide.[7]

Soon after filing the case, Plaintiffs moved to certify a class of all persons or entities "who received faxes from McKesson from September 2, 2009, to May 11, 2010" regarding Defendants' products and services."[8] The district court initially denied certification for failure to meet the requirement that issues common to all class members predominate over any issues affecting only individual members.[9] On appeal, the Ninth Circuit affirmed in part, but reversed as to the certification of a subclass, and remanded the case to the district court.[10] Following remand, the district court conducted limited supplemental discovery and granted Plaintiff's renewed motion for class certification of the aforementioned subclass.[11]

Six years into the parties' litigation, the FCC issued a declaratory ruling in 2019, finding that the TCPA excludes online fax services from the definition of "telephone facsimile machine."[12] Under the TCPA, a "telephone facsimile machine" is an equipment that "has the capacity . . . to transcribe text or images, or both, from paper into an electronic signal and to transmit that signal over a regular telephone line, or to transcribe text or images (or both) from an electronic signal received over a regular telephone line onto paper."[13] In its Amerifactors declaratory ruling, the FCC interpreted the TCPA to exclude online fax services that "effectively receive[] faxes sent as email over the Internet" because an online fax service is "not itself equipment which has the capacity to transcribe text or images (or both) from an electronic signal received over a regular telephone line onto paper."[14] The FCC further reasoned that because the online fax service does not by itself print a fax, such services do not implicate the "advertiser cost-shifting" problem Congress intended to address through the TCPA.[15] The FCC's Amerifactors ruling was challenged in 2020 by unrelated entities, but the FCC has not yet taken the application for review of the order.[16]

In 2020, Defendants moved to decertify the class on the basis of the FCC's Amerifactors ruling. In response to the motion, the district court ordered the parties to submit supplemental briefs to explain whether the FCC's Amerifactors order would bind the court in light of the Supreme Court's recent decision in *PDR Network v. Carlton & Harris Chiropractic*.[17] The *PDR Network* case involved a similar litigation related to the FCC's

7. *Id.*
8. True Health Chiropractic, Inc. v. McKesson Corp., 896 F.3d 923, 928 (9th Cir. 2018).
9. *Id.*
10. *Id.*
11. *Id.*
12. Amerifactors Fin. Grp., LLC, Pet. for Expedited Declaratory Ruling, *Declaratory Ruling*, 344 FCC Rcd 11950, 11950-51 (2019).
13. Brief for Petitioner, *supra* note 5, at 4.
14. Petition for a Writ of Certiorari, *supra* note 1, at 9.
15. *Id.*
16. *Id.*
17. *See True Health Chiropractic*, 2020 WL 7664484, *2; *see also* PDR Network, LLC v. Carlton & Harris Chiropractic, 588 U.S. 1, 6-8 (2019).

interpretation of the TCPA provision prohibiting unsolicited advertisement by fax and the applicability of the Hobbs Act.[18] The Hobbs Act states that the courts of appeals have "exclusive jurisdiction to enjoin, set aside, suspend (in whole or in part), or to determine the validity of" certain "final orders of the Federal Communication Commission."[19] In *PDR Network*, the Supreme Court did not decide whether an FCC order would bind the lower courts but provided a two-part guidance.[20] Specifically, in remanding the case back to the court of appeals, the Supreme Court instructed the court to consider (1) whether the FCC order was a "legislative rule which is issued by an agency pursuant to statutory authority and has the force and effect of law," or an "interpretive rule," which only "advises the public of the agency's construction of the statutes" and (2) whether the parties affected had "prior" and "adequate" opportunities to seek judicial review of the FCC order.[21]

In its Order issued on December 24, 2020, the district court found that in light of *PDR Network* and Ninth Circuit precedent, the court "must treat Amerifactors as authoritative."[22] In reaching its conclusion, the district court rejected Plaintiffs' argument that Amerifactors is not a final order under the Hobbs Act because (1) it is an "interpretive rule" and (2) an application for review of the Amerifactors order was pending before the FCC.[23] Specifically, the district court found that the Supreme Court held in *PDR Network* that an interpretive rule "*may* not be binding on a district court," and the use of "may" indicates that the *PDR Network* ruling does not definitively resolve the issue.[24] Thus, the ruling in *PDR Network* is not "clearly irreconcilable with" a binding Ninth Circuit precedent on the issue, *United States West Communications, Inc. v. Hamilton*. In *Hamilton*, the Ninth Circuit held that under the Hobbs Act, there is no distinction between a "legislative rule" and "interpretive rule" as far as the finality and enforceability of an FCC order is concerned.[25] And what matters, as the Ninth Circuit found, is whether the FCC order was merely "tentative," meaning whether it "determines rights and gives rise to legal consequences."[26] Additionally, the district court noted that per FCC regulations and case law, the reconsideration petition "does not affect the order's finality as it applies to [a defendant's] potential liability under the TCPA."[27] Thus, the court found that Amerifactors was a "final, binding order for purposes of the Hobbs Act," and under the Amerifactors ruling, there would be no liability under the TCPA for faxes received via an online fax service.[28] Consequently, the court modified the class definition to

18. *PDR Network*, 588 U.S. at 1.
19. 28 U.S.C. § 2342(1).
20. *PDR Network*, 588 U.S. at 5.
21. *Id.*
22. *True Health Chiropractic*, 2020 WL 7664484, at *6.
23. *Id.* at *6-7.
24. *Id.*
25. *Id.* at *6 (citing U.S. Commc'ns, Inc. v. Hamilton, 224 F.3d 1049, 1055 (9th Cir. 2000) ("The Hobbs Act itself contains no exception for 'interpretive' rules, and case law does not create one.")
26. *Id.*
27. *Id.* at *7.
28. *True Health Chiropractic*, 2020 WL 7664484, at *4.

"include a Stand-Alone Fax Machine Class and an Online Fax Services Class." Based on the new class definition, Defendants argued that class decertification is warranted because the FCC Amerifactors ruling would "necessitate individualized inquiries to determine whether class members received the advertisements through online fax services or traditional analog fax machines."[29]

On September 29, 2021, the district court ordered Plaintiffs to show cause as to why the class should not be decertified given the new class definition.[30] In its subsequent October 15, 2021 Order, the district court held that Plaintiffs failed to provide sufficient and satisfactory class-wide proof in support of the predominance requirement for certification of a Stand-Alone Fax Machine class.[31] Specifically, Plaintiffs produced two types of proof: (1) declarations from over 100 telephone carriers and (2) expert testimony supporting that in the absence of data "it can be assumed that the class member used a stand-alone fax machine."[32] The proof, in the court's opinion, was not representative, given there were more than 6,000 individual class members, and was not reliable, as it was based on untested assumptions proffered by an expert and Plaintiffs' counsel.[33]

A circuit split exists as to the question of whether FCC orders are binding on district courts. The Second, Third, Fourth, and Eighth Circuits have held that the FCC's interpretive rules of the TCPA are not binding on district courts.[34] The Seventh Circuit has held that district courts are not bound by FCC rules, whereas the Ninth Circuit has taken the opposite view that district courts are bound by all FCC rules, no matter whether they are interpretive or legislative.[35]

II. ANALYSIS

On appeal, the Ninth Circuit affirmed the district court's grant of summary judgment to Plaintiffs on McKesson's consent defenses, decision of decertifying the class, and decision not to award treble damages for abuse of discretion.[36]

---

29. *Id.*

30. Order Decertifying Class, Truth Health Chiropractic v. McKesson Corp., No. 13-cv-02219, 2021 WL 4818945, at *1 (N.D. Cal. Oct. 15, 2021).

31. *Id.*

32. *Id.* at *1 n.2.

33. *Id.*

34. *See, e.g.*, Gorss Motels v. FCC, 20 F.4th 87 (2d Cir. 2021); Robert W. Mauthe MD PC v. Millennium Health LLC, 58 F.4th 93 (3d Cir. 2023); Carlton & Harris Chiropractic, Inc. v. PDR Network, LLC, 883 F.3d 459 (4th Cir. 2018) (remanded by Supreme Court for consideration as to whether the rule was interpretative or legislative); Nack v. Walburg, 715 F.3d 680 (8th Cir. 2013).

35. *See* CE Design, Ltd. v. Prism Bus. Media, Inc., 606 F.3d 443 (7th Cir. 2010); *see also Hamilton*, 224 F.3d 1049 (9th Cir. 2000).

36. True Health Chiropractic, Inc. v. McKesson Corp., No. 22-15710, 2023 WL 7015279, at *1 (9th Cir. Oct. 25, 2023).

A. Summary Judgment to Plaintiffs on McKesson's Consent Defenses

The Ninth Circuit found that Defendants' consent defenses were untenable.[37] Defendants argued that Plaintiffs consented to the advertisement by either voluntarily providing fax numbers on product registration or agreeing to the relevant clause in the end-user license agreements ("EULAs").[38] The Ninth Circuit confirmed the district court's decision that neither the content of the form nor the terms of EULA clearly showed that the features and services they consented to would include promotional advertisements.[39]

B. Decertification Order

The Ninth Circuit held that the district court "correctly found that it was bound by the Federal Communication Commission's Amerifactors declaratory ruling." The court found that the Hobbs Act's "exclusive jurisdiction," which encompasses "any proceeding to enjoin, set aside, annul, or suspend any order of the [FCC] . . . except in limited circumstances," forecloses the district court's ability to review the agency's interpretation.

In response to Plaintiffs' argument on the finality of the case, the Ninth Circuit agreed with the district court that the FCC's Amerifactors decision was both an order of the FCC and a final decision of the FCC.[40] First, the court disagreed with Plaintiffs' proposed distinction between an order issued by the FCC's Consumer and Governmental Affairs Bureau ("Bureau") and an order issued by the full FCC for the purpose of evaluating the FCC order's authority.[41] The Bureau, as the court found, received delegated authority from the FCC to issue rulings in "matters pertaining to consumers and governmental affairs," and such rulings "have the same force and effect" as orders of the full FCC.[42] Second, the Ninth Circuit found that the Amerifactors ruling was final. The Amerifactors ruling, as the court noted, went through the general rulemaking process, and "impose[s] an obligation, den[ies] a right, or fix[es] some legal relationship as a consummation of the administrative process."[43] And in a footnote, the court stated a pending application for review of Amerifactors would not change the finality of the Amerifactors ruling because the ruling is "effective upon release," and in the absence of a stay pending review issued by the full commission, Amerifactors remains in effect.[44]

---

37. *Id.*
38. True Health Chiropractic Inc. v. McKesson Corp., 332 F.R.D. 589, 589, 596, 601 (N.D. Cal. 2019).
39. *True Health Chiropractic*, 2023 WL 7015279, at *1.
40. *Id.* at *2.
41. *Id.*
42. *Id.* (citing 47 U.S.C. § 155(c)(1), (3)).
43. *Id.* (citing Hamilton, 224 F.3d at 1054).
44. *Id.* at *2 n.1.

As the Amerifactors order involves "apply[ing] preexisting rules to new factual circumstances," the Ninth Circuit found that the ruling applies retroactively.[45] Accordingly, the Ninth Circuit affirmed the district court's grant of summary judgment to Defendants on claims related to the use of online fax service because Plaintiffs could not show how to distinguish the stand-alone fax machine subclass and online fax service class.[46]

C. Order Denying Treble Damages

The Ninth Circuit found the district court did not abuse its discretion by denying treble damages to Plaintiffs on individual claims. A court may award treble damages only if "it finds that a defendant 'willfully or knowingly' violated the TCPA."[47]And because Defendants were never made aware of how and why it violated the TCPA in 2008, the Ninth Circuit found that Defendants could not and did not "willfully or knowingly" violate the TCPA.[48]

III. CONCLUSION

For the reasons above, the Ninth Circuit affirmed the district court's judgment that the district court is bound by the FCC's Amerifactors ruling. McLaughlin Chiropractic Associates petitioned the Supreme Court of the United States for a writ of certiorari, which was granted on October 4, 2024.[49]

The Supreme Court heard the oral argument of the case on January 21, 2025.[50] In Oral Argument, Petitioner, McLaughlin Chiropractic, argued that although the courts of appeals would have the exclusive jurisdiction to determine the validity of agency's orders, district courts can consider and review the validity of an agency's interpretation under the Hobbs Act.[51] In support, Petitioner cited Justice Kavanaugh's concurring opinion in *PDR Network*. Specifically, the concurrence states that the Hobbs Act does not bar a party from arguing that the agency's interpretation of the statute is wrong before the district court when the Hobbs Act is silent on whether a party may argue against the agency's legal interpretation in subsequent enforcement proceedings.[52] Thus, under the Hobbs Act, district courts can examine the agency's interpretation of the TCPA "under the usual principles of statutory interpretation, affording appropriate respect to the agency's interpretation" and decide whether to apply the order in the context of the litigation.[53]

45. *True Health Chiropractic*, 2023 WL 7015279, at *2 (quoting Reyes v. Garland, 11 F.4th 985, 991 (9th Cir. 2021)).

46. *Id.*

47. *Id.* at *3 (quoting 47 U.S.C.§ 227(b)(3)).

48. *Id.*

49. Brief for Petitioner, *supra* note 5, at 5.

50. Transcript of Oral Argument at 1, McLaughlin Chiropractic Assoc. v. McKesson Corp., No. 23-1226 (2024), https://www.supremecourt.gov/oral_arguments/audio/2024/23-1226 [https://perma.cc/EUE2-22WU].

51. *See id.* at 4-6, 12.

52. *See PDR Network*, 588 U.S. at 18.

53. *Id.*; *see also* Transcript of Oral Argument, *supra* note 50, at 16-17.

Respondent, McKesson, argued that the Hobbs Act's exclusive jurisdiction should be interpreted to mean district courts cannot review the merits of an agency's final order, and only courts of appeals can hear challenges regarding whether an agency order is unlawful.[54]

54. Transcript of Oral Argument, *supra* note 50, at 34-36.

United States ex rel. Heath v. Wisconsin Bell, Inc.

Mia Shaeffer

92 F.4TH 654 (7TH CIR. 2023)

In *United States ex rel. Heath v. Wisconsin Bell, Inc.*, the Seventh Circuit addressed whether E-rate program reimbursements are subject to the False Claims Act ("FCA"), holding that genuine issues of fact precluded summary judgment on the elements of falsity, *scienter*, and materiality, and, as a matter of law, government funds are involved in the E-rate program.[1] Accordingly, since government funds are involved, fraudulent reimbursement requests under this program fall under the FCA's definition of "claims."[2] The Supreme Court granted certiorari[3] to address whether requests for reimbursement under the E-rate program constitute "claims" for purposes of the FCA.[4] The Supreme Court heard arguments in this case on November 4, 2024.[5] The Supreme Court issued a written opinion on February 21, 2025, affirming the Seventh Circuit and concluding that requests for reimbursement under the E-rate program do "qualify as 'claims' under the FCA."[6]

I. BACKGROUND

The E-rate program provides subsidies to allow schools and libraries "in rural or economically disadvantaged areas" to obtain affordable telecommunications services.[7] The Federal Communication Commission's (FCC) "'lowest-corresponding-price' rule" mandates that service providers in this program "offer schools and libraries 'the lowest price . . . charge[d] to non-residential customers who are similarly situated.'"[8]

Wisconsin Bell, a service provider and participant in the E-rate program, was "aware of the lowest-corresponding-price rule" since its implementation in the 1990s, but declined to ask for clarification on the rule

1. *See* United States ex rel. Heath v. Wisconsin Bell, Inc., 92 F.4th 654, 662, 664-65, 671 (7th Cir. 2023).
2. *See id.* at 666.
3. Wisconsin Bell, Inc. v. United States, 144 S. Ct. 2657 (2024) (mem.).
4. *Wisconsin Bell, Inc. v. United States, ex rel. Todd Heath*, SCOTUSBLOG, https://www.scotusblog.com/case-files/cases/wisconsin-bell-inc-v-united-states-ex-rel-todd-heath/ [https://perma.cc/5K37-88AC].
5. *Id.*
6. Wisconsin Bell, Inc. v. United States ex rel. Heath, 145 S. Ct. 498, 508 (2025).
7. *Heath*, 92 F.4th at 657 (citing Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56).
8. *Id.* at 658 (quoting 47 C.F.R. § 54.500).

and, until 2009, did not formulate any procedures for compliance.[9] Before 2009, Wisconsin Bell treated transactions with schools and libraries identically to transactions with other customers, "offer[ing] the highest prices 'whenever possible.'"[10] Wisconsin Bell began creating policies related to the E-Rate program in 2009, which were not finalized until 2011.[11]

In 2008, Todd Heath brought a *qui tam* action against Wisconsin Bell, alleging a violation of the FCA based on overcharges in violation of the E-rate program rules.[12] In 2015, Heath filed a second amended complaint, the parties conducted discovery, and the district court granted Wisconsin Bell's motion for summary judgment.[13]

II. ANALYSIS

The FCA is violated if a party "knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval" that tends to influence a decision made by the government regarding how to use federal funds.[14] Accordingly, the elements of an FCA case are: (1) falsity, (2) *scienter*, (3) materiality, and (4) federal funds.[15] The Seventh Circuit analyzed each of these elements in turn.[16]

A. Falsity, Scienter, and Materiality

While the district court concluded that Heath did not present sufficient evidence to show falsity,[17] the circuit court found that there was a factual dispute with respect to this element because Heath's expert report showed that, accounting for factors including contract length, location, size, and distance from the provider, schools and libraries were charged higher rates, while other "non-residential customers" were charged less.[18] The court concluded that this showing, in combination with Wisconsin Bell's "admission that it had no methods or procedures in place to comply with the E-rate program" before 2009 and their reluctance to ask for an explanation of the program, created a genuine dispute over whether schools or libraries were charged higher rates in comparison to other similarly situated customers.[19]

The district court, relying on *United States ex rel. Schutte v. SuperValu Inc.*,[20] also found that Heath did not present sufficient evidence of knowledge,

9. *Id.*
10. *Id.*
11. *Id.*
12. *Id.* at 659.
13. *Heath*, 92 F.4th at 659.
14. *Id.* (quoting 31 U.S.C. § 3729(a)(1)(A); Universal Health Servs., Inc. v. United States ex rel. Escobar, 579 U.S. 176, 193 (2016)).
15. *Id*. at 660.
16. *Id.*
17. *Id.* at 660 (citing United States ex rel. Heath v. Wisconsin Bell, Inc., 593 F. Supp. 3d 855, 860 (E.D. Wis. 2022)).
18. *Id.* 660-61.
19. *Heath*, 92 F.4th at 661-62.
20. United States ex rel. Schutte v. SuperValu Inc., 9 F.4th 455, 463-65 (7th Cir. 2021).

or *scienter*, because "Wisconsin Bell's interpretation of the lowest-corresponding-price rule . . . was 'objectively reasonable'" and aligned with the statutory and regulatory language.[21] However, after that ruling, the Supreme Court vacated the Seventh Circuit's *Schutte* decision,[22] finding that knowledge under the FCA means "knowledge and subjective beliefs," and is not an objective standard.[23] Under this standard, the court here found that Heath presented sufficient evidence for an inference of *scienter* because Wisconsin Bell knew about the lowest-corresponding-price rule but failed to set protocols for complying with it until 2009.[24] Wisconsin Bell also failed to explain how, without these protocols, it was possible to know whether it was complying with the rule, which presented an issue of fact regarding "whether Wisconsin Bell was acting with reckless disregard" of the risk that it was violating E-rate program rules.[25] The court also found a genuine dispute of material fact with respect to *scienter* even after Wisconsin Bell began to set E-rate policies in 2009, because Heath presented evidence that "overcharges increased from 2008 through 2010" and did not decrease until 2011, which could lead a factfinder to "reasonably infer that Wisconsin Bell acted in reckless disregard of whether" it was complying with the lowest-corresponding-price rule.[26]

Wisconsin Bell also argued that "Heath failed to demonstrate a factual dispute" with respect to materiality because payments were not "expressly" conditioned upon compliance with the lowest-corresponding-price rule, and the government continued to reimburse Wisconsin Bell after learning about Heath's allegations, but the court disagreed.[27] The court observed that it is relevant whether the government expressly states that a certain condition is required to receive a payment, but not dispositive.[28] Since the lowest-corresponding-price rule is important to the E-rate program, providers should have understood, even without having to expressly certify their compliance, that failure to comply with the rule "could influence reimbursement decisions."[29] The court also concluded that mere allegations are not equivalent to "actual knowledge of actual violations," and had the government known about "actual overcharges," it was "reasonable to infer" that it would not have continued to reimburse Wisconsin Bell.[30] Therefore, the court held that materiality "does not offer an alternative basis for affirming summary judgment."[31]

21. *Heath*, 92 F.4th at 663 (quoting *Heath*, 593 F. Supp. 3d at 861).
22. United States ex rel. Schutte v. SuperValu, Inc., 598 U.S. 739, 758 (2023).
23. *Heath*, 92 F.4th at 663 (quoting *Schutte*, 598 U.S. at 749).
24. *Id.* at 663.
25. *Id.* at 663-64.
26. *Id.* at 664.
27. *Id.*
28. *Id.* at 664 (quoting *Escobar*, 579 U.S. at 194).
29. *Heath*, 92 F.4th at 665.
30. *Id.*
31. *Id.*

B. *Involvement of Federal Funds*

The court next addressed Wisconsin Bell's argument that "any allegedly fraudulent claims for payment of subsidies under the E-rate program" do not constitute claims under the FCA because the money for the program comes from private parties, who pay fees to another private party who runs the program.[32] Therefore, "the government does not 'provide' the program's funds . . . and is not hurt by fraud in the program."[33] In *United States ex rel. Shupe v. Cisco Systems, Inc.*,[34] the Fifth Circuit dismissed a similar FCA case using the same logic.[35]

Here, the Seventh Circuit "decline[d] to follow *Shupe*," concluding that the reimbursement requests considered here are claims under the FCA.[36] While prior to 2009, the FCA's definition of a claim only included claims for which the government "provides any portion of the money which is requested or demanded," the current definition includes any claims for which the government "provides or has provided any portion" of the funds, as well as claims submitted to government agents.[37] The court then analyzed three avenues for application of the FCA to the current case.[38]

1. Funds Are Provided by the U.S. Treasury

Under the past and current definitions of "claim," if the "government provides 'any portion' of the money or property" at issue, regardless of the size of said portion, the FCA can apply.[39] Here, both Heath and the government demonstrated that under the E-rate program, in addition to receiving money from telecommunications providers, the Universal Services Administrative Company ("USAC") "receives funds directly from the U.S. Treasury," which Wisconsin Bell did not dispute.[40] Accordingly, some of the program's money "is comprised of government funds," so false claims submitted to the program fall under both the past and current definitions of a "claim" under the FCA.[41] The court noted that *Shupe* "acknowledged" that claims can fall under the FCA if "any portion" of the funds come from the government, however the court in *Shupe* seemed to be unaware that some of the money for the E-rate program came from the U.S. Treasury.[42]

---

32. *Id.*
33. *Id.*
34. United States ex rel. Shupe v. Cisco Systems, Inc., 759 F.3d 379 (5th Cir. 2014).
35. *Heath*, 92 F.4th at 665-66 (citing *Shupe*, 759 F.3d).
36. *Id.* at 666.
37. *Id.* at 666-67 (quoting 31 U.S.C. § 3729(c) (2008); 31 U.S.C. § 3729(b)(2) (effective May 20, 2009)).
38. *Id.* at 667-71.
39. *Id.* at 667 (citing *Shupe*, 759 F.3d at 383).
40. *Id.*
41. *Heath*, 92 F4th at 667.
42. *Id.* (citing *Shupe*, 759 F.3d at 383-84).

2. The USAC is a Government Agent

The court next analyzed the portion of the FCA which includes claims submitted to an agent of the government, regardless of whether the money belongs to the U.S.[43] The court found the USAC, which "administers the E-rate program for the FCC," meets the criteria for a principal-agent relationship.[44] When the FCC created the USAC to manage the E-rate program, this was a manifestation from the United States of "assent for the USAC to act on [its] behalf."[45] By following the government's directions, the USAC also "manifested its consent" to the arrangement.[46] The court also rejected Wisconsin Bell's argument that the USAC is not a government agent because it "cannot alter the United States' legal obligations."[47] Since the USAC has the power "to bill contributing telecommunications companies," "collect contributions from them," and "distribute funds to eligible recipients,"[48] the USAC is able to "alter[] the relationships between the United States and third parties."[49] Further, the actions of the USAC are overseen by the FCC, a federal agency.[50] Therefore, the court found that "the USAC is an agent of the federal government," and claims submitted to it fall under the FCA's current definition of a "claim."[51]

3. The Government "Provided" the Funds

The court also concluded that "the federal government's role in establishing and overseeing the E-rate program" was enough to render the FCA applicable here.[52] Under the E-rate program, the FCC, as instructed by Congress, "collect[s] fees from telecommunication companies."[53] The FCC has the power to decide what portion of revenue these companies contribute to the program,[54] and the money is then held in the Universal Service Fund.[55] The USAC, created and supervised by the FCC, runs the E-rate program and manages these funds.[56] While the USAC makes the primary determinations regarding the distribution of funds, the FCC can review subsidy denials, as well as assist with "policy and interpretation questions" and debt collection.[57]

---

43. *Id.* (quoting 31 U.S.C. § 3729(b)(2)(A)(i)).
44. *Id.* at 668 (citing United States ex rel. Kraus v. Wells Fargo & Co., 943 F.3d 588, 598 (2d Cir. 2019)).
45. *Id.*
46. *Id.*
47. *Heath*, 92 F4th at 668.
48. *Id.* (citing 47 C.F.R. § 54.702(b)).
49. *Id.*
50. *Id.*
51. *Id.*
52. *Id.*
53. *Heath*, 92 F.4th at 668 (citing 47 U.S.C. § 254(d) (2016)).
54. *Id.* (citing 47 C.F.R. § 54.709 (2022)).
55. *Id.*
56. *Id.*
57. *Id.* at 669 (citing 47 C.F.R. §§ 54.719(b), 54.702(c); ECF No. 111, 112, 113).

The FCA applies when "there is a 'sufficiently close nexus' between the defrauded entity or program and the federal government 'such that a loss to the former is effectively a loss to the latter,'" and the court determined that this nexus is present here.[58] While in other cases, government approval of funds, without the use of government money, was not enough to conclude that the government "provided" the funds, if the government significantly participates in the distribution of certain funds and is the source of the power over the funds, this is sufficient to render the FCA applicable.[59] Here, the court found that the government was significantly involved at "every step leading up to [the] funds being made available," and therefore the FCA applied.[60]

The Seventh Circuit went on to disagree with *Shupe*'s holding for three reasons.[61] First, the Fifth Circuit failed to realize that the E-rate program's money originates from the U.S. Treasury.[62] Second, since 2009, the definition of a claim includes claims sent to government agents, and the USAC acts as a government agent with respect to the E-rate program, and therefore the FCA applies to claims under the current definition.[63] Third, the involvement of Treasury funds "is a sufficient but not necessary basis for applying" the FCA.[64] The FCA "requires only that the federal government provide" the funds at issue, [65] which includes funds provided in an indirect manner as long as the government "maintain[s] an active role in [the] collection and distribution" of the funds.[66] Here, the court concluded that there was no factual dispute over whether money for the E-rate program came from the Treasury, and therefore as a matter of law government funds are involved in the E-rate program.[67]

III. CONCLUSION

The Seventh Circuit found that Heath provided sufficient evidence to demonstrate genuine issues of fact with respect to falsity, *scienter*, and materiality, and thus reversed and remanded the case to the district court.[68] Since it was not disputed that some of the funds for the program come from the U.S. Treasury, the court found as a matter of law that government funds are involved in the program.[69]

---

58. *Id.* (quoting United States ex rel. Yesudian v. Howard Univ., 153 F.3d 731, 738-39 (D.C. Cir. 1998).
59. *Heath*, 92 F.4th at 669-70 (comparing Costner v. URS Consultants, Inc., 153 F.3d 667 (8th Cir. 1998), and Hutchins v. Wilentz, Goldman & Spitzer, 253 F.3d 176 (3d Cir. 2001) (FCA did not apply), with *Kraus*, 943 F.3d at 603 (FCA applied)).
60. *Id.* at 670.
61. *Id.* (citing *Shupe*, 759 F.3d 379).
62. *See id.*
63. *Id.*
64. *Id.*
65. *Heath*, 92 F.4th at 670 (citing *Kraus*, 943 F.3d at 602).
66. *Id.* at 671.
67. *Id.*
68. *Id.* at 662, 664-65, 671.
69. *Id.* at 671.