EDITOR'S NOTE

Welcome to the second Issue of Volume 77 of the *Federal Communications Law Journal*, 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 look forward to presenting 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 Matthew L. Conaty, Doctoral Candidate at the University of Pennsylvania's Annenberg School for Communication, which analyzes presidential war powers afforded by Section 706(a) of the Communications Act of 1934, their structural weaknesses, and the threat they pose to America's presidential democracy.

This Issue also features three student Notes. First, Nicholas Sorice addresses the threat of SLAPP litigation to online consumer reviews, arguing for an application of the FTC's Rule on the Use of Consumer Reviews and Testimonials to categorize consumer reviews as de facto speech on a matter of public interest, thereby enhancing access to anti-SLAPP protections.

Second, Sebrina Thomas discusses domestic violence in the modern age, and how the Violence Against Women Act (VAWA) fails to adequately account for technological abuses like revenge porn and sextortion. As a solution, Thomas proposes supplementing the VAWA with language from similar proposed legislation to effectively close the gaps and prioritize the protection of women.

Third, Vaishali Nambiar analyzes modern law enforcement surveillance efforts that exploit social media data to make immigration decisions. Nambiar argues that such surveillance violates a reasonable expectation of privacy, and by extension, the Fourth Amendment, under the guise of national security, and should therefore require law enforcement to obtain warrants and promote transparent police practices.

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

VOLUME 77

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

Federal Communications Law Journal

The *Federal Communications Law Journal* is published jointly by the Federal Communications Bar Association and The George Washington University Law School. The *Journal* publishes three issues per year and features articles, student Notes, essays, and book reviews on issues in telecommunications, 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. ___ (2024).

FEDERAL COMMUNICATIONS LAW JOURNAL
THE TECH JOURNAL
GW LAW VOLUME 77 ISSUE 1 fcba THE TECH BAR
JANUARY 2025

ARTICLES

Preferred or Prioritized: Probing the Limits of Presidential War Powers Under Section 706(a) of the Communications Act of 1934

By Matthew L. Conaty……127

Section 706(a) of the Communications Act of 1934 affords the President wartime authority to prioritize common carrier traffic per "the national defense and security." This article contends that this little-studied and frighteningly expansive law poses grave risks to expressive liberties under an increasingly imperialistic presidency. Tracing the decades-long evolution of this law, the article highlights both its structural weakness and potential for misuse in the digital age, before offering a comprehensive statutory revision.

NOTES

Reviewing for the Public Interest: Affirming Access to Anti-SLAPP Protection for Consumer Reviews

By Nicholas Sorice……...155

Online consumer reviews play a vital role in the modern economy. Despite (or because of) this, they are often subject to frivolous lawsuits seeking nothing more than to intimidate their authors into taking them down. Often the emotional nature, time, and fiscal expense of litigation result in success for the bully. Thirty-three states and the District of Columbia have laws on the books that could mitigate this problem: anti-SLAPP laws. However, some types of anti-SLAPP laws—those that use a "public interest" standard to define the scope of speech they protect—have not clearly applied in the context of online consumer reviews. This Note argues that the FTC's Rule on the Use of Consumer Reviews and Testimonials would make consumer reviews de facto speech on a matter of public interest by collapsing the commonly used "content and context" test into a single point, thus guaranteeing that consumer reviews fall within the scope of anti-SLAPP protection.

Two Steps Forward, One Step Back: Gaps in the Violence Against Women Act

By Sebrina Thomas……173

Since 1994, the Violence Against Women Act ("VAWA") has strived to protect women from violent acts such as stalking, dating violence, sexual assault, and domestic violence. As time has passed, technology has developed and transformed the way we see domestic violence. Technological abuse is now defined as a form of domestic violence in the VAWA, which includes the unlawful dissemination of intimate images, also known as "revenge porn," and the threat to unlawfully disseminate intimate images, known as "sextortion." These intimate images can be taken without the individual knowing; they can also be created through deepfake technology where they are manipulated to depict individuals without their consent and/or knowledge. Despite the VAWA's acknowledge that domestic violence includes technological abuse, Congress has left gaps in the Act by only providing a civil remedy for revenge porn, but not for sextortion or image-based abuse with deepfake technology. In recent years, legislators have introduced different pieces of legislation that would account for these gaps and provide adequate remedies for image-based abuse victims. This Note argues that Congress should seriously consider adopting language and/or provisions from recent legislative reforms, such as the Stopping Harmful Image Exploitation and Limiting Distribution Act of 2023 and the Preventing Deepfakes of Intimate Images Act, to keep pace with today's technology and sufficiently comport with its goal in protecting women from domestic violence through the VAWA.

Watching and Waiting: Modern Social Media Surveillance of Immigrants and Fourth Amendment Implications

By Vaishali Nambiar ……...…197

Over the past decade, with advances in technology, surveillance efforts by law enforcement have become increasingly sophisticated. The latest avenue being targeted by law enforcement is social media platforms. With millions of users, these platforms host a vast amount of valuable data. An individual's social media data can paint a detailed picture of who they are, showcasing their likes, dislikes, and the important people and places in their lives. Law enforcement agencies have deemed this data useful, particularly in determining who is a threat to the country and making immigration decisions. However, these initiatives have become too invasive and sacrifice the privacy interests of immigrants in the name of national security. This Note urges courts to recognize that individuals retain privacy interests online, and modern social media surveillance techniques utilized by law enforcement are violative of the Fourth Amendment. Additionally, this Note proposes that law enforcement should be required to obtain a warrant prior to carrying out aggressive surveillance tactics. Finally, this Note recommends that there be heightened transparency obligations imposed on law enforcement agencies regarding the efficacy of social media surveillance initiatives.

Preferred or Prioritized: Probing the Limits of Presidential War Powers Under Section 706(a) of the Communications Act of 1934

Matthew L. Conaty*

TABLE OF CONTENTS

I. INTRODUCTION 128
II. THE ORIGIN AND CONSTRUCTION OF SECTION 706 133
III. CRITICAL QUESTIONS OF WAR AND EXECUTIVE AUTHORITY 137
A. The Meaning of "War" 137
B. The Prospects for Judicial Review 142
IV. EMERGING TECHNO-LEGAL CONSIDERATIONS 146
V. A PATH FORWARD 150
VI. CONCLUSION 154

* Doctoral Candidate, The Annenberg School for Communication, University of Pennsylvania; J.D., Harvard Law School; M.A., University of Pennsylvania; M.A., Yale University; B.A., Yale College. Grateful acknowledgement for reviewing and suggesting revisions to drafts of this article is made to Claire Finkelstein, Algernon Biddle Professor of Law and Professor of Philosophy, Carey School of Law, University of Pennsylvania; Joseph Blocher, Lanty L. Smith '67 Distinguished Professor of Law, Duke University School of Law; and the 2024 cohort of the Yale Law School Freedom of Expression Scholars Conference.

I. INTRODUCTION

Imagine, if you will, a near future when a conservative President, in concert with a solid Republican majority in Congress, commits to using military force against "narco-terrorists" on the nation's southern border.[1] The scourge of fentanyl and other opioids, policymakers aver, is devastating our communities, necessitating that the fight directly be taken to the cartels, as Mexico is unable or unwilling to do so itself.[2] In a manner reminiscent of the 2001 Authorization for the Use of Military Force[3]—or perhaps the President's mere observation during a State of the Union address that the nation is now at war with nefarious drug lords[4]—the military turns its sights towards select group of non-state actors, with special operations forces shortly engaged in cross-border strikes.

The conflict abroad proceeds apace, but the homefront threatens to drag it down. Unfavorable reports from embedded correspondents are page one stories on news sites; citizens organize major municipal protests on encrypted mobile apps; and social media platforms augment the unrest through trending topics and newsfeeds.[5] Enraged, the President vows action in the interest of the national security and defense. Under cover of a century-old statute, he squelches the throughput of the cloud computing centers that power these news sites, slows cellular service in large cities to a crawl,[6] and ensures that only one "secure" social media platform[7]—a platform in which he is majority shareholder and on which his posts dominate conversation—operates at anything approaching normal speeds.[8] In each case, the imperatives of wartime necessity, as conceived and conceptualized by the chief executive, take charge; communications undermining these ends ought be minimized, in

---

1. *Cf.* William P. Barr, *The U.S. Must Defeat Mexico's Drug Cartels*, WALL ST. J. (Mar. 2, 2023), https://www.wsj.com/articles/the-us-must-defeat-mexicos-drug-cartels-narco-terrorism-amlo-el-chapo-crenshaw-military-law-enforcement-b8fac731.

2. *Cf.* Ashley S. Deeks, *Unwilling or Unable: Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VA. J. INT'L L. 483, 486 (2012).

3 2001 Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001).

4. *Cf.* Ronald Reagan, President of the United States, Radio Address to the Nation on Federal Drug Policy (Oct. 8, 1982).

5. *See generally* Sadaf R. Ali & Shahira Fahmy, *Gatekeeping and Citizen Journalism: The Use of Social Media During the Recent Uprisings in Iran, Egypt, and Libya*, 6 MEDIA, WAR & CONFLICT 55 (2013).

6. *Cf.* T-Mobile USA, Inc., *Order*, 31 FCC Rcd 11410 (2016) (imposing a $7.5 million penalty on T-Mobile for implementing a "de-prioritization" policy on cellular consumers in contravention of unlimited data plan representations).

7. Consider here the Biden Administration's attempts to foreclose government reliance on TikTok by means of the Federal Acquisitions Regulation, 48 CFR §§ 1 *et seq.* *See, e.g.*, Allyson Park, *JUST IN: TikTok Ban Issued for Federal Government Contractors*, NAT'L DEF. (June 26, 2023), https://www.nationaldefensemagazine.org/articles/2023/6/26/just-in-tiktok-ban-issued-for-federal-government-contractors [https://perma.cc/P48V-VHLX].

8. *Cf.* Cheryl Teh, *A pitch deck for Trump's new company claims he's going to build rivals to CNN, Disney Plus, and Netflix*, Bus. INSIDER (Oct. 21, 2021), https://www.insider.com/trump-pitch-deck-claims-build-rivals-cnn-netflix-truth-social-2021-10 [https://perma.cc/J2AE-UN6A].

the interest of the received public good. The President's authority is at a maximum by way of his exercise of war powers, by and through an explicit congressional delegation of power, the courts are loath to second-guess him, steering well clear of the ostensibly partisan and pecuniary motives for these actions.

Or imagine another near-term future, in which a liberal politician ascends to the office of commander-in-chief. Her platform was grounded, in significant part, on grappling with climate change in an aggressively holistic manner. No longer, she vows in her inauguration speech, will the country's response be dictated by the effects of the phenomenon, awkwardly remediating its effects—from rolling blackouts[9] to ballooning toxic algae blooms[10] to ever-increasing spates of heat-related deaths[11]—in an after-the-fact, piecemeal fashion. Instead, the United States will confront the root causes of the environmental crisis, with climate change elevated from a matter of academic and regulatory concern to a national emergency.

Backed by the "unequivocal" conclusion of the United Nations Intergovernmental Panel on Climate Change "that human influence has warmed the atmosphere, ocean and land,"[12] the President, recalling the paramilitary ambitions and confiscatory methods of her predecessors Richard Nixon[13] and Ronald Reagan[14] in their crackdown on controlled substances, declares a war on polluters. The country is, after all, a signatory to the Paris Agreement to the United Nations Framework Convention on Climate Change,[15] committing it to reduce greenhouse gas emissions beneath internationally brokered thresholds.[16] Accordingly, the President sets her

---

9. *Cf.* Lucio Vasquez & Tom Perumean, *ERCOT says Texas could face rolling blackouts in August, as Houston officials announce cooling centers*, HOUSTON PUB. MEDIA (June 7, 2024), https://www.houstonpublicmedia.org/articles/infrastructure/ercot/2024/06/07/489942/texas-could-face-a-grid-emergency-rolling-blackouts-in-august-ercot-report-says/ [https://perma.cc/8D6C-38KK].

10. *Cf.* Frank Cerabino, *Algae blooms, record heat: Florida climate change puts us all in movie with bad ending*, PALM BEACH POST (July 16, 2023), https://www.palmbeachpost.com/story/news/columns/2023/07/16/algae-blooms-high-temps-hot-ocean-climate-change-challenges-florida/70405223007/ [https://perma.cc/7MUF-GPHF].

11. *See, e.g.*, *Extreme Heat*, U.S. DEP'T OF HEALTH AND HUM. SERVS. (2024), https://www.hhs.gov/climate-change-health-equity-environmental-justice/climate-change-health-equity/climate-health-outlook/extreme-heat/index.html [https://perma.cc/6RGN-9ZMX].

12. *Climate Change*, UNITED NATIONS (2024), https://www.un.org/en/global-issues/climate-change [https://perma.cc/8PLN-YP2Y].

13. *See, e.g.*, Antoine Perret, *Militarization and Privatization of Security: From the War On Drugs to the Fight Against Organized Crime in Latin America*, 105 INT'L REV. RED CROSS 828, 829 (2023).

14. *See, e.g.*, Emily Crick, *Reagan's Militarisation of the 'War on Drugs'*, GLOB. DRUG POL'Y OBSERVATORY (Jun. 13, 2016), https://gdpo.swan.ac.uk/?p=440 [https://perma.cc/NDN2-8DXH].

15. *See generally* Environment Agreement Under the United Nations Framework Convention on Climate Change, Dec. 12, 2015, T.I.A.S. No. 16,1104.

16. *See The Paris Agreement*, UNITED NATIONS (2024), https://www.un.org/en/climatechange/paris-agreement [https://perma.cc/GJ4M-P99C].

sights on the nation's share of the 74 million metric tons of greenhouse gas emissions produced by Bitcoin miners each year,[17] calling upon the aforementioned statute to drastically cap the traffic throughput of the data centers that power large-scale digital excavation.[18]

The scenarios are highly implausible, of course, given the robust protections for speech and assembly of the First Amendment, the due process requirements of the Fifth and the Fourteenth, and the beneficent oversight of a congressionally chartered regulatory body, the Federal Communications Commission ("FCC"). And yet I would argue to the contrary: these are states of affairs not only plausible, but frighteningly likely. As the geopolitical grounds of strife shift from the terrestrial to the digital—and the historical roots of war beget conflicts of ambiguous scope and duration in a multiflorous modernity—presidential ambitions to control and constrain communications, I believe, could flourish in few fields so welcoming as Section 706(a)[19] of the Communications Act of 1934, as amended (the "Act").[20]

Titled "War powers of President," Section 706 is divided into four operative components, each of which "grants specific, communications-related powers to the President in time of war or national emergency."[21] Taken as a whole, Section 706 constitutes a critical component of the country's communication infrastructure[22] evinced, for example, in international

17. *See Cambridge Bitcoin Electricity Consumption Index*, CAMBRIDGE CTR. FOR ALT. FIN. (2024), https://ccaf.io/cbnsi/cbeci/ghg [https://perma.cc/T39V-DZKX]; *UN Study Reveals the Hidden Environmental Impacts of Bitcoin: Carbon is Not the Only Harmful By-product*, UNITED NATIONS UNIV. (Oct. 24, 2023), https://unu.edu/press-release/un-study-reveals-hidden-environmental-impacts-bitcoin-carbon-not-only-harmful-product [https://perma.cc/LZ3G-JFU9]; *cf.* Barry O'Halloran, *Data centres not to blame for electricity squeeze, expert claims*, IRISH TIMES (Aug. 20, 2024), https://www.irishtimes.com/business/2024/08/20/data-centres-not-to-blame-for-electricity-squeeze-expert-claims/ [https://perma.cc/E5S3-6EAL].

18. *See, e.g.*, *Countries Say No to Energy Guzzling Bitcoin Mines*, GREENPEACE (May 14, 2024), https://www.greenpeace.org/usa/countries-say-no-to-bitcoin-mines/ [https://perma.cc/G5AA-97DY].

19. 47 U.S.C. § 606(a).

20. 47 U.S.C. § 151.

21. Amendment of Part 73, Subpart G, of the Comm'n's Rules Regarding the Emergency Broad. Sys., *Report and Order and Further Notice of Proposed Rule Making*, 10 FCC Rcd 1786, ¶ 5 (1994); *see also, e.g.*, CBS Broad., *Notice of Apparent Liability for Forfeiture*, 34 FCC Rcd 8417, ¶ 11 (2019) (deeming the Emergency Alert System critical to effectuating the legislative intent undergirding Section 706, as "an essential national defense, emergency, and public safety system" designed to allow the President to engage rapidly and efficiently in crisis communication with the general public).

22. Section 706 parallels the legislative mandate for the creation of the FCC, which charges it to regulate "commerce in communication by wire and radio . . . for the purpose of the national defense" and "promoting safety of life and property." 47 U.S.C. § 151; *see also, e.g.*, Reorganization and Deregulation of Part 97 of the Rules Governing the Amateur Radio Servs., *Report and Order*, 4 FCC Rcd 4719, 4725 (1989) (restricting, "[i]n the event of an emergency which necessitates the invoking of the President's War Emergency Powers under the provisions of Section 706," transmissions of the radio amateur civil emergency service to select frequencies, per the FCC's plenary authority under Section 151). *Cf.* Yankee Network, Inc. v. FCC, 107 F.2d 212, 218 (D.C. Cir. 1939) (citing Section 706's provision for compensation to civilian radio operators in explicating the "rights and equities" available to current and prospective licensees).

transfers of FCC broadcast licenses, where foreign corporations pledge to abide by "the orders of the President in the exercise of his/her authority under § 706" as a manifestation of their compliance in "effective, efficient, and unimpeded fashion" with domestic law.[23]

Two of these four components—subsections (c) (permitting the President to indefinitely suspend or amend "the rules and regulations applicable to any or all stations or devices capable of emitting electromagnetic radiations")[24] and (d) (permitting the President to, *inter alia*, close or nationalize facilities for communication by wire or radio)[25]—have been the subject of extensive study. Roughly a decade ago, multiple monographs[26] opined on the putative interrelationship of these provisions to nascent legislation contemplating an Internet "kill switch,"[27] while others conceptualized them as vital resources in the nation's ability to engage in cyberwar.[28] More recently, the FCC has deployed them in designating Chinese-funded telecommunications corporations as longitudinal national

23. Robert M. Franklin, Transferor and Inmarsat, PLC, Transferee, *Declaratory Ruling*, 24 FCC Rcd 449, 496, 515 (2009); Petition of TelCove, Inc. for a Declaratory Ruling Pursuant to Section 310(b)(4) of the Communications Act of 1934, as amended, *Order and Declaratory Ruling*, 21 FCC Rcd 3982, 3995 (2006).

24. 47 U.S.C. § 606(c).

25. 47 U.S.C. § 606(d).

26. *See generally* David W. Opderbeck, *Does the Communications Act of 1934 Contain a Hidden Internet Kill Switch*?, 65 FED. COMM. L.J. 1 (2013); Kharson K. Thomspon, *Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate*, 90 TEX. L. REV. 465 (2011); William D. Toronto, *Fake News and Kill-Switches: The U.S. Government's Fight to Respond to and Prevent Fake News*, 79 A.F. L. REV. 167 (2018); *see also* Laura B. West, *Building Cyber Walls: Executive Emergency Powers in Cyberspace*, 11 J. NAT'L SECURITY L. & POL'Y 591, 593-94, 598-604 (2021). *Cf.* Jim Dempsey, *Cybersecurity and the 'Good Cause' Exception to the APA*, LAWFARE (Apr. 29, 2022), https://www.lawfaremedia.org/article/cybersecurity-and-good-cause-exception-apa [https://perma.cc/N4ZY-MEB7]; CATHERINE A. THEOHARY & JOHN ROLLINS, CONG. RSCH. SERV., R41674, TERRORIST USE OF THE INTERNET: INFORMATION OPERATIONS IN CYBERSPACE (2011), https://apps.dtic.mil/sti/tr/pdf/ADA544308.pdf [https://perma.cc/PW4X-Q8GS].

27. *See, e.g.*, Protecting Cyberspace as a National Asset Act of 2010, S. 3480, 111th Cong. (2010); Cybersecurity Act of 2010, S. 773, 111th Cong. (2009).

28. *See, e.g.*, Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J. LAW & TECH. 429, 503-06 (2012); David W. Opderbeck, *Cybersecurity and Executive Power*, 89 WASH. U. L. REV. 795, 798-99, 811-12, 839-44 (2013); Roger D. Scott, *Legal Aspects of Information Warfare: Military Disruption of Telecommunications*, 45 NAVAL L. REV. 57, 58, 66 (1998) ("Moreover, the hypothetical capability to disrupt particular telecommunications could be highly controllable and discriminate, focused on individual frequencies or messages . . . Under § 606(a), the President may direct that national defense communications be given precedence or priority over other communications while the U.S. is engaged in war.").

security threats,[29] pursuant to the executive branch's historically broad operationalization[30] of these same emergency powers.[31]

Yet I maintain that the little-known subsection (a) —which focuses on *slowing* rather than *seizing* the operation of commercial communications instrumentalities—constitutes the far more pernicious (and potentially insidious) tool for forestalling free and open discourse in times of putative crisis.[32] Under this subsection, "[d]uring the continuance of a war in which the United States is engaged," the chief executive (whether directly or through his authorized subordinates or through the FCC), "if he finds it necessary for the national defense and security," may "direct that such communications as in his judgment may be essential to the national defense and security shall have preference or priority with any carrier subject to [the Act]."[33] Such directives may be issued "at and for such times as he may determine," and carriers are civilly and criminally immunized from complying with them.[34]

---

29. *See, e.g.*, Huawei Technologies. USA, Inc. v. FCC, 2 F.4th 421, 443-44 (5th Cir. 2021).

30. *See* Exec. Order No. 10,312, 16 Fed. Reg. 12452, 12452 (Dec. 10, 1951) (explaining that establishment of the CONtrol of ELectromagnetic RADiation ("CONELRAD") alerting system was justified, per executive proclamation of a national emergency, on the basis that "government and non-government radio stations may be silenced or required to be operated in a manner consistent with the needs of national security and defense in the event of hostile action endangering the nation, or imminent threat thereof").

31. *See, e.g.*, Amendment of Sections 87.161, 87.163, and 87.165 of the Comm'n's Rules and Regs. to Provide for the Sec. Control of Air Traffic and Air Navigation Aids, *Order*, 14 F.C.C. 2d 635 (1968) (citing Executive Order 10,312 as grounds for "a detailed operational plan for the security control of specified non-Federal air navigation aids"); Amendment of Part 10 of the Comm'n's Rules and Regs. to Effectuate the Comm'n's CONELRAD Plan for the Public Safety Radio Servs., *Notice*, 42 F.C.C. 642 (1955) (explicating the functional and declaratory basis for the establishment of CONELRAD).

32. *Cf.* DeLorean L. Forbes, *Defining "Emergencies": What the United States Can Learn from the United Kingdom about National Emergencies and the Rule of Law*, 37 ARIZ. J. INT'L & COMPAR. L. 411, 422 (2020) (citing Section 706(c) as one of scores of laws notable in "their potential for abuse" by the President). Notably, the Unplug the Internet Kill Switch Act of 2020, S. 4646, H.R. 8336, 116th Cong. (2020), which was intended to "protect Americans' First and Fourth Amendment rights by preventing a president from using emergency powers to unilaterally take control over or deny access to the internet and other telecommunications capabilities," left subsection (a) untouched in proposing comprehensive revisions to Section 706. Press Release, U.S. Sen. Dr. Rand Paul, Dr. Rand Paul Questions Dr. Fauci on Effectiveness of Government Lockdowns, Shutting Down Economy (Sept. 23, 2020) (on file with author) https://www.paul.senate.gov/news-dr-rand-paul-condemns-effort-prevent-president-trump-stopping-endless-war/ [https://perma.cc/E43E-75N5].

33. *See* 47 U.S.C. § 153(11), (51) (defining "common carrier," "carrier," and "telecommunications carrier" for purposes of the Act). *Cf.* Review of Rules and Requirements For Priority Services, *Report and Order*, 35 FCC Rcd 7685, ¶ 1 (2020) (explaining that subsection (a) forms part and parcel of the means by which the President will "leverage access to commercial communications infrastructure to support national command, control, and communications by providing prioritized connectivity during national emergencies," per "prioritized provisioning and restoration of wired communications circuits or prioritized communications for wireline or wireless calls") [hereinafter Rules and Requirements].

34. 47 U.S.C. § 606(a).

Such broad language—and a marked paucity of extant scholarship on its implications—occasions this paper. In Part One, I provide a brief summary of the subsection's evolution and applications from the first decades of the twentieth century. In Part Two, I highlight two of Section 706(a)'s key weaknesses—a poorly defined use of the term "war" as a trigger for its invocation and manifold barriers to judicial review in the event the President opts to invoke it. In Part Three, I note three key emerging techno-political factors—the increasing use of the information domain as a battlefield; the growing ambit of the statute's reference to "carrier" by way of net neutrality; and the capacious legal assertions of the so-called "imperial presidency"—as grounds for additional concern, should this subsection be weaponized in an emergency of nebulous reach and duration.[35] Finally, I propose a comprehensive statutory fix to redress this state of affairs.

II. THE ORIGIN AND CONSTRUCTION OF SECTION 706

On August 13, 1912, Congress passed Public Law 264, "An Act to regulate radio communication," as an attempt to address the growing problem of congestion on the airwaves.[36] Under it, the operation of "any apparatus for radio communication as a means of commercial intercourse" or international communication was predicated on possession of "a license, revocable for cause . . . granted by the Secretary of Commerce and Labor." Each such license, Congress specified, would not only include operational specifications and limitations but a proviso:

> [T]hat the President of the United States in time of war or public peril or disaster may cause the closing of any station for radio communication and the removal therefrom of all radio apparatus, or may authorize the use or control of any such station or apparatus by any department of the Government, upon just compensation to the owners.[37]

As Toronto details at length,[38] this provision was employed roughly one year after the United States' entry into World War I. On July 16, 1918, Congress jointly empowered the President:

---

35. *Cf.* Richard Jackson & Matt McDonald, *Constructivism, US Foreign Policy, and the "War on Terror," in* NEW DIRECTIONS IN US FOREIGN POLICY 18 (Inderjeet Parmar et al. eds., 2009); Jeffrey Record, *Bounding the Global War on Terror* 13-22 (2003).

36. *See, e.g.*, David Moss et al., *Regulating Radio in the Age of Broadcasting*, HARV. BUS. SCH. CASE 716-043 (2016), https://www.hbs.edu/faculty/Pages/item.aspx?num=50386 [https://perma.cc/GXH9-8Y5B].

37. Radio Act of 1912, Pub. L. No. 264, §§ 1, 2 (1912); *see* Opderbeck, *supra* note 26, at 17, 20.

38. *See* Toronto, *supra* note 26, at 177-78; *accord* Opderbeck, *supra* note 28, at 831-832.

> [W]henever he shall deem it necessary for the national security and defense, to supervise or to take possession and assume control of any telegraph, telephone, marine cable, or radio system or systems or any part thereof, and to operate the same in such manner as may be needful or desirable for the duration of the war . . . ."[39]

Following President Wilson's brief exercise of this power,[40] it lay dormant for eight years, until being codified in the Radio Act of 1927 (the "Radio Act"), which provided for enhanced oversight of radio broadcasts and stations by a new regulatory body, the Federal Radio Commission ("FRC").[41]

In 1929, the Senate considered adoption of "a bill to provide for the regulation of the transmission of intelligence by wire or wireless," which would centralize extant authority held by the Interstate Commerce Commission over wireline communication and that of the FRC over radio in a new "communications commission."[42] Notably, Section 40(c) of the bill was equivalent to the present Section 706(a) of the Act,[43] with its language transposed from a 1917 law that empowered President Wilson to grant "preference or priority" to "traffic or such shipments of commodities as, in his judgment, may be essential to the national defense and security" with respect to "transportation by any common carrier by railroad, water, or otherwise."[44] Five years later, this provision would be enacted unchanged under the Act,[45] through which Congress at last "combined and organized federal regulation of telephone, telegraph, and radio communications" under the supervision of the FCC.[46]

In 1941, pursuant to a congressional declaration of war between the United States and the Empire of Japan, Executive Order 8,964 tasked the year-

---

39. 49 H.R.J. Res. 309, 65th Cong., 40 Stat. 904 (1918).

40. Proclamation of July 22, 1918, 40 Stat. 1807 (1918). Government control was terminated on August 1, 1919, exactly one year after it began. *See* Michael A. Janson & Christopher S. Yoo, *The Wires Go to War: The U.S. Experiment with Government Ownership of the Telephone System During World War I*, 91 TEX. L. REV. 983, 986 n.15 (2013) (citing LEONARD S. HYMAN ET AL., THE NEW TELECOMMUNICATIONS INDUSTRY: EVOLUTION AND ORGANIZATION 81 (1987)).

41. An Act For the regulation of radio communications, and for other purposes, 69 Pub. L. 632, 44 Stat. 1162 (1927).

42. *A Bill to Provide for the Regulation of the Transmission of Intelligence by Wire or Wireless: Hearing on S. 6 Before the S. Comm. on Interstate Com.*, 71st Cong. 21-24 (1929), https://acrobat.adobe.com/id/urn:aaid:sc:VA6C2:5a4eda40-6afb-4951-90a5-7a702e2d6c1a [https://perma.cc/R6GZ-WUJ8].

43. *Id.* at 18.

44. An Act To amend the Act to regulate commerce, as amended, and for other purposes, Pub. L. No. 39, 40 Stat. 270 (1917). *Cf.* 56 Cong. Rec. 2014, 2016, 2029 (1918).

45. *Compare* 47 U.S.C. § 606(a) (2023), *with* 47 U.S.C. § 606(a) (1934).

46. Bureau of Justice Assistance, *The Communications Act of 1934, 47 U.S.C. § 151 et seq.*, U.S. DEP'T OF JUSTICE, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1288 [https://perma.cc/F8HQ-J6FH] (last visited January 1, 2025). *Cf. Roosevelt Urges Board of Control on Wires, Radio*, N.Y. TIMES, Feb. 26, 1934, at 1, https://graphics8.nytimes.com/packages/pdf/business/rooseveltturges.pdf [https://perma.cc/G9KG-YUMC].

old Defense Communications Board[47] with frequency allocation, government seizure or closure of radio stations, and, "in accordance with Section 606(a) of the Communications Act of 1934, to make such arrangements as may be necessary to insure that communications essential to the national defense or security shall have preference or priority . . . "[48] Subsequently given additional powers by Executive Order per contemporary congressional enhancements to Section 706[49] and renamed the Board of War Communications,[50] it was abolished by President Truman on February 24, 1947.[51]

Subsection (a), then, as employed in World War II, bore a functionalist propinquity to the Defense Production Act, which tapped "the domestic industrial base to supply materials and services for the national defense" to satisfy the urgent needs of "military production" and the "unique technological requirements" under "emergency conditions."[52] As Opderbeck

47. *See* Exec. Order Creating the Defense Communications Board and Defining Its Functions and Duties, 5 Fed. Reg. 3817, 3817 (Sept. 26, 1940) (defining the Defense Communications Board as an entity for "coordinated planning for the most efficient control and use of radio, wire, and cable communication facilities under jurisdiction of the United States in time of national emergency," per the needs of the armed forces and "the needs of other governmental agencies, of industry, and of other civilian activities").

48. Exec. Order Prescribing Regs. Governing the Use, Control and Closing of Radio Stations and the Prefrence or Priority of Commc'n, 6 Fed. Reg. 6367, 6367-68 (Dec. 12, 1941).

49. *See* Exec. Order Prescribing Regs. Governing the Use, Control and Closing of Radio Stations and Facilities for Wire Commc'ns, 7 Fed. Reg. 1777, 1777-78 (Mar. 10, 1942). *Cf.* Am. Med. Ass'n v. United States, 130 F.2d 233, 247 n.66 (1942) (citing 47 U.S.C.A. § 606(c), (d), as amended by Pub. L. No. 413) ("It is perhaps significant that in the latest professional development - radio broadcasting - increased emphasis has been placed on . . . governmental control.").

50. *See* Exec. Order No. 9,183, 7 Fed. Reg. 4509, 4509 (June 17, 1942).

51. *See* Exec. Order No. 9,831, 12 Fed. Reg. 1363, 1363 (Feb. 26, 1947).

52. 50 U.S.C. § 4501(a)(1), (3)(C)(i)-(ii), (7).

illustrates, shifting postwar imperatives functionally[53] and substantively[54] relegated it to the realm of civil defense, per a series of Executive Orders that prompted "various agencies, including the Federal Communications Commission, [to] adopt contingency plans for war and national emergencies" under the authority of Section 706.[55] The National Security Council ("NSC") served to coordinate these efforts, ensuring a unified blueprint for preserving the preference of "communications for the federal government under emergency conditions, including nuclear attack."[56]

Recent administrations have employed Section 706(a) as a critical tool for ensuing the uninterrupted flow of "[s]urvivable, resilient, enduring, and effective communications"[57] between and among the various arms of the federal government. The Obama White House's Executive Order 13,618, for instance, tasked both the Assistant to the President for Homeland Security and Counterterrorism and the Director of Office of Science and Technology Policy ("OSTP") with advising on and monitoring the use of the authorities set forth by Section 706, with the latter instructed to "advise the President on the prioritization of radio spectrum and wired communications that support NS/EP [national security/emergency preparedness] functions."[58] The Trump Administration revised these plans, empowering the Director of OSTP "to exercise the authorities vested in the President by section 706(a) . . . if the

53. *Compare* 47 U.S.C. § 151 (creating a Federal Communications Commission for the purpose of, *inter alia*, "the purpose of the national defense" and "the purpose of promoting safety of life and property through the use of wire and radio communications"), *with* STEPHEN K. COLLIER & ANDREW LAKOFF, THE GOVERNMENT OF EMERGENCY: VITAL SYSTEMS, EXPERTISE, AND THE POLITICS OF SECURITY 260-61 (Princeton Univ. Press, 2021) (detailing the "March 1954 Defense Mobilization Order to the [Federal Civil Defense Administration]. . . . which assigned [it] responsibility for measures relating to the protection of life and property against attack and for dealing with the civil defense emergency conditions arising out of attack") (internal quotation marks omitted).

54. *See, e.g.*, *Independent Offices Appropriations for 1967: Hearings Before the Subcomm. on Indep. Offs. of the H. Comm. on Appropriations*, 89th Cong. 1568 (1966) https://www.govinfo.gov/app/details/CHRG-89hhrg61473p2/CHRG-89hhrg61473p2 [https://perma.cc/9TUU-K4LK] (summarizing the "plans and programs" designed by the FCC under Executive Order 11,092, 28 Fed. Reg. 203 (Jan. 9, 1963), "to develop a state of readiness . . . with respect to all conditions of emergency, including attack upon the United States," which "take into account the possibility of Government preference or priority with common carriers or of exclusive Government use or control of communications services or facilities when authorized by law"); Exec. Order No. 11,556, 35 Fed. Reg. 14193, 14193 §§ 2(a), 4(a) (Sept. 9, 1970) (delegating to the Director of the Office of Telecommunications Policy, "the President's principal adviser on telecommunications . . . . the authority vested in the President by subsections 606 (a), (c), and (d) of the Communications Act of 1934, as amended . . . . under the overall policy direction of the Director of the Office of Emergency Preparedness").

55. Opderback, *supra* note 28, at 831.

56. Armstrong v. Exec. Office of the President, 90 F.3d 553, 562 (D.C. Cir. 1996).

57. Exec. Order No. 13,618, 77 Fed. Reg. 40779 § 1 (July 6, 2012).

58. *Id.* at § 2.2.

President takes the actions, including issuing any necessary proclamations and findings, required by that section to invoke those authorities."[59]

III. CRITICAL QUESTIONS OF WAR AND EXECUTIVE AUTHORITY

Given the seemingly innocuous applications of Section 706(a) to date—a pointed exigency arising from the extraordinary demands of existential conflict and a backstop for federal crisis communications in the nuclear age—the scenarios that introduced this paper seem even more implausible. And yet, I maintain that this subsection remains amenable to abuse, exceeding the scope of its historical development and the congressional intent that undergirds it. Key to this argument is its pregnant use of the word *war* and its pointed resistance, when operationalized by the President, to judicial review.

A. The Meaning of "War"

While subsection (a) turns on the phrase "continuance of war in which the United States is engaged," it fails to define that war's character[60]—is it an international armed conflict, an internal armed conflict, or one of the many cases on the margins, such as those in the realm of "cyber operations?"[61] Complicating the question is the use of the passive voice: "engagement" says

59. Exec. Order No. 13,961, 85 Fed. Reg. 79379, 79380 § 6(a) (Dec. 7, 2020); *cf.* U.S. DEP'T OF HOMELAND SEC., FEDERAL EMERGENCY MANAGEMENT AGENCY, FEDERAL CONTINUITY DIRECTIVE 1: FEDERAL EXECUTIVE BRANCH NATIONAL CONTINUITY PROGRAM AND REQUIREMENTS (2017), https://www.gpo.gov/docs/default-source/accessibility-privacy-coop-files/January2017FCD1-2.pdf [https://perma.cc/VR6H-BN58] (summarizing Presidential Policy Directive 40, which "directs the Secretary of Homeland Security through the Administrator of the Federal Emergency Management Agency . . . to coordinate the implementation, execution, and assessment of continuity activities among executive departments and agencies").

60. In a 1939 address to the Indianapolis Bar Association, for example, Senator Robert A. Taft highlighted the "dangers to democratic processes attendant upon modern warfare," by way of the "extensive" emergency authorities afforded the chief executive. 85 CONG. REC. 714. Reviewing Section 706(a), he commented: "It appears, therefore, that [the President's] powers with respect to telephone and telegraph systems are much more limited, and even then may only be exercised in time of war. But we saw that President Wilson imposed a strict censorship in the World War without statutory authority." *Id.* at 715.

61. *See* Prosecutor v. Tadić, No. IT-94-1-l, Decision on Defense Motion for Interlocutory Appeal on Jurisdiction, ¶ 65, 70, (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995), http://www.icty.org/x/cases/tadic/acdec/en/51002.htm [https://perma.cc/3JQH-G6KP]; *Cyber warfare and international humanitarian law: The ICRC's position*, INT'L COMM. RED CROSS (June 28, 2013), https://www.icrc.org/sites/default/files/external/doc/en/assets/files/2013/130621-cyber-warfare-q-and-a-eng.pdf [https://perma.cc/2LYR-GYSZ]; *cf.* John C.F. Tillson & Robert Fabrie, *OSD Duties in the Respond Strategy*, INST. DEF. ANALYSIS (Jan. 1999), https://apps.dtic.mil/sti/tr/pdf/ADA375146.pdf [https://perma.cc/49N3-AFJE] ("During *any war*, the President may order any carrier to give preference or priority for national defense communications.") (emphasis added).

nothing of whether the war at issue began by dint of congressional declaration, arose out of a first strike by a hostile actor, or commenced by way of quasi- or extra-legal action on the part of the commander-in-chief.[62]

Legislative history is of little assistance in defining "war." In hearings on the Radio Act held in March 1924, Major J. O. Mauborgne, amplifying a missive from Secretary of War John W. Weeks, describes the legislation's apparent failure to prioritize the frequency requirements of the Army in times of peace and for the overall national defense. In contrast:

> The situation, of course, in time of war, so far as interfering with other people is concerned, is very nicely taken care of by the bill, because the bill says the President may take over any stations he wants for the War Department, and he can naturally also assume control of broadcasting at that stage of the situation , and he can stop broadcasting, if it becomes necessary to do so in the national defense.[63]

But for a suggestion that the President, in directing traffic, is acting on behalf or in the interest of the military directorate, the "time of war" and "national defense" constructs mirror those in present-day Section 706(a).

The legislative history for the Act is largely similar.[64] In a lengthy exchange between Louis G. Caldwell, chairman of the American Bar Association's radio committee, and Senator Clarence Dill,[65] a nebulous "time of war" is adjudged the predicate to the President's "right to close down any station or to take over any station."[66] Caldwell, however, does suggest, in an interchange with Senator Key Pittman, that the right vests (vis-à-vis the same

62. *Cf.* Robert F. Daly & Donald L. Nielson, *A Review of National Security-Emergency Preparedness Telecommunications Policy*, SRI INT'L 1, 32 (1981) https://apps.dtic.mil/sti/pdfs/ADA100190.pdf [https://perma.cc/95WR-UH9X] ("[E]ach of the specific powers for control is explicitly limited to national emergency and *war conditions*. The powers to establish communications procedures and priorities and to use the armed forces to prevent obstruction of communications services are confined to *conditions of actual war* . . . .") (emphasis added).

63. *To Regulate Radio Communication: Hearings on H.R. 7357 Before the H. Comm. on Merch. Marine and Fisheries*, 68th Cong. 137 (1924).

64. A comparison between the originating bills for the Act, H.R. 8301 and S. 3285, demonstrates no difference between them in the wording of Section 706(a). *See* COMMUNICATIONS BILL: COMPARATIVE PRINT SHOWING DIFFERENCES BETWEEN H.R. 8301 AND S. 3285 AS PASSED BY THE SENATE ON MAY 15, HOUSE COMMITTEE ON INTERSTATE AND FOREIGN COMMERCE 106-07 (1934).

65. Dill was intimately involved in communications policy; as a co-author of the Radio Act, he was a prime architect of the "public interest, convenience, and necessity" standard that undergirds the FCC's licensing and regulatory powers. *See* Erwin G. Krasnow & Jack N. Goodman, *The "Public Interest" Standard: The Search for the Holy Grail*, 50 FED. COMM. L.J. 605, 609-10 (1998).

66. *Committee on Communications: Hearing Before the Comm. on Interstate Com.*, 71st Cong. 52 (1930), https://heinonline.org/HOL/P?h=hein.cbhear/cochus0001 [https://perma.cc/L7ZL-F9P6].

"time of war" phrasing) "as soon as war is declared."[67] A similar discursive construct is employed in testimony by Army Signal Corps Major General George Owen Squier, which asserts that "the Army and Navy in time of war" (as counterposed against "time of peace" and "peacetime") "should have the use of all [available radio frequencies] if necessary" and that the President "will take over everything in time of war anyway."[68]

The implementing regulations for Section 706, 47 CFR § 201.0 *et seq*., are also unavailing. These rules distinguish between "crises and emergencies, wartime and non-wartime," but define the former concept recursively, whereby a "wartime emergency means a crisis or event which permits the exercise of the war power functions of the President under section 706 . . . "[69] While note is taken, however obliquely, of the disparity between the President's "limited non-wartime NS/EP telecommunications functions . . . and wartime NS/EP functions" under the Act, this observation is made in the context of "survival and recovery during a crisis or emergency" occasioning an "unavoidable interdependence between and among Federal, State, and local authorities" and the federal government's use of lesser authorities "for management or control of intrastate carrier services and continuity of interconnectivity with interstate carriers . . . "[70] In other words, "wartime" and its counterpart, for purposes of these rules, are little more than conceits, demarcations of convenience intended to maximize the unity of presidential command across jurisdictional lines whenever Section 706(a) is invoked.[71]

FCC decisions fail to provide any additional granularity. In 2020's *Rules and Requirements for Priority Services*, the agency updated its decades-old rules for granting NS/EP personnel access to "priority service programs" that facilitate emergency communications.[72] Again, the critical inflection point between war and non-war is more semiotic than substantive; revisions to a Department of Homeland Security wireless access framework, for

67. *Id.* at 147 ("There are other provisions of the act that amply protect us in time of war and provide for sufficient control of the situation. The President, for example, can shut down any station, or take it over, as soon as war is declared.").

68. *Id.* at 205.

69. 47 C.F.R §§ 201.2(m), 201.3(a), (b) (2024); *see also* 47 C.F.R § 201.3(e) (2024) (restating the powers available under subsection (a) to the President "during war").

70. 47 C.F.R. § 201.3(b)(1), (2) (2024).

71. *Cf.* 47 C.F.R § 201.3(f) (2024) ("During an attack on the United States by an aggressor nation, and in an immediate postattack period, all decisions regarding the use of telecommunications resources will be directed to the objective of national survival and recovery."). *Cf.* Opderbeck, *supra* note 26, at 41 ("Even if subsection 606(d) is read against a background of unlimited ancillary jurisdiction over the Internet, it applies *only* in wartime. The same is true of subsections (a) and (b), which are war powers only, and not broader emergency powers . . . . This difference makes sense in light of the differing purposes of subsections (a), (b), and (d) in contrast to subsection (c) . . . . [as] a Cold War measure designed to frustrate the capacity of a hostile country such as the Soviet Union to launch a nuclear first strike.").

72. Modernizing Priority Servs. Rules to Support Emergency Personnel, *Notice of Proposed Rulemaking*, 35 FCC Rcd 7685, ¶¶ 1-3 (2020) (predicating rulemaking on the development of Internet Protocol-based technologies in the years following the 1988 establishment of a Telecommunications Service Priority program for NS/EP users).

instance, is bifurcated between the "before and after" of the moment when the President invokes his emergency war powers, even as it recognizes that the temporal formulation itself may be "superseded by the President's emergency war powers."[73]

Caselaw is, in the main, unavailing.[74] One of the few decisions to bear on Section 706(a) is *Bendix Aviation Corp. v. Federal Communications Commission*, in which a group of aviation operators and equipment manufacturers protested the FCC's reclassification of radio bands for civil defense purposes absent statutorily mandated notice-and-comment.[75] The court dismissed their claim pursuant to the expansive national security concerns attendant upon the issuance of Presidential Proclamation 2914, which cited both the "recent events in Korea and elsewhere" and "the increasing menace of the forces of communist aggression" as the basis for "the existence of a national emergency."[76] Supporting the putative need to center "[n]ational trust and responsibility" in the President, the court reasoned, was Section 706, "which in circumstances specified, expands the President's authority to reach and control even already licensed stations and facilities."[77]

A few cases may bear on the question if World War I antecedents to subsection (a) are considered. In *Commercial Cable Co. v. Burleson*, plaintiff telegraph companies sought to enjoin President Wilson's seizure of their communications lines under the aforementioned 1918 joint resolution, arguing that the White House had failed to utilize them for expeditionary military needs and that the seizure occurred on November 16, 1918, five days after an armistice with the Central Powers was signed.[78] The court characterized the first argument as "a lame comprehension of the scope and variety of modern war," noting that cases of domestic espionage and interdependent transnational campaigns militated against the conclusion "that means of telegraphic communications anywhere in the world were not appropriate to its prosecution."[79] The court also dismissed plaintiffs' emphasis on chronological logics, adjudging an armistice not an end to war, but a mere "suspension of hostilities."[80] To this end, the court opined on the President's critical (and Constitutional) role in treaty-making: "The national security and defense is to be judged . . . by the stability of the ensuing state of

73. *Id.* at ¶ 1 (2020).

74. This is also true if the scope of the inquiry is expanded to analogous language in the now-defunct 49 U.S.C. § 1(15)(d), under which the Interstate Commerce Commission, "[i]n time of war or threatened war," was afforded license to give "preference or priority in transportation" upon certification by the President that such was "essential to the national defense and security." *See, e.g.*, Interstate Com. Comm'n v. Or. Pac. Indus., Inc., 420 U.S. 184, 186-87 n.2 (1975); U.S. v. Interstate Com. Comm'n, 352 U.S. 158, 174 (1956); U.S. v. Thompson, 58 F. Supp. 213 n.2 (E.D. Mo. 1944).

75. Bendix Aviation Corp. v. FCC, 272 F.2d 533 (D.C. Cir. 1959).

76. PUB. PAPERS OF THE PRESIDENTS OF THE U.S.: HARRY S. TRUMAN 746-47 (Off. of the Fed. Reg., Nat'l Archives and Recs. Serv., & Gen. Serv. Admin., 1950).

77. *Bendix Aviation Corp.*, 272 F.2d at 540 n.24.

78. Commercial Cable Co. v. Burleson, 255 F. 99, 101, 104-06 (S.D.N.Y. 1919).

79. *Id.* at 104

80. *Id.* at 104-05.

peace. The terms of the final conventions . . . are the measure of that [national] security and defense."[81]

Likewise, in *Central Telephone Co. v. South Dakota*, the Supreme Court, in assessing the legality of federally mandated wartime intrastate telephone rates, deemed dispositive missives from "the highest authorities of the federal Government [that] acknowledged that the war had ended"—namely, messages from President Wilson to Congress dated November 11 and December 2, 1918.[82] Some thirty years later, the Western District of New York would synthesize these decisions in granting the government's motion for an injunction against striking railway workers.[83] While the Korean War was but a few months old, the conflict provided a critical basis for government action,[84] as "[t]he statutes effective only 'in time of war'" attach independently of military engagement, "continu[ing] in force until a formal statement of peace is declared."[85]

"War," then, for purposes of Section 706(a), is nebulous, with potential sources of interpretive guidance given to circular logic and an overweening retreat to the tautologies of executive authority. Simply put, the condition of

---

81. *Id.* at 105-06; *accord* Sw. Tel. & Tel. Co. v. Houston, 256 F. 690, 697 (D. Tex. 1919) ("The signing of the armistice did not terminate the war. We are still at war, although active hostilities have been suspended, and may not be renewed. This Telephone Act, however, must be interpreted in the light of conditions as they existed at the time of its passage by Congress . . . .").

82. Central Tel. Co. v. South Dakota, 250 U.S. 163, 179 (1919); *accord* Woodrow Wilson, President of the U.S., Sixth Annual Message. at UVA Miller Center (Dec. 2, 1918) https://millercenter.org/the-presidency/presidential-speeches/december-2-1918-sixth-annual-message [https://perma.cc/K9MU-35EY] ("And now we are sure of the great triumph for which every sacrifice was made. It has come, come in its completeness, and with the pride and inspiration of these days of achievement quick within us, we turn to the tasks of peace again . . . ").

83. U.S. v. Switchmen's Union of N. Am., 97 F. Supp. 97, 102 (W.D.N.Y. August 11, 1950) ("Next I find that a continuance or resumption of the strike will deprive the Nation of an essential transportation service and will substantially obstruct the flow of interstate commerce and the transmission of the mails of the United States over the affected railway system.").

84. *See id.* at 100 ("It is believed that this court can take judicial notice of the United Nations' conflict over Korea. This greatly emphasizes the necessity for the continued operation of this railroad.") (internal citation omitted); *see also, e.g.*, Parker v. Lester, 98 F. Supp. 300, 303 (N.D. Cal. 1951) (denying, apropos of executive and administrative provisions predicated on prophylactic actions deemed "essential to our national defense, to the implementation of the North Atlantic Pact, Economic Cooperation Administration, and to the prosecution of hostilities in Korea," motion to enjoin requirement that transnational commercial mariners obtain a security clearance as a prerequisite to gainful employment, per a finding that "[h]owever grievous the personal deprivation petitioners have suffered, the additional sacrifice they are called upon to make by this denial of their motion bulks small beside the incalculable loss which might result if this court summarily suspended, even in part, the security program"); *cf.* Harry S. Truman, President of the U.S., Radio and Television Address to the American People on the Need for Government Operation of the Steel Mills (Apr. 8, 1952) ("These are not normal times. These are times of crisis.").

85. *Switchmen's Union of N. Am.*, 97 F. Supp. at 100 ("However, neither the war with Germany nor Japan has ever been dissolved and no treaty of peace has followed these wars.").

war stands appositionally to a condition of non-war in the commander-in-chief's invocation of his war powers; it endures, as something of an analogue to the equally murky national emergency that impinges upon the national security, for as long as the President exercises them, even, *qua* pre-Act precedent, to the bounds of formally declared peace.[86] This formulation accords notably with the distinction under international law between a *declaration of the existence of a state of war* (effecting, at bottom, a relational change between the states subject to it and mobilizing the domestic appurtenances incumbent upon the "law of war," such as Section 706(a)) and a *declaration of war* (substituting the "law of war" for the "law of peace" and undergirding the use of armed force).[87] In other words, in invoking subsection (a), the commander-in-chief can elide the knotty questions of the how, when, and why of a conflict's genesis in focusing on the fact (or "continuance") of its prosecution, attesting to its apparent existence as justification for any and all communications preference and prioritization deemed necessary to its resolution.

B. The Prospects for Judicial Review

Further complicating the potential scope of Section 706(a) are the obstacles to effective judicial review. Assuming, however unlikely,[88] a concerted protest by the statutorily affected, the prospects for redress at bar against putative presidential abuse appear exceedingly remote.

The critical analytical framework for adjudging the constitutionality of emergency executive actions was set forth by *Youngstown Tube & Sheet Co. v. Sawyer*, in which the Supreme Court rebuffed President Truman's attempt to nationalize most of the country's steel mills pursuant to the ongoing police

---

86. *See, e.g.*, DUSTIN A. LEWIS ET AL., INDEFINITE WAR: UNSETTLED INTERNATIONAL LAW ON THE END OF ARMED CONFLICT (Harvard L. Sch. Program on Int'l L. & Armed Conflict, 2017) https://dash.harvard.edu/bitstream/handle/1/30455582/Indefinite%20War%20-%20February%202017_3.pdf?sequence=4&isAllowed=y [https://perma.cc/HMY4-LPM4]. *Cf.* Kevin Snow, *Congress Continues the Long Path Toward Repealing the 2002 AUMF*, FRIENDS COMM. ON NAT. LEGIS. (July 21, 2023), https://www.fcnl.org/updates/2023-07/congress-continues-long-path-toward-repealing-2002-aumf [https://perma.cc/6CNF-RU2Y].

87. *See* JENNIFER K. ELSEA & RICHARD F. GRIMMETT, CONG. RSCH. SERV., RL31133, DECLARATIONS OF WAR AND AUTHORIZATIONS FOR THE USE OF MILITARY FORCE: HISTORICAL BACKGROUND AND LEGAL IMPLICATIONS 22-29 (2006).

88. Subsection (a) specifically immunizes carriers from civil or criminal penalties in "complying with any . . . order or direction for preference or priority herein authorized." 47 U.S.C. § 606(a). Moreover, as detailed by Bd. of Regents v. Nippon Tel. & Tel. Corp., No. A-01-CA-478 SS, 2004 U.S. Dist. LEXIS 28819, at *27 (W.D. Tex. June 1, 2004), there exists a discursive distinction between a corporation amenable, by way of voluntarily licensing, to wartime necessity, and the same private concern rendered effectively "an organ of the state." *See, e.g.*, Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts*, 43 VAND. J. TRANSNAT'L L. 1011, 1016-17 (2010) (explicating, per international law, the legality of compelled civilian participation in armed conflict); *cf.* David Gray, *Is Google a State Agent?*, 27 STAN. TECH. L. REV. P206, P209-14 (2024).

action on the Korean peninsula.[89] In a concurring opinion, Justice Jackson promulgated a tripartite taxonomy for assessing the legality of presidential authority under extraordinary conditions.[90] Germane to the present inquiry is the first circumstance, which establishes that presidential "authority is at its maximum" when predicated on "an express or implied authorization of Congress."[91] There can be little doubt, per the broad enabling language of and well-entrenched history behind subsection (a), that a future chief executive would enjoy "the strongest of presumptions and the widest latitude of judicial interpretation" in a challenge to his powers exercised thereunder.[92]

A potential recourse to this state of affairs might be derived from the non-delegation doctrine.[93] While the Constitution exclusively vests law-making authority in Congress,[94] the 1928 *Hampton* decision provided that the legislature may delegate it to the executive or regulatory realms, provided it is accompanied by "an intelligible principle to which the person or body authorized . . . is directed to conform."[95] Seven years later, however, the Supreme Court cabined this pronouncement, observing in *Panama Refining Co. v. Ryan* "that there are limits of delegation which there is no constitutional authority to transcend"[96]

Putting aside the efficacy of this non-delegation doctrine as a practical check on the ambitions of the executive branch,[97] its utility in forestalling abuse of Section 706(a) is questionable. In *National Broadcasting Co. v. United States*,[98] the Supreme Court considered the scope of the FCC's duties as licensor responsible for allocating portions of a limited electromagnetic spectrum to prospective broadcasters. Observing that "[t]he facilities of radio are not large enough to accommodate all who wish to use them," the Court opined that the FCC was responsible for both "determining the composition of [communications] traffic" and "policing the wave lengths to prevent stations from interfering with each other"[99]—communications management tasks remarkably similar to those described in Section 706(a). In discharging these tasks, the Court emphasized that the FCC "was not left at large" per an intelligible congressional "touchstone"[100]—the statutory "public interest,

89. Youngstown Tube & Sheet Co. v. Sawyer (Steel Seizure), 343 U.S. 579 (1952) (Jackson, J., concurring).

90. *Id.* at 635-38.

91. *Id.* at 635.

92. *Id*. at 637. *Cf.* U.S. v. Western Union Tel. Co., 272 F. 311, 315 (S.D.N.Y. 1921) ("[I]t it does not appear . . . that the President, either in the exercise of the delegated legislative powers given him by Congress or in the exercise of his constitutional power to negotiate treaties, could seize cables even in time of war without legislative authority.").

93. I am indebted to Professor Joseph Blocher for suggesting this line of inquiry.

94. U.S. CONST. art. I, § 1.

95. J.W. Hampton, Jr., & Co. v. United States, 276 U.S. 394, 409 (1928).

96. Panama Refining Co. v. Ryan, 293 U.S. 388, 430 (1935).

97. *See, e.g.*, Keith E. Whittington & Jason Iuliano, *The Myth of the Nondelegation Doctrine,* 165 U. PA. L. REV. 379, 381-83 (2017); Eric A. Posner & Adrian Vermeule, *Interring the Nondelegation Doctrine*, 69 U. CHI. L. REV. 1721, 1721-22 (2002).

98. National Broadcasting Co. v. United States, 319 U.S. 997, 999 (1943).

99. *Id.* at 1110.

100. *Id.*

convenience, and necessity" standard,[101] possessed of sufficient granularity as to defeat invocation of the non-delegation doctrine.[102]

Inasmuch as *National Broadcasting Co.* supports a delegation in peacetime of the highly complex work of communications traffic management—per the well-founded "practical understanding that in our increasingly complex society, replete with ever changing and more technical problems, Congress simply cannot do its job absent an ability to delegate power under broad general directives"[103]—there exists no overriding jurisprudential standard by why such a delegation would be invalid in war, especially in light of the foregoing discussion of the fluid nature of these socio-political conditions.[104] This is particularly true when adjudging the intelligible principles putatively at issue in each delegation: the "public interest, convenience, and necessity" standard, which, while tenable, has been the subject of protracted criticism for its vague construction and historically mutable application.[105] Such phrasing is notable in comparison to Section 706(a)'s reference to traffic management actions deemed "necessary" and "essential" to "the national defense and security,"[106] which is entitled to

101. 47 U.S.C. §§ 307(a), 308, 309(a), 310(d).

102. *See* Richard A. Epstein, *How Bad Constitutional Law Leads to Bad Economic Regulations*, ATLANTIC ONLINE (Oct. 20, 2019), https://www.theatlantic.com/ideas/archive/2019/10/how-bad-constitutional-law-leads-bad-regulations/600280/ [https://perma.cc/P29W-NDQD].

103. Mistretta v. United States, 488 U.S. 361, 372 (1989).

104. Review of the Emergency Alert Sys., 80 Fed. Reg. 37167 (proposed July 30, 2015) (to be codified at 47 C.F.R. pt. 11); *see, e.g.*, Touby v. U.S., 500 U.S. 160, 165 (1991) ("We have long recognized that the nondelegation doctrine does not prevent Congress from seeking assistance, within proper limits, from its coordinate Branches. Thus, Congress does not violate the Constitution merely because it legislates in broad terms, leaving a certain degree of discretion . . . ."); Opp Cotton Mills, Inc. v. Adm'r of Wage & Hour Div., 312 U.S. 126, 145 (1941) ("The Constitution, viewed as a continuously operative charter of government, is not to be interpreted as demanding the impossible or the impracticable. The essentials of the legislative function are the determination of the legislative policy and its formulation as a rule of conduct."). This elision is also evinced by the emergency operations of FCC-licensed broadcasters, which, both legally—*see, e.g.*, Review of the Emergency Alert Sys., *First Report and Order and Further Notice of Proposed Rulemaking*, 20 FCC Rcd 18625, ¶¶ 21-22, 25, 37, 54 (2005), *reconsideration granted in part, denied in part sub nom*, Amendment of Part 11 of the Comm'ns Rules, *Order on Reconsideration*, 33 FCC Rcd 7490 (2019) and practically—*see, e.g.*, Patric R. Spence et al., *Serving the Public Interest in a Crisis: Does Local Radio Meet the Public Interest?*, 19 J. CONTINGENCIES & CRISIS MGMT. 227, 227, 232 (2011)—are structured along the same "public interest" construct attendant under ordinary conditions.

105. *See, e.g.*, Krasnow & Goodman, *supra* note 65; David B. Froomkin, *The Nondelegation Doctrine and the Structure of the Executive*, 41 YALE J. ON REG. 60, 78-79, 88, 92-93 (2024); Randolph J. May, *A Modest Plea for FCC Modesty Regarding the Public Interest Standard*, 60 ADMIN. L. REV. 895, 899-901 (2008); Willard D. Rowland Jr., *The Meaning of "the Public Interest" in Communications Policy, Part I: Its Origins in State and Federal Regulation*, 2 COMM. L. & POL'Y 309, 309-15 (1997); Willard D. Rowland Jr., *The Meaning of "the Public Interest" in Communications Policy – Part II: Its Implementation in Early Broadcast Law and Regulation*, 2 COMM. L. & POL'Y 363, 364-66 (1997).

106. 47 U.S.C. § 606(a) ("During the continuance of a war in which the United States is engaged, the President is authorized, if he finds it necessary for the national defense and security, to direct that such communications as in his judgment may be essential to the national defense and security . . . .").

especial deference as an extension of the President's constitutional authority as commander-in-chief.[107]

The aforementioned pre-Act cases buttress these conclusions, subordinating the whys-and-wherefores of specific communicative preferences or prioritizations to the judgment of the Commander-in-Chief. In *Commercial Cable*, the court reasoned that the purpose of the joint resolution authorizing executive seizure and control of the nation's telecommunications infrastructure "was to put the property at the general disposal of the President in the discharge of some of his constitutional functions, without inquiry as to the specific purposes which he might have in mind."[108] Judicial second-guessing would, in any case, threaten the urgent business of the "effective prosecution" of the war; the President, in the cause of the national defense, "had to act quickly, certainly, and without the trammels of courts or private interests."[109] More pointedly, in *Dakota Central*, the Supreme Court dismissed attacks upon "the motives" impelling President Wilson to take charge of telephone lines; "as the contention at best concerns not a want of power, but a mere excess or abuse of discretion in exerting a power given, it is clear that it involves considerations which are beyond the reach of judicial power."[110]

Further pre-Act cases provide additional support. In *Southwestern Telegraph and Telephone Co. v. City of Houston*,[111] the Texas Southern District, quoting the seminal *Legal Tender Cases*,[112] enjoined a municipality's attempt to forestall the imposition of government-prescribed calling rates. "The act authorizing the taking over of the telegraph and telephone lines, being a war measure, should be liberally construed," the *Southwestern Telegraph and Telephone* court reasoned, and clear deference paid to Congress's use of "its vast power in time of war and public peril . . . for the husbanding and marshaling of the resources of the nation."[113] A state court, confronting directly the fact of corporate seizure, put it more bluntly, apropos of a series of federal authorities: "The war power and all powers incident to it

---

107. *See, e.g.*, In re NSA Telecomms. Records Litig., 671 F.3d 881, 897-98 (9th Cir. 2011) (because a challenged provision of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. §§ 1801 *et seq.*, "arises within the realm of national security—a concern traditionally designated to the Executive as part of his Commander-in-Chief power . . . the intelligible principle standard need not be overly rigid … The Supreme Court has repeatedly underscored that the intelligible principle standard is relaxed for delegations in fields in which the Executive has traditionally wielded its own power.") (citation omitted).

108. 255 F. at 102.

109. *Id.* at 103-04.

110. 250 U.S. at 184. *But see id.* at 176 (deeming it "the duty of the court in a proper proceeding" to examine "recitals" by the executive branch regarding the wartime necessity for increasing telephone rates per an apparent congressional disapproval of such an assertion).

111. Sw. Tel. and Tel. Co. v. Houston, 256 F. 690, 696 (S.D. Tex. 1919).

112. 79 U.S. 457, 563 (1871) ("In certain emergencies government must have at its command, not only the personal services—the bodies and lives—of its citizens, but the lesser, though not less essential, power of absolute control over the resources of the country.").

113. Sw. Tel. & Tel. Co., 256 F. at 696.

reside in the nation's right of self-preservation, and the means of enforcing such right are left to the discretion of the nation, and cannot be interfered with at the pleasure of the States or their courts."[114]

A final impediment to effective judicial review arises from the seemingly anodyne subject matter of subsection (a). Well apart from the instrumentalities at the commander-in-chief's disposal undergirding the deployment of brigades and batteries—or even the reconstitution of civilian-facing communication systems in the face of existential threats[115]—subsection (a) is possessed of a far less-threatening recourse to traffic management. The President, in other words, might not have the authority to eliminate the ability of citizens to access a platform like Substack or Bluesky, but could merely throttle the data throughput of the servers that support it, blurring the nexus between the articles critical of his administration that it contains (or, more charitably, articles inimical to his estimation of the "national defense and security"[116] and a charge of censorship .[117] This, I think, suggests something of the constitutionally vexing muddle between "defensive" and "offensive" executive power explicated by Keynes, where otherwise judicially actionable abuses of presidential war authority are cloaked as actions taken incidental to it.[118]

IV. EMERGING TECHNO-LEGAL CONSIDERATIONS

Thus far, my discussion of Section 706(a) has been centered on the past. Beyond this, however, there exist contemporary and emerging factors that enhance the potential for statutory abuse—as set forth in the introduction to this paper—from the possible to the likely, given a President impelled primarily by the prospect of partisan or personal gain.[119]

---

114. Read v. Central Union Tel. Co., 213 Ill. App. 246, 255 (Ill. App. Ct. 1919).

115. Again, I note the contrast between subsection (a) and the provision by subsections (c) and (d) for the wholesale seizure of wire or wireless systems by the federal government, which, as Brenner and Clarke, *supra* note 88, at 1060, observe of the cyber battlefield, would effectively render facility owners and operators civilian conscripts under the international law of armed conflict.

116. 47 U.S.C. § 606(a).

117. *Cf.* Holder v. Humanitarian Law Project, 561 U.S. 1, 7, 34-35 (2010) (delineating, per a First Amendment challenge to statutory measures proscribing "the provision of "material support or resources to certain foreign organizations that engage in terrorist activity, the grounds for judicial deference to prophylactic measures taken in connection with efforts to confront evolving threats in an area where information can be difficult to obtain and the impact of certain conduct difficult to assess . . . . The Government, when seeking to prevent imminent harms in the context of international affairs and national security, is not required to conclusively link all the pieces in the puzzle before we grant weight to its empirical conclusions").

118. *See* EDWARD KEYNES, UNDECLARED WAR: TWILIGHT ZONE OF CONSTITUTIONAL POWER 88-89 (1982).

119. *Cf.* Dell Cameron, *Secrecy Concerns Mount Over Spy Powers Targeting US Data Centers*, WIRED (May 14, 2024), https://www.wired.com/story/section-702-ecsp-civil-liberties-letter/ [https://perma.cc/67RV-HSFX] (detailing resistance to recent expansion of data center surveillance powers by the executive branch under Section 702 of FISA).

The first, and most important, is modern warfare's increasing use of the *information domain as a battlefield*, a development that portends, at best, a fractious understanding of the potential scope and impact of Section 706(a). As Aldrich observed nearly twenty-five years ago, cyberspace is "ethereal," where "weapons . . . bought in any computer store . . . innocuously manipulate bits of data" to wreak attenuated havoc on "telecommunications companies, power companies, financial centers, and the like."[120] This fluidity, he opined, has serious ontological implications with respect to "using established law of armed conflict constructs to assess military necessity, proportionality, collateral damage, and the like."[121] Little has changed in the quarter-century hence. As the 2017 version of the North American Treaty Organization's Cyber Defense Center of Excellence's Tallinn Manual drily observes, "[t]he application of the law of armed conflict to cyber operations can prove problematic," with such basic concepts as "[t]he existence of a cyber operation, its originator, its intended object of attack, or its precise effects" still the subjects of contestation amongst scholars.[122]

With the epistemology of war itself cast asunder[123]—a concerted nadir in the particular case of subsection (a), as per Part II.A of this paper—on what foundation can normative claims be staked? How might, for example, we classify the geopolitical aims in and legal justifications for slowing Facebook servers to prevent the spread of anti-Kashmiri misinformation by the Indian Army?[124] Does throttling communications critical to domestic protests (that oppose, say, acts of imperialism by the United States or one of its proxy states) amount to censorship or a valid response to suspected fifth columnists?[125] Is prioritizing the voices of Iranian dissidents across social media a valid adjunct to the country's ceaseless war on terror or an undue violation of national sovereignty?[126]

All these questions, of course, presuppose an understanding of the increasingly byzantine technical means and methods through which digital preference and prioritization will be effectuated. Data centers, like Amazon

120. Richard W. Aldrich, *How Do You Know You Are at War in the Information Age?*, 22 HOUS. J. INT'L L. 224-25 (2000).

121. *Id.* at 226.

122. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 377 (Michael N. Schmitt ed., 2017) (ebook).

123. *Cf.* David G. Delaney, *Cybersecurity and the Administrative National Security State: Framing the Issues for Federal Legislation*, 40 J. LEGIS. 251, 263-64 (2013-14) (arguing, per *Youngstown*, that "[t]he President's military powers are simply a starting point to consider steps that the cyber administrative national security state must take to understand and address security issues of the digital age").

124. *See* Joseph Menn & Gerry Shih, *Under India's Pressure, Facebook Let Propaganda and Hate Speech Thrive*, WASH. POST (Sept. 26, 2023), https://www.washingtonpost.com/world/2023/09/26/india-facebook-propaganda-hate-speech/ [https://perma.cc/BJY2-K6QE].

125. *Cf.* Jonathan Guyer, *The 2010s was a decade of protests. Why did so many revolutions fail?*, VOX (Oct. 1, 2023), https://www.vox.com/world-politics/23896050/protest-decade-2010-revolutionary-handbook-vincent-bevins-arab-spring-brazil-occupy-hong-kong [https://perma.cc/WQS6-ZKEJ].

126. *See, e.g.*, Ali & Fahmy, *supra* note 5, at 59.

Web Services, constitute the backbone of the modern Internet; central to worldwide connectivity and traffic exchange, they are vital national resources in (and vulnerable targets of) concerted transnational conflict.[127] Yet even in peacetime, the operations of these institutions, controlled by a handful of insular global corporations and operating well outside the regulatory gaze and popular ken, are difficult to understand.[128]

The second is Section 706's reference to *common carrier*. Defined by the Act as "any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or interstate or foreign radio transmission of energy,"[129] the term has traditionally applied to telephone companies.[130] In 2016, however, the FCC expanded its reach to encompass broadband Internet access service ("BIAS") providers in the interests of network transparency and openness.[131] While this regulatory initiative, known as net neutrality, was abandoned two years later in favor of a return to a "light-touch regulatory framework,"[132] agency leadership has embarked in 2023[133] on a successful campaign to resurrect it.[134] This, of course, places cable television, satellite, and digital subscriber line Internet access providers squarely within Section 706(a)'s crosshairs, enabling the President to engage in the very practices—blocking, throttling, and non-neutral data

127. *Cf. Connecting America: Oversight of the FCC: Hearing Before the Subcomm. on Energy & Com.*, 118th Cong. 2 (2023) (statement of Commissioner Geoffrey Starks) https://www.congress.gov/117/meeting/house/114545/witnesses/HHRG-117-IF16-Wstate-StarksG-20220331.pdf [https://perma.cc/SYC5-4HLU] (noting that "network security threats like foreign-owned data centers" demand a whole-of-government strategy "to protect U.S. communications stored within or that otherwise transit these data centers"); *Privacy and Data Protection Task Force*, FCC (2023), https://www.fcc.gov/privacy-and-data-protection-task-force [https://perma.cc/A9DU-DR57] (establishing a comprehensive "public-private approach" to tackling "problems that erode the public's trust in data protection" and imperil "the nation's communications supply chain").

128. *See, e.g.*, Molly Wood, *We Need to Talk About 'Cloud Neutrality'*, WIRED (Feb. 10, 2020), https://www.wired.com/story/we-need-to-talk-about-cloud-neutrality/ [https://perma.cc/9Z5Y-78SF].

129. 47 U.S.C. § 153(11).

130. *See, e.g.*, Mark A. Hall, *Common Carriers Under the Communications Act*, 48 U. CHI. L. REV. 409, 416-18, 420 (1981).

131. *See* Protecting and Promoting the Open Internet, *Report and Order on Remand, Declaratory Ruling, and Order*, 30 FCC Rcd 5601, ¶¶ 13-29 (2015) [hereinafter *Open Internet Order*].

132. *See Restoring Internet Freedom*, 33 FCC Rcd 312, ¶ 1 (2017); *cf.* Toronto, *supra* note 26, at 180-181.

133. *See Safeguarding and Securing the Open Internet*, 89 Fed. Reg. 45404, 45404 (May 22, 2024); *cf.* Eva Dou, *FCC's Net Neutrality Battle is Back After Years of Deadlock*, WASH. POST (Sept. 28, 2023), https://www.washingtonpost.com/technology/2023/09/28/fcc-net-neutrality/; Press Release, FCC, Chairwoman Rosenworcel Proposes to Restore Net Neutrality Rules (Sept. 26, 2023), https://docs.fcc.gov/public/attachments/DOC-397235A1.pdf [https://perma.cc/BHD2-CE2Z].

134. *See* Safeguarding and Securing the Open Internet; Restoring Internet Freedom, 89 Fed. Reg. 45404, 45404 (final proposed rule May 22, 2024) (to be codified at 47 C.F.R. pts. 8 and 20) (adopting "a *Declaratory Ruling, Report and Order, Order, and Order on Reconsideration* that reestablishes the FCC's authority over broadband internet access service" as of July 22, 2024).

prioritization—that net neutrality was designed to prevent.[135] Further complicating matters are claims that the FCC may *already* enjoy common carrier authority over platforms like social media sites and search engines by dint of 47 U.S.C. § 230, the controversial "good Samaritan" protection for content moderation.[136]

Finally, there stands the historical consolidation of dispersed federal authorities in a singular individual—the so-called *imperial presidency*, by "which enormous discretionary power to respond to national security crises and perceived dangers is concentrated in the office of the president."[137] In the wake of the attacks of September 11, 2001, government officials seized upon a national security crisis to propound new theories of executive authority in the realm of enhanced interrogation tactics,[138] warrantless electronic surveillance,[139] and targeted killings of United States nationals abroad.[140] As the Brennan Center's recent release of some 500 pages of "presidential emergency action documents" ("PEADs") from 2004 to 2008 demonstrates, Section 706 was not immune from the Bush Administration's efforts to amass

---

135. *See Open Internet Order*, *supra* note 130, at ¶ 4; *Preserving the Open Internet, Broadband Industry Practice, Notice of Proposed Rulemaking*, 25 FCC Rcd 17968, 17974-75 (2010); *cf.* Opderbeck, *supra* note 26, at 37 ("At most, [Section 706(a)] might authorize the President to change some of the requirements for Internet traffic . . . perhaps, for example, by requiring ISPs to *throttle* P2P applications suspected of use by a terrorist organization."). A final ironic twist is found in FCC Chairman Rosenworcel's summary of the advantages that will accrue to the country from reclassification, the vast majority of which concern enhancements to national security and public safety. *See* FCC Office of the Chairwoman, *FACT SHEET: National Security and Public Safety Impacts of Restoring Broadband Oversight* (Oct. 5, 2023), https://docs.fcc.gov/public/attachments/DOC-397494A1.pdf [https://perma.cc/28NV-MSME]; *cf.* Robbie Troiano, *Assessing the Current State of Net Neutrality and Exploring Solutions in Creating and Maintaining Open, Available, and Innovative Internet and Broadband Services*, 14 J. BUS. & TECH. L. 553 (2019) (explicating the contested "common carrier" classification as central to FCC efforts to prohibit purported traffic management abuses on the part of Internet service providers).

136. *See, e.g.*, Joel Thayer, *The FCC's Legal Authority to Regulate Platforms as Common Carriers*, FED. SOC. BLOG (Mar. 29, 2021) https://fedsoc.org/commentary/fedsoc-blog/the-legal-authority-for-the-fcc-to-regulate-platforms-as-a-common-carrier [https://perma.cc/Q958-ND3L] ("Because Section 230 sits in Title II, all services covered under the statute are subject to the Title's rulemaking authority under Section 201(b) . . . Traditionally, Section 201(b) applies to rules related to common carriers.").

137. Paul Starobin, *Imperial Presidency Has Long History*, GOVERNMENT EXECUTIVE (Feb. 22, 2006), https://www.govexec.com/federal-news/2006/02/imperial-presidency-has-long-history/21214/ [https://perma.cc/M9R8-XRF8].

138. *See, e.g.*, Memorandum from Jay S. Bybee, Assistant Att'y Gen., to Alberto R. Gonzales, Counsel to the President (Aug. 1, 2002), (available at https://www.justice.gov/media/852816/dl?inline).

139. *See, e.g.*, Letter from John C. Yoo, Deputy Assistant Att'y Gen., Office of Legal Counsel, to U.S. District Judge Colleen Kollar-Kotelly (May 17, 2002) (available at https://www.justice.gov/media/879011/dl?inline).

140. *See, e.g.*, Memorandum from David J. Barron, Acting Assistant Att'y Gen., Office of Legal Counsel, to the Att'y Gen. Re: Applicability of Federal Criminal Laws and the Constitution to Contemplated Lethal Operations Against Shaykh Anwar al-Aulaqi (July 16, 2010) (available at https://www.justice.gov/sites/default/files/olc/pages/attachments/2015/04/02/2010-07-16_-_olc_aaga_barron_-_al-aulaqi.pdf [https://perma.cc/7W4Q-9PKT]).

"powers that appear to lack oversight from Congress, the courts, or the public."[141] While the text of the relevant PEADs is largely accurate,[142] handwritten comments from NSC staffers suggest that subsection (a) might "app[ly] toward interstate carriers beyond lang[uage] of statute, inc[luding] by FCC" and "to noncommon carriers—this is beyond statutory lang[uage]."[143] Further reflections on the scope of Section 706(a) question whether a "[p]roclamation [is] still necessary under National Emergencies Act,"[144] a Watergate-era legislative check on the President's use of extraordinary powers in a crisis.[145] There seems little doubt that these troubling initiatives will increase, particularly as lawmakers debate the merits of a "defend forward" strategy for information warfare, by which the United States military would embrace "an operational tempo of continuous—or persistent—engagement with adversaries in the cyber domain."[146]

V. A PATH FORWARD

Taking the preceding sections together, the inherent ambiguity and potential applications of Section 706(a) demand reparative action. Such a fix should be both immediate and comprehensive, particularly as social media

141. Benjamin Waldman, *New Documents Illuminate the President's Secret, Unchecked Emergency Powers*, BRENNAN CTR. FOR JUST. (May 26, 2002), https://www.brennancenter.org/our-work/analysis-opinion/new-documents-illuminate-presidents-secret-unchecked-emergency-powers [https://perma.cc/2FV5-E9U2].

142. *See generally* Himamauli Das (2004), OSTP NS/EP Wartime Authorities Under 47 U.S.C. Section 706 and E.O. 12472(a)(2) NSC Provides Policy Direction; Himamauli Das (2004), Questions for Section 706 PEAD Review. National Security Advisor – Legal Advisor (noting, for example that the relevant "state of emergency" and "triggers" for use of Section 706(a) are the "continuance of a war" and a "necess[ity] for the national defense and security," respectively); Himamauli Das (2004), Communications Act Section 706 47 USC § 606. Declassified and released by the George W. Bush Presidential Library under the Freedom of Information Act (FOIA) to the Brennan Cent. for Just, FOIA Request No. 2015-0067-F 1, 3-4 (2015), https://www.brennancenter.org/sites/default/files/2022-05/t030-014-006-peads-20150067f_0.pdf#page= [https://perma.cc/UTT6-Q3PZ] [hereinafter 2015 FOIA Request].

143. 2015 FOIA Request at 1.

144. *Id.* at 3.

145. *See* 50 U.S.C. §§ 1601; *cf.* Note, *The International Emergency Economic Powers Act: A Congressional Attempt to Control Presidential Emergency Power*, 96 HARV. L. REV. 1102, 1102-1103 (1983) ("The problem posed by the need to permit but still to limit emergency power . . . has been a troublesome issue for the theory and practice of liberal government. On the one hand, United States constitutional law has long recognized that crises provide occasions for the exercise of extraordinary national powers and that, especially in the context of foreign affairs, the Executive is peculiarly well suited to invoke such power.").

146. Robert Chesney, *The Domestic Legal Framework for US Military Cyber Operations*, HOOVER INST. (2020), https://www.hoover.org/sites/default/files/chesney_webreadypdf.pdf [https://perma.cc/8N2Y-TWLT].

platforms themselves may fall within the ambit of the statute in the near future.[147]

A statutory prophylactic ought to be constructed, I believe, that addresses the statute's manifold weaknesses. Such a fix should be narrowly drawn; as Weitzman notes of rehabilitating the National Emergencies Act: "[c]ertain congressional attempts to limit or constrain inherent presidential crisis authorities through legislation might even be regarded as unconstitutional interferences with the President's authority to exercise a power committed to her and her alone."[148] Yet it should also be comprehensive enough to redress the statute's systemic shortcomings—namely, the vagueness of its reference to "war," the unclear mechanism for judicial review of executive action taken pursuant to it, and, most crucially, its apparent failure to recognize First Amendment liberties as a counterbalance to Article II authorities.

As a preliminary matter, it must be noted that Section 706 does contain an organic check on the exercise of powers delineated thereunder. Subsection (g), "Limitations upon Presidential Power," reads:

> Nothing in subsection (c) or (d) shall be construed to authorize the President to make any amendment to the rules and regulations of the [FCC] which the [FCC] would not be authorized by law to make; and nothing in subsection (d) shall be construed to authorize the President to take any action the force and effect of which shall continue beyond the date after which taking of such action would not have been authorized.[149]

Clearly, the first clause of the foregoing could be amended to incorporate a specific reference to subsection (a), thereby circumscribing presidential authority within the bounds set forth by Congress under the Act.

Yet while this constitutes an important step, I believe it does not end the inquiry. Since 1967, the FCC has maintained a NS/EP restoration priority program for telecommunications carriers, by which civilian traffic may be degraded in the interest of wartime exigency.[150] "As originally drafted, the rules were intended as a regulatory carveout to allow common carriers to

147. *See* Moody v. NetChoice, LLC, 144 S. Ct. 2383 (2024) (remanding First Amendment challenges by interactive service providers to Texas and Florida content moderation laws for, *inter alia*, assessment of whether providers are properly classed as common carriers); *see also, e.g.*, Removing Section 230 Immunity for Official Accounts of Censoring Foreign Adversaries Act, S. 941, 118th Cong. (2024); Legislative Proposal to Sunset Section 230 of the Communications Decency Act, 170th Cong. 543 (2024).

148. Samuel Weitzman, *Back to Good: Restoring the National Emergencies Act*, 54 COLUM. J.L. & SOC. PROBS. 365, 371 (2021).

149. 47 U.S.C. § 606(g).

150. *See* Rules and Requirements, *supra* note 33, at ¶¶ 4-9 (explaining the purpose and operation of the Telecommunications Service Priority, Wireless Priority, and Government Emergency Telecommunications Services); Nat'l Sec. Emergency Preparedness Telecomm. Serv. Priority Sys., *Report and Order*, 3 FCC Rcd 6650, para. 2 (1988) (summarizing historical development of these provisions).

provide telecommunications services, which would ordinarily be subject to the non-discrimination requirements of Section 202(a), on a prioritized basis."[151] Far from constituting an action "which the [FCC] would not be authorized by law to make,"[152] Presidential prioritization fits comfortably within these provisions, facially evading the Act's prohibition on affording "any undue or unreasonable preference or advantage to any particular person, class of persons, or locality"[153] under cloak of national security.

To this end, I look to other portions of the United States Code for solutions to the structural problems outlined above. In culling a workable definition of "war," the War Powers Resolution[154] is an ideal source, given that it both promulgates "a congressional definition of the word 'war' in article I"[155] and "provides a logical, constitutional allocation of war powers" in distinguishing between "a declaration of war" and a "specific statutory authorization" [156] for employment of the armed forces.[157] More specifically, the statute imposes specific reporting requirements upon the President "[i]n the absence of a declaration of war," which accords with the notion that "specific statutory authorization for military action, while based on Congress's power to authorize military action, must be viewed as being subsidiary to a formal declaration of war and cannot constitute a wartime state of affairs."[158] Applied to the question at hand, this discursive construction both elides the heretofore tangled (and tautological) attempts to define subsection (a)'s reference to "continuance of war" and elucidates the manner by which limitations upon presidential traffic prioritization should be imposed—i.e., in all cases short of a declaration of war under color of Article I, Section 8.[159]

As to the First Amendment, Title 47 itself instructs the FCC to "proceed cautiously and with appropriate restraint" in proposing forfeitures for or predicating license renewals upon broadcasts of indecent or profane

151. Rules and Requirements, *supra* note 33, at ¶ 26.

152. The Communications Act of 1934, 47 U.S.C. § 606(g).

153. *Id.* § 202(a); *cf. Open Internet Order*, *supra* note 130, at ¶¶ 441-52 (predicating bans on the throttling and paid prioritization of BIAS traffic upon, *inter alia*, Section 202 of the Act).

154. 50 U.S.C. §§ 1541-1548.

155. Stephen L. Carter, *The Constitutionality of the War Powers Resolution*, 70 VA. L. REV. 101, 101-02 (1984).

156. 50 U.S.C. § 1541(c).

157. Christopher J. Schmidt, *Could a CIA or FBI Agent Be Quartered in Your House during a War on Terrorism, Iraq or North Korea?*, 48 ST. LOUIS L.J. 587, 618 (2004).

158. *Id.* at 618-19.

159. This is also commensurate with the vast weight of caselaw discussed in Part III, *supra*, which recognized executive primacy in dictating the scope and duration of traffic prioritization within the context of a declared war (i.e., World Wars I and II).

material,[160] notwithstanding the criminalization of such acts.[161] Section 326 of the Act specifically disclaims the FCC's "power of censorship over the radio communications or signals transmitted by any radio station" and prohibits it from imposing any "regulation or condition" that will "interfere with the right of free speech by means of radio communication."[162] While not directly applicable to the instant inquiry by dint of its reference to "radio communications",[163] this language appears eminently adaptable to ensuring the primacy of constitutional considerations when prioritizing telecommunications traffic.[164]

Finally, as Mortenson notes of the nebulous reach of presidential ambition in times of exigency, "executive branch interpretation often proceeds either out of sight or without a clear path to judicial review."[165] Here, I consider a statutory revision that would afford a predictable, accessible, and robust mechanism[166] for carriers putatively affected by action taken pursuant to Section 706(a) to obtain court intervention at the earliest possible date, taking into account the extraordinary circumstances surrounding the executive's invocation of emergency. Here, an explicit right to appeal to the United States Court of Appeals for the District of Columbia seems appropriate; reflecting review mechanisms presently in place under Section 402(b) of the Act for aggrieved carriers, this accords with extant Section 706(g)'s use of FCC orders as a conceptual framing for executive action.

---

160. WDBJ TV, Inc., *Notice of Apparent Liability for Forfeiture*, 30 FCC Rcd 3024, ¶ 11 (2015); Good Karma Broad., LLC, *Forfeiture Order*, 27 FCC Rcd 10938, ¶ 15 n.61 (2012); Application of Texas Educ. Broad. Coop., Inc. for Renewal of License for Station KOOP(FM), Hornsby, Tex., *Memorandum Opinion and Order and Notice of Apparent Liability for Forfeiture*, 22 FCC Rcd 13038, ¶ 17 (2007).

161. *See* 18 U.S.C. § 1464 ("Whoever utters any obscene, indecent, or profane language by means of radio communication shall be fined under this title or imprisoned not more than two years, or both.").

162. 47 U.S.C. § 326.

163. *See, e.g.*, Review of Foreign Ownership Policies for Broad., Common Carrier and Aeronautical Radio Licensees under Section 310(b)(4) of the Commc'ns Act of 1934, as Amended, *Notice of Proposed Rulemaking*, 30 FCC Rcd 11830, ¶ 14 (2015) (recognizing "the distinct nature of the services provided by common carriers and broadcast stations" in the context of foreign ownership attribution).

164. As the FCC itself observed in 1974, the existence of Section 326 of the Act means the expansive traffic management powers afforded the FCC (which, as discussed above, circumvent the non-delegation doctrine by dint of the "public interest, convenience, and necessity" standard) "must be reconciled with free speech considerations." Petition of Action For Children's TV (ACT) for Rulemaking Looking Toward the Elimination of Sponsorship and Commercial Content in Children's Programing and the Establishment of a Weekly 14-Hour Quota of Children's TV Programs, *Children's Television Report and Policy Statement*, 50 F.C.C. 2d. 1, 3 (1974).

165. Julian Davis Mortenson, *Article II Vests the Executive Power, Not the Royal Prerogative*, 119 COLUM. L. REV. 1169, 1173 (2019).

166. Or, more fulsomely, judicial review that will "(1) maximize participation by the three branches of government; (2) provide clear and predictable rules; (3) identify substantive norms to guide governmental action or judicial review or both; and (4) allocate the burden of legislative inaction on the party best positioned to overcome it." Mario L. Barnes & F. Greg Bowman, *Entering Unprecedented Terrain: Charting a Method To Reduce Madness in Post-9/11 Power and Rights Conflicts*, 62 U. MIAMI L. REV. 365, 412 (2008).

A revised subsection (g), incorporating the considerations set forth above, would thus read:

> *Nothing in subsection (a), (c) or (d) shall be construed to authorize the President to make any amendment to the rules and regulations of the FCC which the FCC would not be authorized by law to make; and nothing in subsection (d) shall be construed to authorize the President to take any action the force and effect of which shall continue beyond the date after which taking of such action would not have been authorized. If in the absence of a declaration of war, as such term is understood under section 1541 of title 50, United States Code, the President, whether directly, or through such person or persons as he designates for the purpose, or through the FCC, gives directions that such communications as in his judgment may be essential to the national defense and security shall have preference or priority with any carrier subject to this chapter:*
> *(1) nothing in subsection (a) shall be construed to authorize the President, whether directly, or through such person or persons as he designates for the purpose, or through the FCC, to censor the communications of any carrier subject to this chapter or otherwise interfere with the right of free speech by means of telecommunications; and*
> *(2) such directions shall be treated as an order of the FCC for purposes of appeal under section 402(b) of this title by any person who is aggrieved or whose interests are adversely affected by their issuance.*

VI. CONCLUSION

Thirteen years ago, the Senate Committee on Homeland Security and Governmental Affairs concluded that while "Section 706 gives the President the authority to take over wire communications in the United States and, if the President so chooses, shut a network down . . . it is not clear that the President could order a lesser action."[167] This paper has presented a case to the contrary, per factors intrinsic to the construction of subsection (a) and emerging techno-legal concerns. It has also provided a means of remediation, in the form of a specific statutory fix that should be implemented as rapidly as possible. As an augment to existing scholarship on the potentially pernicious applications of Section 706(c) and (d)—and a reflection upon the seeming inadequacy of existing legal frameworks to constrain excesses of executive authority over wired and wireless modalities—this paper thus

167. S. REP. No. 111-368, at 10 (2010).

stands as a further bulwark against presidential assumption of "plenary authority" over national communications in exigent times.[168]

168. Patrick A. Thronson, *Toward Comprehensive Reform of America's Emergency Law Regime*, 46 U. MICH. J.L. REFORM 737, 754 n.124 (2013) (postulating that the Obama Administration reached such a conclusion in deeming Section 706 sufficient "to unilaterally seize control of radio and television stations, phone systems, and the Internet").

Reviewing for the Public Interest: Affirming Access to Anti-SLAPP Protection for Consumer Reviews

Nicholas Sorice*

TABLE OF CONTENTS

I. INTRODUCTION 158
II. SLAPPS AND ANTI-SLAPP LEGISLATION 160
III. ANTI-SLAPP LEGISLATION AND CONSUMER REVIEWS 165
A. General Public Interest Anti-SLAPP 166
B. Review-Friendly Anti-SLAPP 170
IV. RULE ON THE USE OF CONSUMER REVIEWS AND TESTIMONIALS AS JUSTIFICATION FOR EXPANDED ANTI-SLAPP SCOPES 170
A. In Narrow and Review Friendly Jurisdictions 171
B. In General Public Interest Jurisdictions 171
V. CONCLUSION 174

* J.D., May 2025, The George Washington University Law School. B.S., 2019, International Relations and Diplomacy, Mercy University. I would like to thank the FCLJ Editorial Board for their invaluable guidance, Caitlin Brosseau for introducing me to this topic, Hannah Ward for listening to me drone on about this for almost two years, and my family for their constant love and support.

I. INTRODUCTION

You have just had the worst meal of your life. The soup was cold and under-seasoned, your medium-rare steak came out looking like a charcoal briquette, and you are fairly certain you saw a cockroach scurry into the kitchen. Naturally, you decide to leave a review online to warn future diners. Time passes and you have forgotten about the experience, when suddenly a process server shows up at your door, informing you that the restaurant is taking you to court for defamation.

This scenario is, unfortunately, commonplace.[1] For most individuals, the time, cost, and emotional energy necessary to fight this legal battle just isn't worth it, and they choose to take down their review. These suits, motivated by a desire to silence critics, have been named "strategic lawsuits against public participation" or "SLAPPs."[2] Thirty-three states and the District of Columbia have enacted "anti-SLAPP laws"[3] to combat this abusive use of litigation by allowing a SLAPP target to quickly and affordably resolve a meritless claim. However, even in states that have robust anti-SLAPP protections, it is not always clear that consumer reviews are protected by their ambit.[4]

As this Note further explores below, anti-SLAPP statutes can be divided into several categories, as defined by the scope of the speech they protect. Statutes like California's are usually thought to fall under the broadest category of anti-SLAPP protection because their scope covers "any written or oral statement or writing made in a place open to the public or a public forum in connection with an issue of public interest."[5] The key inquiry for consumer reviews under this type of statute is whether the review constitutes speech made in a public forum on an issue of public interest. Some states have resolved this ambiguity by explicitly including consumer reviews in their anti-

1. *See* YELP, 2022 TRUST & SAFETY REPORT 16 (Feb. 1, 2023), https://issuu.com/yelp10/docs/2022_yelp_trust_safety_report?fr=sZmZkYzU3NDM2NzY [https://perma.cc/Z7Q2-MLYK] (labeling 48 businesses with "Questionable Legal Threat Alerts," meaning Yelp was aware of that business' history of using legal threats to suppress negative reviews); The Transparency Company, Comment Letter on Proposed Trade Regulation Rule on the Use of Reviews and Endorsements, 1, 15 (Jan. 9, 2023), https://regulations.gov/comment/FTC-2022-0070-0044 [https://perma.cc/Y3CK-BMGJ] (estimating thousands of lawyers are hired each year to use legal threats to suppress negative reviews).

2. *See* UNIF. PUB. EXPRESSION PROT. ACT prefatory note (UNIF. L. COMM'N 2020).

3. *See* Dan Greenberg et al., *Anti-SLAPP Statutes: 2023 Report Card*, INST. FOR FREE SPEECH (Nov. 2, 2023), https://www.ifs.org/anti-slapp-report/ [https://perma.cc/8VRZ-WFSW]. A map is available providing more information about each state's anti-SLAPP law and a grade based on the IFS' criteria for anti-SLAPP laws. *Id.*

4. *See* Eric Goldman, *CA Anti-SLAPP Cases Involving Consumer Reviews as Matters of Public Concern*, TECH. & MKTG. L. BLOG (Feb. 3, 2011), https://blog.ericgoldman.org/archives/2011/02/ca_antislapp_ca.htm [https://perma.cc/TH29-F5JX] (reviewing California application of anti-SLAPP laws for consumer reviews).

5. CAL. CIV. PROC. CODE § 425.16(e)(3) (Deering 2023); *see* Greenberg, Keating & Knowles-Gardner, *supra* note 3 (California receiving a grade A+ score for its anti-SLAPP statute).

SLAPP laws.[6] The issue lies in those states that have not made the line explicit in their statutes. This ambiguity could be resolved with the promulgation of the Federal Trade Commission's Trade Regulation Rule on the Use of Consumer Reviews and Testimonials.[7] By calling SLAPPs on consumer reviews an unfair or deceptive act, the rule would affirm these reviews as a vital part of the modern economy,[8] and, as a secondary effect, expand access to anti-SLAPP protection in these public interest states.

The regulation's section 465.7(a) makes it an unfair or deceptive act or practice "for anyone to use an unjustified legal threat or a physical threat, intimidation, or false accusation in an attempt to prevent a consumer review or any portion thereof from being written or created or cause a consumer review or any portion thereof to be removed."[9] There is no federal anti-SLAPP law, and this regulation does not substitute the need for one.[10] As discussed below, anti-SLAPP laws provide substantive legal benefits, in a procedural form, that allow a SLAPP target to quickly and affordably resolve the meritless claim.[11] Section 465.7(a) may not provide such direct benefits. This regulation expands the FTC's enforcement capacity, allowing it to "seek civil penalties against violators and obtain redress for consumers or others injured by the conduct."[12] While this is likely to deter some amount of

6. WASH. REV. CODE § 4.105.010(3)(b)(ii) (2023) (excluding commercial speech from anti-SLAPP protection, but explicitly includes consumer reviews); OKLA. STAT. tit. 12, § 1431(7)(e) (2023) (defining "matters of public concern" in part to be those issues related to "a good, product or service in the marketplace").

7. Trade Regulation Rule on the Use of Consumer Reviews and Testimonials, 16 C.F.R. § 465.7(a) (2024).

8. *See The Reviews Are In: Yelp Users are Four-Star Consumers*, NIELSEN (Jun. 2013), https://www.nielsen.com/insights/2013/the-reviews-are-in-yelp-users-are-four-star-consumers/ [https://perma.cc/58WT-HP9Y]. In 2013, 85% of consumers found local business information online, 51% of Yelp users made their purchasing decisions after visiting the site, and 93% of the time Yelp usage resulted in "occasionally, frequently or always making a purchase from a local business. *Id.*; *Consumer Trust in Online, Social, and Mobile Advertising Grows*, NIELSEN (Apr. 2012), https://www.nielsen.com/insights/2012/consumer-trust-in-online-social-and-mobile-advertising-grows/ [https://perma.cc/53SQ-ZQXR]. In 2012, Nielsen found that 70% of global consumers trusted online reviews as their source of brand information, making it the second most trusted source behind recommendations from friends and family). *Id.*

9. 16 C.F.R. § 465.7(a).

10. *See generally* Julio Sharp-Wasserman & Evan Mascagni, *A Federal Anti-SLAPP Law Would Make Section 230(c)(1) of the Communications Decency Act More Effective*, 17 FIRST AMEND. L. REV. 367, 370 (2019) (arguing that a federal anti-SLAPP law would close current loopholes that allow for forum-shopping, abuse of favorable choice of law principles, and a circuit split over the applicability of anti-SLAPP provisions in diversity cases); Nicole J. Ligon, *Solving SLAPP Slop*, 57 U. RICH. L. REV. 459, 480–81 (2023) (arguing that a federal anti-SLAPP law is necessary to reduce forum shopping and create consistent levels of protection for SLAPP targets).

11. *See* Roni A. Elias, *Applying Anti-SLAPP Laws in Diversity Cases: How to Protect the Substantive Public Interest in State Procedural Rules*, 41 T. MARSHALL L. REV. 215, 216, 237 (2016) (arguing that the current Circuit Split over the applicability of state anti-SLAPP laws in federal court on diversity action can be resolved by understanding the laws to use a procedural mechanism to vindicate a substantive right).

12. Trade Regulation Rule on the Use of Consumer Reviews and Testimonials, 88 Fed. Reg. at 49378.

SLAPP-ing from happening in the first place, it does little to help an individual whose SLAPP instigator was not dissuaded by potential FTC action.

This note proceeds in three sections. Section I provides a brief history of the SLAPP and anti-SLAPP statutes, which scholars have traditionally taxonomized as narrow petitioning statutes, moderate/indirect petitioning statutes, and broad public interest statutes based on the kinds of speech protected in different jurisdictions. While this taxonomy is useful in understanding the historical limits of anti-SLAPP protection, this Note proposes a new taxonomy which centers consumer reviews and highlights how the FTC's rule would impact these statutes' applications by dividing the statutes into narrow, general public interest, and review-friendly. This new taxonomy allows, in Section II, for an examination of how anti-SLAPP laws are understood in the age of the Internet review. Finally, Section III examines how the FTC's rule can expand access to anti-SLAPP protections in general public interest jurisdictions, with particular emphasis on the established tests for "issues of public interest."

II. SLAPPS AND ANTI-SLAPP LEGISLATION

The term SLAPP was coined by Professors Penelope Canan and George W. Pring in their seminal 1988 work *Strategic Lawsuits Against Public Participation*, which conceptualized SLAPPs as suits brought to retaliate against one party's exercise of the right to petition to the detriment of the other.[13] They further identified that there was usually a likely power or economic disparity between the filer and target favoring the filer, or else a battle between a public interest group and industrial interests.[14] They also described the way in which SLAPP filers would "recast the offending political behavior as common torts, and thereby mask the original nature of the dispute."[15] Finally, they identified that SLAPP filers almost always lost the

13. *See* Penelope Canan & George W. Pring, *Strategic Lawsuits Against Public Participation*, 35 SOC. PROBS. 506, 508-10 (Dec. 1988) (identifying four settings for the emergence of a SLAPP: 1) "One party approached some government body or office about a matter that affected some other party"; 2) "two parties concurrently petitioned the same government body, seeking different (usually opposite) exercises of government power"; 3) "more complicated arrangements" that resulted from different parties petitioning different government bodies; and 4) boycotts).

14. *Id.* at 510-11 ("[I]ndividual and organizational lead filers had economic, occupational, or industrial interests at stake. On the other hand, first named targets were often citizens, public interest groups, or civic and social organizations."). While they acknowledge that legal documents alone are not enough to get a full picture of the relative status of litigants, in "small scale" conflicts they use a landlord/tenant conflict and the dispute between a neighbor who wanted to build a tennis court on wetlands and the neighbor who opposed him as typifying examples. *Id.* at 510. They also identify instances where there are clear power imbalances (between corporations and individuals), and even in disputes between "large organizations with plenty of resources" it was States against public interest groups, and industry groups against environmentalist organizations. *Id.* at 511.

15. *Id.*

case on a motion to dismiss or by final disposition.[16] As the Court of Common Pleas of Pennsylvania explained, SLAPP filers engage in these suits "as a means of intimidation and harassment, not because [they] believe in the success of their claims."[17] Thus, the four essential characteristics of SLAPPs are: (1) retaliation against the exercise of a First Amendment right; (2) a power disparity between the filer and target; (3) the filer's recasting of its motivation from silencing a critic into a cognizable legal claim; and (4) the filer's lack of any real desire to be vindicated in a court of law. Or, as a California Appeals Court phrased it, "while SLAPP suits masquerade as ordinary lawsuits the conceptual features which reveal them as SLAPPs are that they are generally meritless suits brought by large private interests to deter common citizens from exercising their political or legal rights or to punish them for doing so."[18]

To aid SLAPP targets and deter SLAPP filers, states began to enact anti-SLAPP statutes.[19] While states' anti-SLAPP laws vary, the Uniform Law Commission has provided a Uniform Public Expression Protection Act ("UPEPA") which serves as a blueprint for an ideal anti-SLAPP law. [20] UPEPA represents an idealized form of anti-SLAPP law, and so it is used here to explain the basic mechanics of this statutory protection, while noting where particular statutes diverge from the model. Anti-SLAPP laws typically provide a SLAPP target access to a special motion to strike.[21] Once the special motion is filed, the proceedings are stayed until the motion is resolved.[22] The motion is heard on an expedited basis.[23] The movant (the SLAPP target) must

16. *See id.* at 514 (finding SLAPP defendants won dismissals in 68% of cases, and 83% of final judgments—significantly, those final judgments took, on average, 32 months to reach).

17. *See* O'Neill v. Rossum, No. 2017-03836-MJ, 2017 WL 4973220, *6 (Pa. Ct. Com. Pl. Oct. 23, 2017) (trial order). Here, a real estate developer brought suit for defamation, tortious interference with contract, and civil conspiracy against a group of local environmentalists who protested in local government hearings, press conferences, and by disseminating fliers. *Id.* Defendants succeeded in getting dismissal based on the *Noerr Pennington* Doctrine and Pennsylvania's narrow anti-SLAPP law, but still faced another several years of appeals before the case was finally concluded. *Id.*

18. Wilcox v. Super. Ct., 27 Cal. App. 4th 809, 816 (2d Dist. Ct. App. 1994) (overruled in part on other grounds).

19. *See* UNIF. PUB. EXPRESSION PROT. ACT prefatory note (explaining the history of anti-SLAPP laws).

20. *See generally*, UNIF. PUB. EXPRESSION PROT. ACT (UNIF. L. COMM'N 2020). As of January 2024, UPEPA has been adopted by six states and has been introduced in an additional seven. Uniform Law Commission, *Public Expression Protection Act*, ULC, https://www.uniformlaws.org/committees/community-home?CommunityKey=4f486460-199c-49d7-9fac-05570be1e7b1 [https://perma.cc/Y5AL-FA4N] (last visited Jan. 19, 2024).

21. UNIF. PUB. EXPRESSION PROT. ACT § 3 (UNIF. L. COMM'N 2020).

22. *Id.* § 4. Not all anti-SLAPP laws feature the stay. *See, e.g.*, N.M. STAT. ANN. § 38-2-9.1 (West 1978) (New Mexico anti-SLAPP law calls for expedited hearing but provides for no stay of proceedings).

23. UNIF. PUB. EXPRESSION PROT. ACT § 5 (UNIF. L. COMM'N 2020). The hearing must be within 60 days of the motion in UPEPA, but the length varies across jurisdictions, with some statutes not having any specific time listed. *See* CAL.CIV. PROC. § 425.16(f) (Deering 2023) (California's law requires the hearing be within 30 days of the motion, "unless docket conditions of the court require a later hearing"); N.M. STAT. ANN. § 38-1-9.1(A) (West 1978) (New Mexico's law calls for the motion to be heard "on a priority or expedited basis," but does not include a specific timeframe).

show that this cause of action "arose from" their speech, and that their speech falls within the scope of the anti-SLAPP law's protection.[24] If this burden is met, it then shifts to the non-moving party to show that either the original speech is excepted from the scope of the law, or they have established a prima facie case for each essential element of their claim.[25] If the SLAPP filer is successful in the latter option, the burden shifts back to the movant to show that the SLAPP filer's cause of action fails to state a claim or that there is no genuine issue of material fact.[26] In addition to the expedited time to hearing, there is a time limit set on how long the judge can take before issuing a ruling on the motion.[27] UPEPA, and other anti-SLAPP statutes, includes a right to an immediate interlocutory appeal for a movant who has been denied.[28] Finally, upon a granted motion, the movant is entitled to costs and attorney's fees, or the responding party may receive the same if the court finds the anti-SLAPP motion was frivolous.[29]

Access to this mechanism provides SLAPP targets with valuable protection. The honest reviewer from the hypothetical at the start of this Note is much less likely to kowtow to the restaurant if they know they have access to this protection. The stay of proceedings limits the emotional and financial burden of going through discovery, and the expedited time to hearing and

24. UNIF. PUB. EXPRESSION PROT. ACT §§ 2(b), 7(a)(1) (UNIF. L. COMM'N 2020). Additionally, this is where the FTC's Proposed Rule on Consumer Reviews and Testimonials would be applied. The SLAPP target should be able to show, in public interest jurisdictions, that if the FTC considers this type of suit an unfair or deceptive trade practice, that the speech itself is on a matter of public interest, and therefore within scope of the statute.

25. *Id.* §§ 2(c), 7(a)(2)-(3)(A). Section 2(c) provides for exceptions to protected speech, and Section 7(a)(2) allows the SLAPP filer to show that this speech fall under that exception, while Section 7(a)(3)(A) allows the filer to show that the cause of action is not, in fact, meritless, as they have made out a prima facie case for each essential element of their claim. *Id.*

26. *Id.* § 7(a)(3)(B). The burden shifting framework differs by jurisdiction, with some jurisdictions not even including a burden shift at all. *Compare id.*, *with* MO. REV. STAT. § 537.528 (2023) (Missouri's statute requires the movant to show that the speech is in scope and that they prevail on the merits).

27. UNIF. PUB. EXPRESSION PROT. ACT § 8. UPEPA recommends 60 days, but this also varies. *Compare id.*, *with* Cal. CIV. PROC. § 425.16(f) (Deering 2023) (making no mention on time to ruling), *and* NEV. REV. STAT. § 41.660(3)(f) (2024) (requiring ruling on the motion "within 20 judicial days" of the motion being served).

28. UNIF. PUB. EXPRESSION PROT. ACT § 9. Not all statutes include this right, and some allow either party the right. *Compare id.*, *with* MO. REV. STAT. § 537.528(3) (2023) (Missouri allows either party the right to an interlocutory appeal), *and* VA. CODE ANN. § 8.01-223.2 (2023) (no interlocutory appeal in Virginia).

29. UNIF. PUB. EXPRESSION PROT. ACT § 10. UPEPA provides for mandatory award of fees and costs to a prevailing movant, and mandatory award to the respondent if the court finds the anti-SLAPP motion was frivolous or only intended to delay proceedings. *Id.* In practice, states differ on whether the award is mandatory and whether the respondent is entitled to costs and fees on a defeated motion. *See* VA. CODE ANN. § 8.01-223.2(C) (2023) (allowing that Virginia courts "may" award fees and costs to a party that successfully invokes anti-SLAPP immunity. There is no mention of fee-shifting for the benefit of the SLAPP filer); MASS. GEN. LAWS ch. 231, § 59H (2023) (providing for mandatory award of fees to the successful movant, but no sanctions for a frivolous invocation of the mechanism).

disposition reduces the time burden. Most critically, if the reviewer prevails on their motion, all financial costs are borne by the SLAPP filer.[30]

At this point, it is important to make two related observations: the potential constitutional issues with anti-SLAPP statutes, and the distinction between Canan and Pring's initial conception of the SLAPP and its application to consumer reviews.

The nature of anti-SLAPP laws creates tension between the target's First Amendment rights and the filer's right to redress.[31] Unlike a motion for summary judgment, which requires the judge to determine whether there exists a genuine issue of material fact, or a motion to dismiss for failure to state a claim, which only requires that the plaintiff plausibly *state* a claim, the anti-SLAPP motion creates a heightened burden wherein the plaintiff needs to show they have a probability of *prevailing* on their claim.[32] The highest courts in Washington, Minnesota, and New Hampshire found existing or proposed anti-SLAPP statutes[33] unconstitutional.[34] The District of Columbia Court of Appeals found the plain language of the District's anti-SLAPP statute would lead to a similar conclusion, but applied the canon of constitutional avoidance to supplant the pleading standard with the summary judgment standard.[35] One way these concerns might be ameliorated is through statutes that cover a narrow band of speech activity that gets to the core

30. *See* UNIF. PUB. EXPRESSION PROT. ACT § 10 cmt. 1 (UNIF. L. COMM'N 2020) (arguing without the mandatory award of fees, the SLAPP target still bears the financial costs, and "the effect of the abusive cause of action is nevertheless achieved").

31. *See* Nick Phillips & Ryan Pumpian, *A Constitutional Counterpunch to Georgia's Anti-SLAPP Statute*, 69 MERCER L. REV. 407, 408 (2018) (arguing that while anti-SLAPP laws are "well intentioned," they overweigh the target's First Amendment rights at the expense of the filers "right to a jury, due process, equal protection, and ironically, the right to petition").

32. *Compare* FED. R. CIV. P. 56(a) (summary judgment standard), *with* FED. R. CIV. P. 12(b)(6) (motion to dismiss for failure to state a claim); Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (explaining plausibility standard for a 12(b)(6) motion); *and* CIV. PROC. § 425.16(b)(3) (court must determine if the plaintiff has a probability that they will prevail on their claim).

33. Washington has since repealed that law and passed a new anti-SLAPP law. *See* WASH. REV. CODE § 4.24.525 (2020) (repealed 2021); WASH. REV. CODE § 4.105 (2023) (current law).

34. *See* Davis v. Cox, 351 P.3d 862, 874 (Wash. 2015) (overruled on other grounds) (finding Washington anti-SLAPP law "invades the jury's essential role of deciding debatable questions of fact," violating jury trial right); Leiendecker v. Asian Women United of Minn., 895 N.W.2d 623, 635 (Minn. 2017) (finding Minnesota anti-SLAPP law violates right to jury where tort historically had a jury right); Opinion of Justices, 641 A.2d 1012, 1015 (1994) (finding proposed New Hampshire anti-SLAPP procedure requires Court to weigh the pleadings and affidavits in a way that violates right to jury).

35. *See* Competitive Enter. Inst. v. Mann, 150 A.3d 1213, 1236-37 (D.C. 2016) (holding that to avoid unconstitutional interpretation of D.C. anti-SLAPP statute, the plain text needed to be read to impart a different standard of review than an ordinary reading would indicate).

protections of the First Amendment.[36] This is because, when speech strikes at the heart of the First Amendment's protection, the First Amendment serves as a defense, even when harm has been caused; the right to expression functionally trumps the right to redress.[37] These constitutional considerations and the original focus of Canan and Pring's work lead to the second point: how do consumer reviews fit into this scheme?

While Canan and Pring were focused on the right to petition, and some states have kept their anti-SLAPP laws narrow to avoid constitutional concerns, there has always been divergence on the scope of applicability of anti-SLAPP protection.[38] SLAPPs are not easily limited to a single fact pattern.[39] Recognizing this reality, many states have enacted anti-SLAPP legislation that protects some combination of freedom of the press, the right to petition, the right of association, and freedom of speech on matters of public concern.[40] These broader categories of protected activities and acceptable fora for the speech naturally led to divergences in states' anti-SLAPP laws and jurisprudence.[41]

Scholars have recognized a trichotomy in anti-SLAPP statutes based on the scope of protected conduct: narrow or direct petitioning statutes, moderate

36. *See, e.g.*, MASS. GEN. LAWS ch. 231 § 59H (2023) (applying anti-SLAPP law only to speech made before a governmental body, made in connection to an issue under consideration or review by a governmental body, or statements likely to encourage such a review or enlist public participation in an effort to consider such a review); MO. REV. STAT. § 537.528 (2023) (applying anti-SLAPP law in connection with a public hearing or meeting, or in a quasi-judicial proceeding); 27 PA. CONS. STAT. § 8302(a) (2023) (applying anti-SLAPP law only to speech made to the government related to the enforcement or implementation of an environmental law or regulation).

37. *See, e.g.*, Snyder v. Phelps, 562 U.S. 443, 451-52 (2011) (internal citations omitted). Discussed in more detail below, the question for the court was not whether Phelps' speech caused Snyder to suffer from intentional infliction of emotional distress, but whether the speech was on an issue of public interest. *Id.* If it was, it was "at the heart of the First Amendment's protection," and Snyder could not hold Phelps liable, whether Phelps caused Snyder's emotional distress or not. *Id.*

38. *See* CAL. CIV. PROC. CODE § 425.16(e) (Deering 2023) (passed in 1992, California's was one of the first anti-SLAPP statutes and included a scope of protected speech beyond just petitioning activities).

39. *See* UNIF. PUB. EXPRESSION PROT. ACT prefatory note ("SLAPPs defy simple definition. They can be brought by and against individuals, corporate entities, or government officials across all points of the political or social spectrum. They can address a wide variety of issues—from zoning, to the environment, to politics, to education.").

40. *See, e.g.*, CAL. CAL. CIV. PROC. CODE § 425.16(e) (Deering 2023); COLO. REV. STAT. § 13-20-1101(2)(a); HAW. REV. STAT. § 634G-2 (2022); IND. CODE § 34-7-7-2 (2024); KY. REV. STAT. ANN. § 454.462(1) (West 2023).

41. *Compare* CAL. CIV. PROC. CODE § 425.16 (Deering 2023) (protecting speech made in a broad array of fora on a broad array of subject matters), *with* 27 PA. CONS. STAT. § 8302 (2023) (providing immunity to speech only made in court or to a government body in connection with enforcing or implementing an environmental law or regulation).

or indirect petitioning statutes, and broad or public interest statutes.[42] While this taxonomy historically has been a useful framework, for the purposes of this Note, I propose a modified one. I consolidate the narrow and moderate categories (i.e., those which only apply to direct and indirect petitioning activities) and divide the broad category into general public interest states and review-friendly states based on explicit statutory language and jurisprudence. Using this new taxonomy of narrow, general public interest, and review-friendly, I then analyze how the FTC's proposed Rule on the Use of Consumer Reviews and Testimonials would convert general public interest states into review-friendly states through their method of public interest analysis.

III. ANTI-SLAPP LEGISLATION AND CONSUMER REVIEWS

As noted above, the SLAPP and anti-SLAPP were first conceptualized before the Internet became ubiquitous. As technology expanded the ability of the average person to comment on the world around them in a public forum, the importance of access to legal protection for that speech also expanded.[43] Critics have argued that as anti-SLAPP laws' applicability has broadened to meet those needs in the Internet era, they lose Pring and Canan's original "theoretical justification."[44] However, returning to the four characteristics Pring and Canan identified as common throughout SLAPPs and comparing this description to the restaurant review hypothetical at the beginning of this Note, it is clear that the review-based SLAPP and the petitioning-based SLAPP are not really so distinct. The restaurant is retaliating against the consumer's speech, utilizing its enhanced resources to convert a desire to silence the consumer into a cognizable claim for defamation that it has no real desire to win, so long as the consumer takes their review down.

If application and expansion of the anti-SLAPP beyond its original theoretical underpinnings can be justified, it now becomes necessary to see

---

42. *See, e.g.*, Matthew D. Bunker & Emily Erickson, *The Jurisprudence of Public Concern in Anti-SLAPP Law: Shifting Boundaries in State Statutory Protection of Free Expression*, 44 HASTINGS COMM. & ENT. L. J. 133, 138-40 (2022) (slightly different, using "petition" "public concern" and "additive public-concern" to describe statutes that only relate to petitioning activity, all public concern, and public concern with some particular limitations); Sharp-Wasserman & Mascagni, *supra* note 10, at 380-82 (comparing the broad anti-SLAPP statutes of California to the narrow ones of New Mexico and Pennsylvania); Shannon Hartzler, Note, *Protecting Informed Public Participation: Anti-SLAPP Law and the Media Defendant*, 41 VAL. U. L. REV. 1235, 1248 (2007) (using narrow, moderate, broad taxonomy).

43. *See*, Matthew D. Bunker & Emily Erickson, *#Aintturningtheothercheek: Using Anti-SLAPP Law as a Defense in Social Media*, 87 UMKC L. REV. 801, 801-02 (2019) (explaining the evolution of anti-SLAPP jurisprudence and the significance of being able to avail yourself to the mechanism "beyond the original SLAPP paradigm"); Sharp-Wasserman & Mascagni, *supra* note 10, at 367-69 (highlighting the overlapping nature of Section 230 of the Communications Decency Act and anti-SLAPP laws).

44. *See* Andrew L. Roth, Comment, *Upping the Ante: Rethinking Anti-SLAPP Laws in the Age of the Internet*, 2016 BYU L. REV. 741, 742 (2016) (arguing that while anti-SLAPP legislation is well intentioned, it becomes difficult because of its "outdated empirical basis and incomplete theoretical justification").

how jurisdictions have done so, if at all. Seventeen states have no current anti-SLAPP law on the books, and therefore are not included in this taxonomy.[45]

Narrow anti-SLAPP jurisdictions have SLAPP statutes which apply only to speech that in some way involves petitioning the government. There are currently eleven states that fall under this branch.[46] While there is variation within this category, none of these statutes are likely to cover consumer reviews.[47]

A. General Public Interest Anti-SLAPP

Sixteen states have what this Note calls "general public interest anti-SLAPP laws."[48] These statutes protect speech on matters of public interest, without defining with particularity when speech should qualify as a matter of public interest. California's anti-SLAPP law, for example, grants access to the anti-SLAPP procedure when a suit arises from an act "in furtherance of

45. *See* Greenberg et. al, *supra* note 3 (Alabama, Alaska, Idaho, Iowa, Michigan, Minnesota, Mississippi, Montana, New Hampshire, North Carolina, North Dakota, Ohio, South Carolina, South Dakota, West Virginia, Wisconsin, and Wyoming do not have anti-SLAPP laws).

46. Arkansas, Delaware, Florida, Illinois, Maine, Massachusetts, Missouri, Nebraska, New Mexico, Pennsylvania, and Rhode Island. *Id.*

47. *See* ARK. CODE ANN. § 16-63-503 (2023) (applying scope to speech that is intended to influence government action); DEL. CODE ANN. tit. 10, §§ 8136-8137 (2022) (applying scope to "actions involving public petition and participation," where that phrase is limited to "public applicant[s] or permitee[s]"); FLA. STAT. § 768.295 (2023) (applying scope requires speech be made "before a governmental entity" about a subject under review or consideration by a governmental entity, or that the speech be made in or in connection with certain media); 735 ILL. COMP. STAT. 110/15 (2023) (covering speech "genuinely aimed at procuring favorable government action, result, or outcome"); ME. STAT. tit. 14, § 556 (2023) (covering only petitioning activity); MASS. GEN. LAWS ch. 231, § 59H (covering petitioning activity); MO. REV. STAT. § 537.528 (2023) (requiring speech to be "made in connection with a public hearing or public meeting, in a quasi-judicial proceeding before a tribunal or decision-making body of the state or any political subdivision of the state"); NEB. REV. STAT. § 25-21,242 (2023) (requiring the speech to relate to "a public applicant or permittee" who brought the claim the motion seeks to dismiss); N.M. STAT. ANN. § 38-2-9.1(A) (West 1978) (applying to speech made in or in connection with public hearings and meetings); 27 PA. CONS. STAT. §§ 8301-02 (2023) (requiring the speech be related to environmental laws or regulations); 9 R.I. GEN. LAWS § 9-33-2 (2023) (using "matter of public concern" language, but also requires a showing that the exercise of free speech was not a "sham," where that requires showing the speech was intended to effect government action).

48. *See* ARIZ. REV. STAT. ANN. § 12-751 (2023) (Arizona actually covers any speech at all, as long as the defendant can establish that the current action was primarily motivated by a desire to silence them); CAL. CIV. PROC. CODE § 425.16(e) (Deering 2023); COLO. REV. STAT. § 13-20-1101 (2023); CONN. GEN. STAT. § 52-196(a)(1) (2023) (defining "matter of public concern" for purposes of the anti-SLAPP motion. Although consumer reviews are not included, the analysis of a consumer review's applicability would fall under (B) and allow for the same logic as the rest of the statutes in this category); GA. CODE ANN. § 9-11-11.1 (2023) (Georgia's statute has received negative judicial treatment discussed infra); HAW. REV. STAT. § 634G-2(a)(3); § 34-7-7-1 (2022); LA. CODE CIV. PROC. ANN. art. 971(a)(1) (2023); NEV. REV. STAT. §41.637(4) (2023); N.J. STAT. ANN. § 2A:53A-50(b)(3) (West 2023); N.Y. CIV. RIGHTS LAW §§ 70-a, 76-a (McKinney 2020); OR. REV. STAT. § 31.150(2) (2023); TEX. CIV. PRAC. & REM. CODE ANN. § 27.001(7) (West 2023); UTAH CODE ANN. § 78B-25-102(2)(c) (LexisNexis 2023); VT. STAT. ANN. tit. 12, § 1041(i) (2023); VA. CODE ANN. § 8.01-223.2(A) (2023).

the person's right of petition or free speech under the United States Constitution or the California Constitution in connection with a public issue."[49] It then recursively defines the act as (in part) "(3) any written or oral statement or writing made in a place open to the public or a public forum in connection with an issue of public interest, or (4) any other conduct in furtherance of the exercise of the constitutional right of petition or the constitutional right of free speech in connection with a public issue or an issue of public interest."[50] In other words, the act says that a defendant should have access to anti-SLAPP protection when they are being sued for speaking about an issue of public interest, and you will know they are being sued for speaking on an issue of public interest when they were speaking on an issue of public interest. Whether a given piece of speech is on a matter of public interest then, is a question for the court, and how courts have made this determination becomes the critical inquiry.

While the Supreme Court has not had occasion to define "matter of public concern" in the context of an anti-SLAPP statute, it has confronted the phrase in several notable cases related to broader First Amendment concepts. Unfortunately, as the Court has itself acknowledged, the test it has formulated for a matter of public concern is somewhat murky.[51] Most recently, the Court wrestled with this test in *Snyder v. Phelps*. In this case, the Westboro Baptist Church, led by Fred Phelps, held a protest with inflammatory picket signs outside of the funeral of Matthew Snyder, a Marine Lance Corporal killed in Iraq. Matthew Snyder's father sued Phelps, his daughters, and the Church for intentional infliction of emotional distress.[52] The Court considered whether the picket signs addressed matters of public concern, as that type of speech is central to First Amendment protections.[53] If the Court answered in the affirmative, then holding Phelps liable for intentional infliction of emotional distress for that speech would be an abridgment of his First Amendment rights.[54] Relying on its precedent in *Connick v. Meyers*, 461 U.S. 138 (1983), the Court looked to the "content, form, and context" of the speech "as revealed by the whole record."[55] The Court ultimately determined that despite the vulgarity of the signs, they were broadly meant to address issues of national significance, namely the Church's views on homosexuality, the Catholic Church, and the morality of the nation, in a context that, because of its objectionable nature, would capture as much attention as possible.[56] This "content, form, and context" test has been criticized as circular and unclear, leading to "an unpredictable free speech environment."[57] The basic function,

49. CAL. CIV. PROC. CODE § 425.16(b)(1) (Deering 2023).
50. *Id.* § 425.16(e).
51. City of San Diego v. Roe, 543 U.S. 77, 83 (2004) ("the boundaries of the public concern test are not well defined").
52. *See Snyder*, 562 U.S. at 448-50.
53. *See id.* at 444 ("Whether the First Amendment prohibits holding Westboro liable for its speech in this case turns largely on whether that speech is of public or private concern").
54. *See id.* at 451-52.
55. *Id.* at 453 (internal citations omitted).
56. *Id.* at 454-56.
57. *See* Bunker & Erickson, *supra* note 42, at 147.

as illustrated in *Snyder v. Phelps*, is to look at what issue the speech purports to address (content), and how the delivery of the speech (form) relates back to that issue (context).

At the state level, there has been more on-point jurisprudence defining "public concern" in the anti-SLAPP and consumer review contexts. In California, for instance, the historical trend had been to construe the anti-SLAPP statute as broadly as possible.[58] Despite the courts' stated preference for a broad construction, there has been reluctance at times to find that online consumer reviews meet the initial burden of establishing themselves as speech on a matter of public interest.[59] *Wilbanks v. Wolk*, is referred to as the "leading case" for online consumer reviews and anti-SLAPP law.[60] Under the *Wilbanks* test, a consumer review is considered in the public interest when:

> (1) the subject of the statement or activity precipitating the claim was a person or entity in the public eye; (2) the statement or activity precipitating the claim involved conduct that could affect large numbers of people beyond the direct participants; [or] (3) whether the statement or activity precipitating the claim involved a topic of widespread public interest.[61]

More recently, in *FilmOn.com Inc. v. Double Verify, Inc.*, the California Supreme Court refined the public interest inquiry into a two-part analysis asking "what public interest or . . . issue of public interest the speech in question implicates" (the content of the speech) and "what functional relationship exists between the speech and the public conversation," (the context of the speech).[62] Essentially, without directly citing it, California has adopted at least part of the *Snyder* test.[63]

The Oregon Supreme Court has similarly stated the question of whether a review is on a matter of public concern turns on the Supreme Court's "content, form, and context," test.[64] In *Lowell v. Wright*, the Oregon Supreme Court was asked to determine whether a consumer review left by Wright, an employee of a rival piano shop of Lowell's, was a matter of public concern for First Amendment purposes.[65] Although Wright was availing himself of a

58. *See* Chaker v. Matteo, 209 Cal. App. 4th 1138, 1145 (Cal. App. 4th 2012) (citations omitted) ("[C]ases which have considered the public interest requirements of the Anti-SLAPP Law have emphasized that the public interest may extend to statements about conduct between private individuals.").

59. *See* Dunne v. Lara, No. B210779, 2009 WL 3808345, at * 15-16 (Cal. Ct. App. Nov. 16, 2009) (holding disgruntled motorcycle repair shop customer's online reviews not in public interest because they only concerned those who would be interested in getting motorcycle repair services in that geography); Sandra Caron European Spa, Inc. v. Kerber, No. A117230, 2008 WL 3976463, at * 1 (Cal. App. Ct. August 28, 2008) (spa customer's negative reviews not in public interest).

60. *Chaker*, 209 Cal. App. 4th at 1145 (citing Wilbanks v. Wolk, 121 Cal. App. 4th 883 (Cal. App. 2004)).

61. Wilbanks v. Wolk, 121 Cal. App 4th 883, 898 (Cal. App. 4th 2004).

62. FilmOn.com Inc. v. DoubleVerify Inc., 439 P.3d 1156, 1165 (Cal. 2019).

63. *See* Bunker & Erickson, *supra* note 42, at 150.

64. *See* Lowell v. Wright, 512 P.3d 403, 418-19 (Or. 2022).

65. *See id.*

First Amendment public comment defense, and not using the anti-SLAPP mechanism, the court explained that the analytical question of whether the speech was on a matter of public concern was the same "content, form, and context" test.[66] Although the court expressed doubt that an online consumer review should be considered *de facto* speech on a matter of public interest, it also expressed that under the right circumstances it could be.[67] However, because Lowell had not asked the court to overturn earlier precedent holding that a similar review was on a matter of public interest, the court allowed the entirety of Wright's review to qualify without engaging in a full content, form, context analysis.[68] Given this case, it appears that for the time being in Oregon, an online consumer review will easily qualify as speech on a matter of public interest, but it will be necessary to reaffirm this qualification should the Oregon Supreme Court see a case which challenges its earlier precedent.

The Georgia Supreme Court, in analyzing its state's most recent anti-SLAPP law noted the broad similarities between its law and California's.[69] While the discussion of whether the speech at issue fell within the scope of the anti-SLAPP statute was relatively limited to a holding that it did, the court appeared to rely on the California precedent, citing *FilmOn.com Inc*, in reaching that determination.[70] Once again, the test for the public interest will rely on the content, context, and form of the speech.

In the context of an online review, Colorado's recently enacted anti-SLAPP law[71] saw litigation in the online review context in *Tender Care Veterinary Ctr., Inc. v. Lind-Barnett*.[72] In *Tender Care*, a disgruntled patient of a rural veterinary clinic left negative reviews online.[73] The court first noted, as the Georgia court did, the similarity between the Colorado and California statutes, and explained that it would look to California case law for guidance in construing and applying the Colorado statute.[74] The court then applied the two-step *FilmOn.com* analysis (again, a modified *Snyder* analysis of "content

66. *See id.* at 418.
67. *See id.* at 418.
68. *See id.* at 419.
69. *See* Wilkes & McHugh, P.A. v. LTC Consulting, L.P., 830 S.E.2d 119, 124 (Ga. 2019) (noting that Georgia's anti-SLAPP statute had recently been amended, effecting the court's ability to rely on their own precedent, "thus, in interpreting our new OCGA § 9-11-11.1, we may look to California case law interpreting § 425.16 for guidance, especially decisions — such as the ones cited in this opinion — that employ the same kind of statutory analysis that we generally use").
70. *See id.* at 128.
71. § 13-20-1101 was enacted in 2019. COLO. REV. STAT § 13-20-1101 (2023).
72. Tender Care Veterinary Ctr., Inc. v. Lind-Barnett, 2023 COA 114 (as of writing, this appears to be the highest court in Colorado to have addressed the new anti-SLAPP statute). The Colorado Supreme Court has granted certiorari in part to determine whether there needs to be a "nexus" in which the movant's speech "encourages, facilitates, or contributes to a general debate," whether the "matter of public concern" standard for defamation and invasion of privacy is the same as the "matter of public interest" standard, and whether the speaker's motive is a consideration in evaluation of the anti-SLAPP motion. Lind-Barnett v. Tender Care Veterinary Ctr., Inc., No. 24SC8, 2024 Colo. LEXIS 890 (Sept. 3, 2024).
73. *See* Tender Care Veterinary Ctr., Inc., 544 P.3d at 695-96.
74. *See id.* at 697-98.

and context") to determine if the defendant's reviews qualified as speech on a matter of public interest.[75]

Although this review is not completely exhaustive, it is largely indicative of the approach courts take in analyzing the public interest question.[76] At the federal level, whether speech implicates an issue of public interest is based on a fact intensive analysis of the speech's content, context, and form. At the state level, much the same applies, if slightly streamlined to an analysis of what the content of the speech is, and how that relates to the public interest it purports to connect to.

B. Review-Friendly Anti-SLAPP

Six jurisdictions (five states and the District of Columbia) have enacted anti-SLAPP statutes I refer to as "review-friendly."[77] Some of these jurisdictions explicitly include speech on a "good, product, or service in the marketplace" in their definition of a matter of public concern.[78] In other jurisdictions, such as Kentucky and Washington, one section of the statute prohibits use of the anti-SLAPP mechanism by a defendant who is in the primary business of selling goods and services when the speech at issue is related to the sale of goods or services, but includes an exception to this exception when the speech at issue is a consumer review.[79] In those jurisdictions, the statute makes clear that anti-SLAPP protection is not meant to apply to most categories of commercial speech (like advertising), but that consumer reviews are meant to be protected. In either type of jurisdiction, there is no question that consumer reviews fall within the scope of the public interest because the statute tells the reader it does. So long as a reviewer can satisfy the rest of the anti-SLAPP procedure's requirements, they will likely receive its protections.

IV. RULE ON THE USE OF CONSUMER REVIEWS AND TESTIMONIALS AS JUSTIFICATION FOR EXPANDED ANTI-SLAPP SCOPES

Having established a taxonomy for anti-SLAPP laws, categorized the existing statutes within that taxonomy, and explained how general public interest jurisdictions conceptualize speech on matters of public interest, we

75. *See id.* at 698-700.

76. *See generally* Bunker & Erickson, *supra* note 42 (providing a more detailed overview of the evolution of the public concern analysis in anti-SLAPP context).

77. D.C., Kansas, Kentucky, Oklahoma, Tennessee, and Washington. *See* Greenberg et. al, *supra* note 3.

78. *See* D.C. CODE § 16-5501(3) (2023); KAN. STAT. ANN. § 60-5320(7)(E) (2023); OKLA. STAT. tit. 12, § 1431(7)(e) (2023); TENN. CODE ANN. § 20-17-103(6)(E) (2023).

79. *See* KY. REV. STAT. ANN. §§ 454.462(2)(a)(3) and 454.462(2)(b)(2) (West 2023) (exempting commercial speech in 2(a)(3), then 2(b)(2) clarifies that anti-SLAPP protection applies to consumer reviews); WASH. REV. CODE §§ 4.105.010(3)(a)(iii) and 4.105.010(3)(b)(ii) (2023) (exempting commercial speech in (3)(a)(iii) then clarifying that consumer reviews are included under anti-SLAPP protections with (3)(b)(ii)).

can now turn to how an application of the FTC's Rule on the Use of Consumer Reviews and Testimonials might impact each jurisdiction.[80]

A. In Narrow and Review Friendly Jurisdictions

The FTC's Rule on the Use of Consumer Reviews and Testimonials will not have any impact on an individual SLAPP-target's access to anti-SLAPP protection in narrow jurisdictions. To qualify for anti-SLAPP protection in these jurisdictions, the speech must take place either in the direct context of petitioning activities, or as an indirect effort to petition the government.[81] While there are conceivable instances where a consumer review could be recast as a form of indirect petitioning[82], nothing about the Rule on the Use of Consumer Reviews and Testimonials would result in authority to transform all consumer reviews into indirect petitioning efforts. The Rule on the Use of Consumer Reviews and Testimonials' recognition of consumer reviews as speech in need of protection should make such speech implicitly a matter of public concern (as discussed below). Being speech on a matter of public concern, however, is not the same as being speech related to petitioning activities. This does not mean that SLAPP-targets in these jurisdictions are defenseless.[83] Ideally, the existence of an FTC regulation prohibiting these SLAPPs would prevent them from being filed in the first place. If the FTC is successful in bringing an enforcement action, they may "more readily obtain monetary redress for victims."[84]

In reviewer friendly jurisdictions, the FTC's Rule on the Use of Consumer Reviews and Testimonials is likely to have minimal impact. Since these jurisdictions already include consumer reviews in the scope of their anti-SLAPP statutes, a new reading isn't necessary to shore up their protection. Like narrow jurisdictions, however, there should be an overall reduction in SLAPP's filed against consumer reviews if the primary purpose of the FTC's Rule on the Use of Consumer Reviews and Testimonials is effective.

B. In General Public Interest Jurisdictions

In general public interest jurisdictions, the FTC's Rule on the Use of Consumer Reviews and Testimonials would have a profound impact on a SLAPP-target's ability to access anti-SLAPP protection. As discussed above, at the federal level the applicable test for speech as a matter of public interest

80. *See* 16 C.F.R. § 465.7(a).

81. *E.g.*, ch. 231, § 59H (Massachusetts statute applying only to petitioning speech).

82. For instance, a review of a dirty restaurant might call on the Board of Health to take action.

83. *See, e.g.*, *Lowell*, 512 P.3d. Wright did not avail himself of the anti-SLAPP mechanism available to him, but instead used a First Amendment public comment defense, which is available regardless of the presence of an anti-SLAPP law. *Id.* Such defendants will not benefit from the procedural gifts of the anti-SLAPP mechanism, but still receive the same substantive protection the mechanism is designed to instill.

84. Trade Regulation Rule on the Use of Consumer Reviews and Testimonials, 88 Fed. Reg. at 49377.

is whether, based on the "content, context, and form" of the speech, it can be said to reflect a broad public concern.[85] At the state level, in the anti-SLAPP context, this test has morphed through the broad application of the *FilmOn.com, Inc.* standard to simply content and context, or an investigation into what public interest the speech is argued to connect to, and how it makes that connection.[86] The FTC's Rule on the Use of Consumer Reviews and Testimonials would make it an unfair or deceptive act or practice "to use an unjustified legal threat . . . to prevent a consumer review or any portion thereof from being written or created or cause a consumer review or any portion thereof to be removed."[87] This makes it clear that online consumer reviews implicate a matter of public interest, because the very existence of the rule is predicated on the importance of the consumer review ecosystem to the nation's economy.[88] The FTC states "the number of online reviews and aggregate ratings are extremely important for consumer purchase decisions," and "the presence of online reviews improves consumer welfare via reductions in both search costs and the level of information asymmetry that

85. *Snyder*, 562 U.S. at 453 (internal citations omitted).

86. *See FilmOn.com Inc.*, 439 P.3d at 1165 (step one: identify the public interest the speech proports to reflect; step two: identify how the speech interacts with that public interest); *Wilkes & McHugh, P.A.*, 830 S.E.2d at 128 (Georgia applying *FilmOn.com*); *Tender Care Veterinary Ctr., Inc.*, 544 P.3d at 697-98 (Colorado applying *FilmOn.com*).

87. 16 C.F.R. § 465.7(a).

88. *See* Attorneys General of D.C., Pennsylvania, & Illinois, Comment Letter on Proposed Trade Regulation Rule on the Use of Reviews and Testimonials (Sept. 29, 2023), https://portal.ct.gov/-/media/ag/press_releases/2023/2023929-comment-of-23-state-ags-ftc-consumer-reviews-and-testimonials.pdf [https://perma.cc/RAF7-98MX] (state Attorneys General recognizing the significance of protecting consumer reviews as "laudable"); Consumer Reports, Comment Letter on Proposed Trade Regulation Rule on the Use of Reviews and Testimonials, (Sept. 29, 2023), https://advocacy.consumerreports.org/wp-content/uploads/2023/10/Comments-of-Consumer-Reports-In-Response-to-the-Federal-Trade-Commission-Notice-of-Proposed-Rulemaking-on-the-Use-of-Consumer-Reviews-and-Testimonials-.pdf [https://perma.cc/5NY2-CTB5] (stating unfair and deceptive practices in review space "mutated on large e-commerce platforms"); Tripadvisor, Comment Letter on Proposed Trade Regulation rule on the Use of Reviews and Testimonials (Jan. 9, 2023), https://www.regulations.gov/comment/FTC-2022-0070-0036 [https://perma.cc/V4KN-3ESC] ("for travelers, cost combined with the time commitment and natural risk of traveling to parts unknown make real-time traveler reviews nearly indispensable"); Trustpilot, Comment Letter on Proposed Trade Regulation Rule on the Use of Reviews and Testimonials, (Sept. 29, 2023), https://downloads.regulations.gov/FTC-2023-0047-0084/attachment_1.pdf [https://perma.cc/6M2Q-YPZH]. ("[G]enuine, honest and real experiences shared online are invaluable, both to the people who write and read them, and to the businesses who can use them to understand their customers and improve their offerings."); Yelp, Comment Letter on Proposed Trade Regulation Rule on the Use of Reviews and Testimonials, (Jan. 6, 2023) https://www.regulations.gov/comment/FTC-2022-0070-0028 [https://perma.cc/3DBW-FG4K] (according to an internal Yelp survey conducted in 2022, respondents claimed they read "a median of five reviews" before making a purchase, and another study found that 90% of people on Yelp compare businesses before making a spending decision); The Transparency Company, Comment Letter on Proposed Trade Regulation Rule on the Use of Reviews and Testimonials, (Jan. 10, 2023), https://www.regulations.gov/comment/FTC-2022-0070-0044 [https://perma.cc/LAK8-4QFR] (stating the review management industry is worth over an estimated $8.8 billion, showing the value that businesses place in managing and suppressing negative reviews).

exists prior to purchase."[89] In numbers, the FTC estimated, during the NPRM phase, that perfect implementation of all aspects of its proposed Rule would result in annual "welfare improvements from better informed-purchased decisions" between 5.8 and 15.85 billion dollars.[90] While this estimate does not address the individual impact of a reduction in review suppression, it highlights the importance of a free flow of reviews to an issue of public interest, the national economy.

The FTC's treatment of consumer reviews as something that requires protection from the unfair or deceptive act of a SLAPP collapses the two-step analysis into a single point. A consumer review is speech on a matter of public importance because we recognize that, so long as it is a consumer review, it is of importance to the public, and it connects to that public interest by virtue of being a consumer review. Its content and context overlap.

Consider again the hypothetical at the beginning of this Note. You leave a review about your terrible restaurant experience, and the restaurant attempts to use a SLAPP to get you to take the review down. Without the FTC's Rule on the Use of Consumer Reviews and Testimonials, you would need to argue that your review related to the public interest because 1) the content served the public's interest in knowing which restaurants in the area were worth patronizing; and 2) the review itself adequately related to that public interest without becoming about your personal vendetta with the restaurant.[91] With the FTC's Rule on the Use of Consumer Reviews and Testimonials in place, however, your argument could be: 1) the content of your post relates to a matter of public importance because the FTC has recognized the public value of consumer reviews; and 2) the review exists in context as a consumer review.

Critics would argue that this overextends the anti-SLAPP law in a way state legislatures and Canan & Pring had not intended.[92] They may claim that this steps past the balancing line between the SLAPP-target's First Amendment rights and the filer's right to a trial.[93] However, this need not be the case for two reasons.

First, as discussed above, when speech touches on a matter of public interest, it reaches the core of First Amendment protections, and the need to protect that speech is greater than the right to redress, even where the speech may have been harmful.[94] The Westboro Baptist Church's signs hurt Mr. Snyder.[95] The speech at issue likely did inflict emotional distress upon Mr. Snyder; the jury found Phelps and the Church guilty and liable for almost

89. Trade Regulation Rule on the Use of Consumer Reviews and Testimonials, 88 Fed. Reg. at 49382.

90. *Id.* at 49383-84.

91. *See Tender Care Veterinary Ctr., Inc.*, 544 P.3d at 700-02 (Lind-Barnett's posts failed to satisfy second prong of public interest because they were ultimately, in context, about exercising her hatred for the veterinary hospital).

92. *See* Roth, *supra* note 44, at 743 (certainly this is a long walk from the original petitioning scope of Canan & Pring's study).

93. *See* Philips & Pumpian, *supra* note 31, at 408.

94. *See Snyder*, 562 U.S. at 451-52.

95. *See id.* at 450 (describing Mr. Snyder's thoughts of the picketing as causing him to become "tearful, angry, and physically ill").

eleven million dollars of damages.[96] Likewise, negative consumer reviews can devastate a business.[97] The harm to the business is as real as the harm to Mr. Snyder, but the speech at issue reaches a crucial public interest, and as such requires the strongest protections the First Amendment can provide.[98]

Second, while this understanding of public interest broadens access to the anti-SLAPP mechanism at the first hurdle, it does not help the SLAPP defendant if the plaintiff can show that their claim is not meritless. The SLAPP target's burden is alleviated during the first step of the anti-SLAPP analysis, establishing that the Act applies, but this does not mean that the SLAPP filer (or plaintiff, if the suit is not, in fact meritless) cannot still establish a prima facie case during the second step.[99] If the review truly is defamatory, being able to establish that the review is in scope of the statute does not mean the motion will automatically be granted. If the claim was frivolous, and you sought to abuse the broadened applicability of anti-SLAPP protection, you may end up owing the attorney's costs and fees.[100]

Rather, this reading of the public interest standard expands access to the anti-SLAPP statute in a way that is consistent with the goals of these statutes. It speeds up time of deliberation, reduces the expenses of litigation, and ensures that meritless suits meet quick ends.

V. CONCLUSION

Anti-SLAPP legislation provides valuable protection against frivolous lawsuits meant to quash a person's access to First Amendment rights. Currently, there is ambiguity over access to this mechanism in general public interest jurisdictions.[101] Through application of the FTC's Rule on the Use of Consumer Reviews and Testimonials to the "content and context" test for public interest, consumer reviews should have a much easier time clearing the first requirement of winning an anti-SLAPP motion.

By easing access to the anti-SLAPP mechanism at the first stage, consumers receive a deeper degree of protection in line with the goals of the legislation. Anti-SLAPP laws are designed to reduce the time and hassle caused by frivolous litigation, but while consumer reviews remain in a gray area in general public interest jurisdictions, their power to do so is hampered. In affirming the consumer review's status as de facto speech on a matter of public interest, we assure that a negative review never costs more than one bad night out.

---

96. *See id.*

97. Ross Marchant, *The Impact of Online Reviews on Businesses*, BRIGHTLOCAL (Mar. 15, 2017), https://www.brightlocal.com/blog/the-impact-of-online-reviews/ [https://perma.cc/DW5Z-LU6S] (one negative review could reduce customers by 22%, or about thirty customers).

98. *See Snyder*, 562 U.S. at 458.

99. *See* UNIF. PUB. EXPRESSION PROT. ACT prefatory note (explaining the flow of a motion under an anti-SLAPP law).

100. *See id.* § 10.

101. *See supra* Part III(A).

Two Steps Forward, One Step Back: Gaps in the Violence Against Women Act

Sebrina Thomas*

TABLE OF CONTENTS

I. INTRODUCTION 177

II. BACKGROUND 179

A. What is Domestic Violence? 179

B. The Current Legal Frameworks on Image-Based Abuse 182

1. The Violence Against Women Act 183

a. The VAWA's Development from 1994 to Present 183
b. Revenge Porn in the VAWA 185
c. The VAWA Makes No Mention of Sextortion 185
d. The VAWA Makes No Mention of Image-Based Abuse Created with Deepfake Technology 186

C. Current Federal Reform Efforts Addressing Image-Based Abuse 187

1. Understanding the Stopping Harmful Image Exploitation and Limiting Distribution Act of 2023 187
2. Understanding the Preventing Deepfakes of Intimate Images Act 188

D. Current State Legislation Targeting Image-Based Abuse 189

1. State Legislation on Revenge Porn 189
2. State Legislation on Sextortion 190
3. State Legislation Addressing Image-Based Abuse Facilitated by Deepfake Technology 190

III. ANALYSIS 191

* J.D., May 2025, The George Washington University Law School; Senior Production Editor, Federal Communications Law Journal, Volume 77; B.S. May 2021, Legal Studies, University of Central Florida. Thank you to the entire FCLJ staff for their dedication and hard work, without which this publication would not have been possible. My heartfelt gratitude also goes to the late Professor Lucarelli for all of his invaluable guidance, and my family and close friends for their continuous support and encouragement.

A. Congress Should Reauthorize the VAWA to Include Appropriate Civil and Criminal Remedies to Combat the Growth of Image-Based Abuse 192

1. What the VAWA is Missing 192
2. Congress Should Consider Incorporating Language Exhibited in the SHIELD and PDII Acts to Adequately Address Image-Based Abuse 194

IV. CONCLUSION 197

I. INTRODUCTION

What if one day, when living your life as you normally do—like walking your dog in the morning, or stopping at a coffee shop, or visiting the bank to deposit a check—your life completely changes in an instant? It is not because your car suddenly gets a flat tire, or you forgot about a meeting you had for work. Instead, it's because intimate images of yourself have been shared online for the world to see. You have no idea who would share these photos and why they would do so, especially without your consent or even knowledge. You ask yourself: who would intentionally share your intimate images? Who would share your photos for the world to see? Who would do this to a person? Who would do this to *you*?

You begin to realize that your body, your entire being, is now visible for the entire world and you cannot do anything about it. You realize the people closest to you such as your parents, siblings, friends, co-workers, neighbors, and complete strangers can now see a part of you they should never see without your consent. You become consumed with regret for even taking the photos in the first place. Then you wonder, how will your friends and family view you? What will they think of you? What if you want to get a new job and the employer sees this? What if the girls whispering behind you at the coffee shop this morning were murmuring about your pictures and you just didn't know?

Although society would prefer to look away or feign indifference to this experience many women face, the harm women endure is not something to ignore, nor is it out of the ordinary. Up to 1 in 5 adults are victims of revenge porn.[1] Victims have reported that their intimate photos were released by a current or previous romantic partner without their permission.[2] Victims have stated that their photos were released by a complete stranger or by someone close to them— a friend, family member, or co-worker.[3] Victims of sextortion are blackmailed, threatened, or coerced in sending intimate images and videos of themselves.[4] It has been estimated by the Internet Crime Complaint Center, a division in the FBI dedicated to investigating cybercrimes, "that they [have] received over 18,000 sextortion-related complaints nationally."[5] Studies "illustrate the disturbing trend of sextortion," including that "half of sextortion victims are threatened several times per day, with 1 in 4 receiving

1. Conor Walsh, *Revenge Porn: The Latest Research and Law Enforcement Efforts*, TRAINING INST. ON STRANGULATION PREVENTION (May 30, 2023), https://www.strangulationtraininginstitute.com/revenge-porn-the-latest-research-and-law-enforcement-efforts/ [https://perma.cc/P92L-6KSR].

2. *See id.*

3. *See id.*

4. *See* FBI, INTERNET CRIME REPORT (2021), https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf, at 12; *see also The Rise of 'Sextortion' on Social Media and How to Protect Youth*, LINEWIZE (Feb. 3, 2023) [hereinafter *Rise of Sextortion*], https://www.linewize.com/blog/the-rise-of-sextortion-on-social-media#:~:text=Approximately%205%25%20of%20students%20reported,13%20or%20younger%20when%20threatened [https://perma.cc/5YWF-KHFK].

5. *See* Rise of Sextortion, *supra* note 4.

between 10 and 19 threats per days."[6] Additionally, it has been reported that "almost *half* of [perpetrators] follow through on their threats if the victim does not comply" (emphasis added).[7]

Once faced with image-based abuse, victims experience a plethora of effects such as feeling shame or embarrassment, so much so that some do not report the incident.[8] Victims also experience a "decline in [their] mental health and wellbeing" where they become "increasingly secretive with [their] digital devices" and have "[s]udden and unexplained personality changes or mood swings."[9] The FBI has reported that "more than a dozen sextortion victims were reported to have [lost their lives to] suicide."[10]

Domestic violence no longer appears solely through its traditional forms such as physical or verbal abuse. Rather, domestic violence has transformed due to the advancement in technology which has led to the birth of image-based abuse.[11] Image-based abuse is the use of technology such as phones, computers, surveillance, and deepfake technology to facilitate domestic violence.[12] It is important to recognize that image-based abuse does not have a heavy bulk of research behind it due to underreporting.[13] However, it is clear that the structures in place to protect women from domestic violence have not sufficiently kept pace with today's current state of technology. As technology advances so should the laws covering domestic violence. Who is Congress really punishing? Is it punishing the perpetrators who release a woman's intimate images without their consent? Or the victims themselves by not establishing a stronger statutory framework that victims can use to receive justice for the horrific acts carried out against them?

This Note will focus on technological abuse through a general lens as it pertains to women. Technological abuse can be further complicated and exacerbated "due to race and ethnicity, age, sexual orientation, religion, gender identity/expression, socioeconomic status . . . disability, and [immigration] status."[14] The intersectionality of these factors, being a victim

---

6. *Id.*
7. *Id.*
8. Walsh, *supra* note 1.
9. Rise of Sextortion, *supra* note 4.
10. Press Release, U.S. Att'y's Off., S. Dist. of Ind., FBI and Partners Issue National Public Safety Alert on Sextortion Schemes (Jan. 19, 2023) (on file with author), https://www.justice.gov/usao-sdin/pr/fbi-and-partners-issue-national-public-safety-alert-sextortion-schemes [https://perma.cc/WT4Q-XSDF].
11. Walsh, *supra* note 1.
12. *See generally About Abuse*, WOMENSLAW.ORG, https://www.womenslaw.org/about-abuse/abuse-using-technology/ways-abusers-misuse-technology [https://perma.cc/JUX5-3WKQ] (last updated Sept. 30, 2024) (choose "Ways Survivors and Abusers Misuse Technology"; then choose "Abuse Involving Texts, Photos, and Videos"; then choose "Abuse Involving Nude/Sexual Image"; then choose "Definitions and basic information").
13. *Id.*
14. UNESCO, "YOUR OPINION DOESN'T MATTER, ANYWAY": EXPOSING TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE IN AN ERA OF GENERATIVE AI 11 (2023), https://unesdoc.unesco.org/in/documentViewer.xhtml?v=2.1.196&id=p::usmarcdef_0000387483&file=/in/rest/annotationSVC/DownloadWatermarkedAttachment/attach_import_2ef6fbfd-84e7-475e-a70e-c6e574f0645a%3F_%3D387483eng.pdf&locale=en&multi=true&ark=/ark:/48223/pf0000387483/PDF/387483eng.pdf [https://perma.cc/HNA7-PKYG].

of image-based abuse and domestic violence as a whole deserves and requires its own discussion. This Note argues that the legal framework in place for protecting victims of domestic violence is inadequate because it has not kept pace with today's technology and the evolution of domestic violence with technology. Ultimately, the current legislation is not serving Congress' intended purpose of protecting women. Congress has made steps forward in accounting for the victims who experience domestic violence through technology.[15] However, the remedies available to victims of image-based abuse are insufficient. Accordingly, to effectively protect women from domestic violence, Congress should adopt legislation similar to the proposed Stopping Harmful Image Exploitation and Limiting Distribution Act of 2023 ("SHIELD Act") or the Preventing Deepfakes of Intimate Images Act ("PDII Act") to help resolve the unsatisfactory legal frameworks covering domestic violence on the federal level.[16]

Part II.A will provide factual background on what domestic violence is, how it has evolved as technology has advanced, and what revenge porn, sextortion, and image-based abuse with deepfake technology (collectively referred to as "image-based abuse") encompass. Part II.B will provide background on the current legal frameworks in place that cover image-based abuse on both the federal and state level. Part II.B.1 will provide background on the Violence Against Women Act ("VAWA"). Part II.C will discuss recent federal reform efforts on image-based abuse. Part II.D will provide background on current state legislation that covers image-based abuse. Part III will discuss the gaps left by Congress in addressing image-based abuse through the VAWA and what should be done to fill in the gaps. Finally, Part IV will conclude this analysis.

II. BACKGROUND

A. What is Domestic Violence?

Domestic violence, otherwise known as intimate partner violence, is "a pattern of behavior in any relationship that is used to gain or maintain power and control over an intimate partner."[17] To be classified as domestic violence, actions must be performed by a person who is either "a current or former spouse . . . intimate partner of the victim, or person similarly situated to a spouse of the victim."[18] Moreover, domestic violence may be performed by someone who "is cohabitating, or has cohabitated, with the victim as a spouse or intimate partner . . . shares a child in common with the victim . . . or

15. *See* 15 U.S.C. § 6851 (creating a civil cause of action relating to the disclosure of intimate images).

16. The Stopping Harmful Image Exploitation and Limiting Distribution Act of 2023, S. 412, 118th Cong. (2023); Preventing Deepfakes of Intimate Images Act, H.R. 3106, 118th Cong. (2023).

17. *What Is Domestic Abuse?*, UNITED NATIONS, https://www.un.org/en/coronavirus/what-is-domestic-abuse [https://perma.cc/6JDJ-D7CV] (last visited Jan. 25, 2024).

18. 34 U.S.C. § 12291(a)(12)(A).

commits [these acts] against a youth or adult victim who is protected from those acts under the family or domestic violence laws of the jurisdiction."[19] The acts carried out against a victim can include "behaviors that intimidate, manipulate, humiliate, isolate, frighten, terrorize, coerce, threaten, blame, hurt, injure, or wound."[20]

Domestic violence can encapsulate a broader degree of abusive conduct than many might initially recognize or realize. Many may primarily think of domestic violence in the forms of physical, verbal, emotional, or sexual abuse. This is a rational belief as domestic violence encompasses "the use of or attempted use of physical abuse or sexual abuse, or a pattern of any other coercive behavior committed, enabled, or solicited to gain or maintain power and control over a victim, including verbal, psychological . . . . " and economic abuse.[21] However, by virtue of today's prevalent use of technology, domestic violence can also take the form of technological abuse.[22]

Technological abuse, also known as image-based abuse, is domestic violence facilitated through technology and has occurred since as early as the 1980s, but "did not become widespread [or prevalent] until around 2010."[23] Technological abuse is performed when the "act or pattern of behavior that occurs within domestic violence . . . occurs using any form of technology, including but not limited to: internet enabled devices, online spaces and platforms, computers, mobile devices, cameras and imaging programs, apps, location tracking devices, communication technologies, or any other emerging technologies."[24] These acts are executed as a means to coerce, stalk, or harass another person and can take many forms including sending abusive texts, spying on someone through the tracking system on their device, and sharing intimate photos or videos of someone without their consent.[25]

Sharing intimate photos or videos of an individual without their consent is called image-based sexual abuse, otherwise termed as revenge porn or nonconsensual pornography.[26] The photos are disseminated without the victim's consent or permission and commonly show the victim engaged in a sexual act and/or nudity.[27] Additionally, the photos may be taken without the

19. 34 U.S.C § 12291(a)(12)(B)-(D).

20. *About the Office on Violence Against Women*, U.S. DEP'T JUST., OFF. ON VIOLENCE AGAINST WOMEN (Dec. 6, 2023), https://www.justice.gov/ovw/domestic-violence [https://perma.cc/YF95-MZJA].

21. 34 U.S.C § 12291(a)(12).

22. *See id.*

23. Chance Carter, *An Update on the Legal Landscape of Revenge Porn*, NAT'L ASSOC. ATT'Y GEN. (Nov. 16, 2021), https://www.naag.org/attorney-general-journal/an-update-on-the-legal-landscape-of-revenge-porn [https://perma.cc/6JRK-EXRW]. *See generally* Alexa Tsoulis Reay, *A Brief History of Revenge Porn*, N.Y. MAG. (July 19, 2013), https://nymag.com/news/features/sex/revenge-porn-2013-7/ [https://perma.cc/TU9K-LTU4].

24. 34 U.S.C. § 12291(a)(40).

25. *See Technology-Facilitated Abuse*, SAFE STEPS, https://www.safesteps.org.au/understanding-family-violence/types-of-abuse/technological-facilitated -abuse/ [https://perma.cc/3GFM-JFF4] (last visited Nov. 11, 2023).

26. *See Image-based Sexual Abuse: An Introduction*, END CYBER ABUSE, https://endcyberabuse.org/law-intro/ [https://perma.cc/R3KS-HDC8] (last visited Nov. 11, 2023) [hereinafter *Image-based Sexual Abuse*].

27. *See id.*

victim's knowledge, shared without the victim's consent, or both.[28] When posted—either on websites that host nonconsensual porn, social media, email, text, or other messaging services—the photos can include the victim's name or other identifying information such as their phone number, email, or social media links.[29] Up to 1 in 5 adults are victims of revenge porn.[30] Victims experience a range of symptoms and effects such as changes in sleep and eating patterns, nightmares, post-traumatic stress disorder, depression, anxiety, trust concerns, and suicidal thoughts.[31]

Revenge porn addresses the actual dissemination of intimate photos without the victim's consent.[32] However, there can be situations where the abuser does not disseminate the photos at all, but rather attempts or threatens to expose or distribute them unless the victim complies with their demands.[33] This is called sexual extortion or "sextortion."[34] Sextortion can take on different forms, specifically with how the perpetrators gain access to the victim's intimate photos.[35] For example, the perpetrator may hack into the victim's electronic devices and access their stored photos and webcams.[36] The perpetrator may take a nonconsensual recording of the victim, or a former or current intimate partner may take photos of the victim with their consent, but then subsequently threaten to disseminate them.[37] Through online dating scams the perpetrator may lure, groom, and sexually extort their victims by using social media or instant messaging platforms such as Instagram, X, or WhatsApp.[38] Once the perpetrator has possession of the intimate images, they may return "with additional demands and threaten to disseminate content to friends and family if the victim doesn't comply."[39]

As mentioned, in revenge porn and sextortion schemes, the victim may be unaware that the photos were taken because the photos are obtained "through theft, hacking, hidden cameras, or recorded sexual abuse" or through deepfake technology.[40] Deepfake technology "uses a form of artificial intelligence called deep learning to make images of fake events" and can

---

28. *See id.*
29. *See* Carter, *supra* note 23.
30. *See* Walsh, *supra* note 1.
31. *See* Kristen Zaleski, *The Long Trauma of Revenge Porn*, OXFORD U. PRESS BLOG (Sept. 22, 2019), https://blog.oup.com/2019/09/the-long-trauma-of-revenge-porn/ [https://perma.cc/DK99-6TMC].
32. *See* Image-based Sexual Abuse, *supra* note 26.
33. *See* Asia A. Eaton et al., *The Relationship Between Sextortion During COVID-19 and Pre-pandemic Intimate Partner Violence: A Large Study of Victimization Among Diverse U.S. Men and Women*, VICTIMS & OFFENDERS (Jan. 30, 2022), https://doi.org/10.1080/15564886.2021.2022057 [https://perma.cc/H5JY-8AAZ].
34. *Id.*
35. *See id.* at 2-3.
36. *See id.*
37. *See id.*
38. *See* Rise of Sextortion, *supra* note 4.
39. *Id.*
40. *Frequently Asked Questions*, CYBER C.R. INITIATIVE, https://cybercivilrights.org/faqs/ [https://perma.cc/U48M-RRVR] (choose from the dropdown "Shouldn't people just stop creating or sharing intimate pictures of themselves?") (last visited Jan. 25, 2024) [hereinafter *Cyber Civil Rights FAQ*].

further exacerbate the growth of image-based abuse.[41] Individuals who have never taken intimate images can become victims of image-based abuse as a result of this technology because the perpetrator can use images and videos victims have posted on their personal pages and morph them to create pornographic content without their consent.[42] Deepfake technology has even become a weapon used in politics to create and spread false information under the guise of trusted sources.[43] As a result, there is a growing fear that deepfake technology will become a new weapon for perpetrators of revenge porn and sextortion because it can and will expand the amount of potential victims of image-based abuse.[44]

B. The Current Legal Frameworks on Image-Based Abuse

Technological abuse is an ever-growing problem with no signs of slowing down.[45] On the federal level, a statutory framework that has been implemented with the goal of combatting domestic violence and violent acts against women is the VAWA.[46] States and territories of the United States have adopted statutes in order to address technology-facilitated domestic violence and to provide victims with causes of actions for the cybercrimes of revenge porn and/or sextortion.[47] Currently, there is no federal law on deepfake

41. Ian Sample, *What Are Deepfakes – and How Can You Spot Them?*, GUARDIAN (Jan. 13, 2020), https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them [https://perma.cc/N3BG-54BU].

42. *See* Chenxi Wang, *Deepfakes, Revenge Porn, and the Impact on Women*, FORBES (Nov. 1, 2019), https://www.forbes.com/sites/chenxiwang/2019/11/01/deepfakes-revenge-porn-and-the-impact-on-women/?sh=157312081f53 [https://perma.cc/7L4P-348L]; *see also* Nandini Comar, *The Rise of Revenge Porn*, GARBO (Oct. 29, 2021), https://www.garbo.io/blog/revenge-porn [https://perma.cc/LT8D-7DFB]; *see also* Kate Conger & John Yoon, *Explicit Deepfake Images of Taylor Swift Elude Safeguards and Swamp Social Media*, N.Y. TIMES (Jan. 26, 2024), https://www.nytimes.com/2024/01/26/arts/music/taylor-swift-ai-fake-images.html [https://perma.cc/Q972-X8PK] (making deepfake technology, and more generally, A.I. tools has become "widely popular but have made it easier and cheaper than ever to create . . . deepfakes, which portray people doing or saying things they have never done").

43. Nick Barney & Ivy Wigmore, *What is Generative AI? Everything You Need to Know*, TECHTARGET, https://www.techtarget.com/whatis/definition/deepfake [https://perma.cc/5KFQ-B8SP] (last visited Jan. 26, 2024); *see also* Kevin Collier & Scott Wong, *Fake Biden Robocall Telling Democrats Not to Vote is Likely an AI-Generated Deepfake*, NBC NEWS (Jan. 22, 2024), https://www.nbcnews.com/tech/misinformation/joe-biden-new-hampshire-robocall-fake-voice-deep-ai-primary-rcna135120 [https://perma.cc/TC97-C3WN] (creating a pre-recorded message from a "fake President Joe Biden" that told New Hampshire voters not to vote).

44. Wang, *supra* note 42.

45. *See, e.g.*, *Image Based Abuse*, JOYFUL HEART FOUND. (citing *The Issue*, MY IMAGE MY CHOICE, https://myimagemychoice.org [https://perma.cc/46UC-JQNQ] (last visited Nov. 3, 2024)) https://www.joyfulheartfoundation.org/learn/image-based-abuse [https://perma.cc/BWU5-3JA2] (last visited Nov. 3, 2024) (increasing by 1,780% increase compared with 2019, there were 276,149 deepfake images online with a total number of 4,219,974,115 views as of January 2024).

46. *See, e.g.*, Violent Crime Control and Law Enforcement Act of 1994, H.R. 3355, 103rd Cong. (1994).

47. *See, e.g.*, D.C. CODE § 22-3053 (2024).

technology in the context of domestic violence, however some states, such as Illinois, have adopted legislation that addresses this new and growing concern.[48]

1. The Violence Against Women Act

Prior to 1994, there was an apparent rise in violent crime, specifically violent acts against women.[49] These violent acts included sexual assault, domestic violence, dating violence, and stalking.[50] There was a need for "criminal provisions and key grant programs that [would] improve the criminal and civil justice system."[51] Additionally, domestic violence was not accounted for once "abusers would cross state lines to avoid prosecution."[52]Historically, the family sphere has been viewed as a private institution, thus law enforcement was reluctant to interfere with cases of domestic violence in the interest of maintaining family privacy.[53] For example, prior to the VAWA's enactment, it was not required nor encouraged for law enforcement to adhere to protection orders filed in "other states, tribes, and territories."[54] These problems did not go unnoticed by Congress which led to the introduction of the VAWA.

a. The VAWA's Development from 1994 to Present

Finalized proposals authored by then-Senator of Delaware, Joseph Biden, and Colorado representative, Patricia Schroeder, led to the VAWA's incorporation into the U.S. Code: the Violent Crime Control and Law

48. Cassandre Coyer, *States Are Targeting Deepfake Pornography – But Not in a Uniform Way*, ALM LAW (Aug. 10, 2023), https://www.law.com/legaltechnews/2023/08/10/states-are-targeting-deepfake-pornography-but-not-in-a-uniform-way/ [https://perma.cc/T5HB-J233] (allowing victims of "digitally manipulated pornographic content" to sue for damages).

49. *See About the Office on Violence Against Women*, U.S. DEP'T JUST., OFF. ON VIOLENCE AGAINST WOMEN, https://www.justice.gov/file/29836/download [https://perma.cc/J2ET-NHSJ] (last visited Jan. 25, 2024).

50. *See id.*

51. FACT SHEET: VIOLENCE AGAINST WOMEN ACT II, CLINTON WHITE HOUSE ARCHIVE, https://clintonwhitehouse3.archives.gov/women/violence_factsheet.html [https://perma.cc/A2FD-2V2Z] (last visited Jan. 23, 2024).

52 Tara Law, *The Violence Against Women Act Was Signed 25 Years Ago. Here's How the Law Changed American Culture*, TIME (Sept. 12, 2019), https://time.com/5675029/violence-against-women-act-history-biden/ [https://perma.cc/WTP5-PFUW].

53. *See* Prince v. Massachusetts, 321 U.S. 158, 166 (1944) (stating that the private realm of family life cannot be entered by a State, notwithstanding certain exceptions); *see generally* LISA N. SACO, CONG. RSCH. SERV., R45410, THE VIOLENCE AGAINST WOMEN ACT (VAWA): HISTORICAL OVERVIEW, FUNDING, AND REAUTHORIZATION 1 (2019), https://www.everycrsreport.com/files/20190423_R45410_672f9e33bc12ac7ff52d47a8e6bd974d96e92f02.pdf [https://perma.cc/Y4DP-A3KP].

54. *Id.*

Enforcement Act of 1994.[55] The Act brought forth tougher penalties for offenders of domestic violence and, in part, created programs "to develop and strengthen effective law enforcement and prosecution strategies to combat violent crimes against women . . . . "[56] Since 1994, the VAWA has been reauthorized four times: in 2000, 2005, 2013, and most recently in 2022.[57] Reauthorization entails changes to a particular act, in this case the VAWA, in which the Act is subject to additions and deletions.[58] The 2000 and 2005 reauthorizations contained no mention of technological abuse or the dissemination of intimate images.[59] The 2013 reauthorization arguably "close[d] critical gaps in services and justice" and acknowledged the role technology plays with domestic violence.[60] In regard to violent crimes on school campuses, the reauthorization stated that sexual assault and stalking can be committed through the use of technology.[61] Ultimately, despite the inclusion of technology, there was still no mention of the unlawful dissemination of or threat to disseminate intimate images.[62] The VAWA was reauthorized in 2022 and provided survivors of domestic violence with resources such as housing and legal assistance.[63] The 2022 reauthorization updated and expanded several provisions including the increase in funding for culturally specific resources. Most notably, in this context, it included an acknowledgment of online harassment, abuse, and combats cybercrimes.[64]

---

55. *See* Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, 108 Stat. 1976 (1994); *see also* David M. Heger, *The Violence Against Women Act of 1994*, NAT'L VIOLENCE AGAINST WOMEN PREVENTION RSCH. CTR., https://mainweb-v.musc.edu/vawprevention/policy/vawa.shtml#:~:text [https://perma.cc/XU26-BP2B] (last updated Dec. 7, 2000).

56. *About the Office on Violence Against Women*, U.S. DEP'T JUST., OFF. ON VIOLENCE AGAINST WOMEN, https://www.justice.gov/ovw/stop-violence-against-women-formula-grant-program [https://perma.cc/G5W6-AZ7V] (last visited Jan. 25, 2024).

57. *See, e.g.*, Violence Against Women Act Reauthorization Act of 2022, Pub. L. No. 117-103, 136 Stat. 49 (2022).

58. *See What is Reauthorization?*, DC ADVOC. PARTNERS, https://dcpartners.iel.org/wp-content/uploads/2021/09/What-is-Reauthorization-session-6.pdf [https://perma.cc/V7WD-E2V5] (last visited Jan. 23, 2024).

59. *See* Victims of Trafficking and Violence Protection Act of 2000, H.R. 3244, 106th Cong. (2000); *see also* Violence Against Women and Department of Justice Reauthorization Act of 2005, H.R. 3402, 109th Cong. (2005).

60. *VAWA 2013 Reauthorization*, NAT'L NETWORK TO END DOMESTIC VIOLENCE, https://nnedv.org/content/vawa-2013-reauthorization/ [https://perma.cc/CPV2-S7U7] (last visited Nov. 4, 2024); *see also* Violence Against Women Reauthorization Act of 2013, S. 47, 113th Cong. § 303(2)(A)(ii) (2013).

61. *See* Violence Against Women Reauthorization Act of 2013, Pub. L. No. 113-4, 127 Stat. 87 (2013) (codified at § 303(2)(b)(A) (2013)).

62. *See id.* § 303.

63. Statement, The White House, Fact Sheet: Biden-Harris Administration Celebrates the Twenty-Ninth Anniversary of the Violence Against Women Act (Sept. 13, 2023) (on file with author) [hereinafter 2023 White House VAWA Fact Sheet], https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/13/fact-sheet-biden-harris-administration-celebrates-the-twenty-ninth-anniversary-of-the-violence-against-women-act/ [https://perma.cc/DY4W-WZED].

64. *See id.*

b. Revenge Porn in the VAWA

The 2022 reauthorization added provisions concerning image-based abuse "to address cybercrime and the nonconsensual dissemination of intimate pictures."[65] Under Title 15 U.S.C. § 6851(b)(1)(A), a victim of nonconsensual pornography has a right to a civil action.[66] The statute states that "an individual whose intimate visual depiction is disclosed . . . without the consent of the individual, where such disclosure was made by a person who knows that, or recklessly disregards whether, the individual has not consented to such disclosure, may bring a *civil* action against that person in an appropriate district court" (emphasis added).[67] A victim can recover actual or liquidated damages in the amount of $150,000.[68] Under the court's discretion, a victim may attain "a temporary restraining order, a preliminary injunction, or a permanent injunction ordering the defendant to cease display or disclosure of the visual depiction."[69] The statute further acknowledges that victims to nonconsensual pornography can be children; therefore, "in the case of an individual who is under 18 years of age . . . the legal guardian of the individual . . . may assume the identifiable individual's rights."[70] Finally, the victim may be provided a pseudonym in order to maintain their confidentially through injunctive relief granted by the court.[71]

Ultimately, victims of nonconsensual pornography are now able to pursue civil actions against perpetrators; however, neither the VAWA or any other federal legislation qualify revenge porn as a federal crime. For revenge porn to be prosecuted on the federal level, other avenues must be taken, such as through the stalking or harassment laws, depending on the facts and conduct of the case.[72]

c. The VAWA Makes No Mention of Sextortion

Despite there being a federal civil remedy for revenge porn—the actual dissemination and disclosure of intimate images—the VAWA does not address sextortion—the *threat* to disseminate or disclose intimate images.[73] In fact, there is no mention of sextortion at all.[74] A victim of sextortion is unable to turn to the VAWA for a cause of action, nor can they turn to another

---

65. EMILY J. HANSON, CONG. RSCH. SERV., R47570, THE 2022 VIOLENCE AGAINST WOMEN ACT (VAWA) REAUTHORIZATION 2 (2023), https://crsreports.congress.gov/product/pdf/R/R47570/2 [https://perma.cc/P4SD-X32W]; *see also* 2023 White House VAWA Fact Sheet, *supra* note 63.

66. *See generally* 15 U.S.C. § 6851(b)(1)(A).

67. *Id.*

68. *Id.* § 6851(b)(3)(A)(i).

69. *Id.* § 6581(b)(3)(A)(ii).

70. *Id.* § 6581(b)(1)(B).

71. *Id.* § 6581(b)(3)(B).

72. *See* Janet Portman, *Revenge Porn: Laws + Penalties*, CRIMINALDEFENSELAWYER, https://www.criminaldefenselawyer.com/resources/revenge-porn-laws-penalties.htm [https://perma.cc/Q6JP-H7YY] (last updated Oct. 18, 2023).

73. *See* Violence Against Women Act Reauthorization Act of 2022, Pub. L. No. 117-103, 136 Stat. 49 (2022).

74. *See generally id.*

federal law that *specifically* addresses "sextortion."[75] To successfully prosecute sextortion cases that do not involve children, other federal statutes must be utilized as there's no "on-point federal law that covers the sexual elements of sextortion."[76] Different facts will lead prosecutors to different statutes which results in "different penalties" that require different elements to be proven.[77] Hence, the prosecution of sextortion cases is inconsistent.[78]

Generally with sextortion cases, prosecutors may turn to the federal interstate extortion statute which provides four possible avenues for extortion victims.[79] Seemingly, out of the four avenues, victims of sextortion can only go through one avenue: the perpetrator being fined, imprisoned for not more than two years, or both.[80] If the victim has experienced highly targeted attacks, a prosecutor may turn to the federal stalking law, which sentences a perpetrator up to five years in prison and a fine depending on the severity of the crime.[81] Some cases may even involve a perpetrator who hacked into the victim's social media accounts, thus leading a prosecutor to "the Computer Fraud and Abuse Act, the identity theft law, or both."[82]

d. The VAWA Makes No Mention of Image-Based Abuse Created with Deepfake Technology

The VAWA does not address image-based abuse perpetrated with deep fake technology nor does it provide any protections for those who experience the disclosure of fake intimate images created with deepfake technology.[83] Like with "general" revenge porn and sextortion, revenge porn and sextortion via deepfake technology will likely have to be prosecuted with other federal statutes if the facts of the case allow it, *i.e.*, laws covering extortion, identity

75. *Sextortion – Should It Be a Federal Crime?*, HG.ORG, https://www.hg.org/legal-articles/sextortion-should-it-be-a-federal-crime-53756 [https://perma.cc/UX3P-LZAH] (last visited Jan. 23, 2024).

76. Benjamin Wittes et al., *Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault*, CTR. FOR TECH. INNOVATION BROOKINGS INST. (May 11, 2016), https://www.brookings.edu/articles/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/ [https://perma.cc/LL63-TVP4].

77. *Id.*

78. *Id.*

79. *See* 18 U.S.C. § 875.

80. *See id.* § 875(d).

81. *See* 18 U.S.C. § 2261A; *see also* Wittes et al., *supra* note 75 (addressing sextortion cases leads prosecutors to potentially turn to stalking statutes when the perpetrator is highly targeting the victim such as when a former partner who cannot walk away let go of the relationship or "someone with pathological obsession with a particular victim"); *see* 18 U.S.C. § 2661(b)(5).

82. Wittes et al., *supra* note 76; *see also* 18 U.S.C. § 1030; *see also* 18 U.S.C. § 1028A.

83. *See* Press Release, Congressman Joseph Morelle, Congressman Joe Morelle Authors Legislation to Make AI-Generated Deepfakes Illegal (May 5, 2023) (on file with author), https://morelle.house.gov/media/press-releases/congressman-joe-morelle-authors-legislation-make-ai-generated-deepfakes [https://perma.cc/6BRM-C5GL].

theft, and stalking.[84] Additionally, a perpetrator can be sued "using a variety of legal theories" such as defamation, false light claims, and violation of publicity rights.[85]

C. Current Federal Reform Efforts Addressing Image-Based Abuse

Legislators have noticed that Congress has effectively left gaps in its current statutory framework. The VAWA has fallen flat in fulfilling its object and purpose of combatting violent acts against women by failing to provide adequate remedies for victims of image-based abuse. To address this failure, some legislators have proposed bills to combat the new means of technological abuse. Two recent examples of bills that attempted to fill in the gaps left by Congress were proposed by U.S. Senators Amy Klobuchar and John Cornyn (the SHIELD Act), and Congressman Joseph Morelle (the PDII Act).[86]

1. Understanding the Stopping Harmful Image Exploitation and Limiting Distribution Act of 2023

The growing issue of image-based sexual abuse has not gone unnoticed. There have been repeated efforts on the federal level to "establish . . . federal criminal liability for [perpetrators] who distribute others' private or explicit images online without consent."[87] In 2023, U.S. Senators Amy Klobuchar and John Cornyn introduced bipartisan legislation to address and combat this prevailing issue of image-based sexual abuse: the SHIELD Act.[88] The SHIELD Act would have complemented the VAWA and provided criminal penalties for revenge porn.[89] If the SHIELD Act had been adopted, an individual who knowingly mailed or distributed an intimate visual depiction of another individual "using any means or facility of interstate or foreign commerce or affecting interstate or foreign commerce" would've been in violation of the Act.[90] Additionally, it would've been unlawful to mail or distribute an intimate visual depiction of an individual with knowledge of or reckless disregard for the lack of consent of the individual to the distribution[91]

---

84. *See generally* Adam Dodge et al., *Using Fake Video Technology to Perpetuate Intimate Partner Abuse*, DOMESTIC VIOLENCE ADVISORY, https://www.cpedv.org/sites/main/files/webform/deepfake_domestic_violence_advisory.pdf [https://perma.cc/PK7B-ZZDY] (last visited Jan. 25, 2024).

85. *Id.* at 7.

86. *See* News Release, Sen. Amy Klobuchar, Klobuchar, Cornyn Introduce Bipartisan Legislation to Address Online Exploitation of Private Images (Feb. 28, 2023) https://www.klobuchar.senate.gov/public/index.cfm/2023/2/klobuchar-cornyn-introduce-bipartisan-legislation-to-address-online-exploitation-of-private-images [https://perma.cc/7JNQ-F5CK]; *see also* Morelle, *supra* note 83.

87. Klobuchar, *supra* note 86; *see also* S. 412. *See generally* H.R. 3106.

88. Klobuchar, *supra* note 86; *see also* S. 412.

89. *See* S. 412 § 1802(c)(1).

90. *Id.* § 1802(b)(1).

91. *See id.* § 1802(b)(1)(A).

where the content "was not voluntarily exposed by the individual in a public or commercial setting"[92] or where the content "is not a matter of public concern."[93] In the case that the person depicted consented to the *creation* of the depiction, it could not have been said that they also consented to the *distribution* of the depiction.[94] As a result, the individual who mailed or distributed the depiction would have been subject to a fine, "imprisoned not more than 5 years, or both."[95] Restitution would have also been available as a reparation for the victim.[96]

Additionally, the SHIELD Act would have provided a criminal remedy in addition to existing civil remedies to victims of sextortion.[97] Any person who threatened to commit an offense under the Act—knowingly mailing or distributing an intimate visual depiction of an individual—would've faced a fine, imprisonment of no more than 5 years, or both.[98] Furthermore, violators of the SHIELD Act would have faced civil forfeiture in which any distributed material, interest in property, and personal property "used, or intended to be used . . . to commit or to facilitate the commission of such violation" would have been required to be forfeited to the government.[99]

2. Understanding the Preventing Deepfakes of Intimate Images Act

Another form of legislation that has been introduced to provide adequate remedies for victims of image-based abuse is the PDII Act.[100] Congressman Joseph Morelle, a representative for New York, authored the PDII Act to "protect the right to privacy online amid a rise of artificial intelligence and digitally-manipulated content."[101] Congressman Morelle stated that "it's critical we take proactive steps to combat the spread of disinformation and protect individuals from compromising situations online."[102] The PDII Act would have added a section to the VAWA discussing the disclosure of intimate images.[103]

Currently, the VAWA has one section that discusses the disclosure of intimate images.[104] The section defines a "depicted individual" as "an individual whose body appears in whole or in part in an intimate visual depiction and who is identifiable . . . . "[105] The PDII Act would have added a separate section following Section 1309 of the VAWA, to address the

92. *Id.* § 1802(b)(1)(B).
93. *Id.* § 1802(b)(1)(C).
94. *See id.* § 1802(b).
95. 170 CONG. REC. S4338-39 (daily ed. July 10, 2024) (statement of Sen. Peter Welch).
96. *See* S. 412 § 1802(c)(3).
97. *See id.* § 1802(e); *see* 170 Cong. Rec. S 4338-39 (2024).
98. *See* 170 Cong. Rec. S 4338-39 (2024).
99. *See* S. 412 § 1802(c)(2); *see also* 18 U.S.C. § 981.
100. H.R. 3106.
101. Morelle, *supra* note 83.
102. *Id.*
103. *See* H.R. 3106 § 2.
104. *See* Consolidated Appropriations Act, H.R. 2471, 117th Cong. § 1309 (2022).
105. *Id.* § 1309(a)(3).

"disclosure of intimate digital depictions."[106] This section would have supplemented the definition of a "depicted individual," adding that a depicted individual as it relates to this section, is "an individual who, as a result of digitization or by means of digital manipulation, appears in whole or in part in an intimate digital depiction and who is identifiable."[107]

Like the VAWA's section on the disclosure of intimate images, an individual whose intimate digital depictions have been disclosed without their consent may bring a civil action under the PDII Act.[108] However, under the PDII Act, the perpetrator would be subject to a fine or imprisonment of not more than 2 years.[109] The PDII also would have addressed the growing issue with deepfake technology as it pertains to politics, providing for a criminal action where a perpetrator could have faced a fine and/or 10 years of imprisonment if the violation could be "reasonably expected to affect the conduct of any administrative, legislative, or judicial proceeding of a Federal, State, local, or Tribal government agency, including the administration of an election or the conduct of foreign relations; or facilitate violence."[110]

D. Current State Legislation Targeting Image-Based Abuse

As previously stated, victims of revenge porn and sextortion do not currently have a criminal remedy, and victims of sextortion do not have a civil cause of action on the federal level. Similarly, victims of image-based abuse derived from deepfake technology do not have a civil or criminal remedy on the federal level. Slowly but surely, states have been working towards implementing statutes to address the inadequacies of remedies on the federal law by providing victims of image-based abuse with a civil and/or criminal remedy.

1. State Legislation on Revenge Porn

Forty-nine states plus the District of Columbia ("D.C."), Puerto Rico, and Guam have criminalized revenge porn.[111] The only state that has not enacted a statute to criminalize revenge porn is South Carolina.[112] In the District of Columbia, it is unlawful "for a person to knowingly publish one or more sexual images of another identified or identifiable person, whether obtained directly from the person or from a third party or other source, when: (1) [t]he person depicted did not consent to the publication of the sexual image; (2) [t]he person publishing the sexual image knew or consciously disregarded a substantial and unjustifiable risk that the person depicted did

106. H.R. 3106 § 1309A.
107. *Id.* § 1309A(a)(2).
108. *See id.* § 1309A(b)(1).
109. *See id.* § 1309A(d).
110. *Id.* § 2252D(2)(b)(2).
111. *See Nonconsensual Distribution of Intimate Images*, CYBER C.R. INITIATIVE, https://cybercivilrights.org/nonconsensual-distribution-of-intimate-images/ [https://perma.cc/VSQ3-25HB] (last visited Nov. 4, 2024).
112. *Id.*

not consent to the publication; and (3) [t]he person published the sexual image with the intent to harm the person depicted or to receive financial gain."[113] If found in violation of this code, the perpetrator would be found guilty of a felony and can be fined, imprisoned for no more than 3 years, or both.[114] In Texas, if the perpetrator disseminates images with the intent to cause harm; is aware that the person depicted had a reasonable expectation that the images would remain private; the disclosure of the images actually causes harm; or the images reveal the identity of the depicted person; then they have committed a state jail felony.[115] Thus, different states have set forth different frameworks in order to combat revenge porn.

2. State Legislation on Sextortion

As to sextortion, currently, twenty-eight states and D.C. have enacted sextortion laws.[116] In spite of not having a statute that criminalizes revenge porn, South Carolina does have a statute that criminalizes sextortion.[117] In South Carolina, an individual who "intentionally and maliciously threatens to release, exhibit, or distribute a private image of another in order to compel or attempt to compel the victim to do any act or refrain from doing any act against [their] will, with the intent to obtain additional private images or anything else of value," must be imprisoned.[118] The length of imprisonment depends on whether the act was a first offense or not.[119] Florida has a more general statute that addresses threats and extortion;[120] A person commits a second degree felony if they "either verbally or by written or printed communication, maliciously threatens" to accuse someone of another crime or offense; threatens an injury to another; or to expose or disgrace another with the intent to extort money or any act.[121] States including New Mexico, North Carolina, and Massachusetts are silent on sexual extortion.[122]

3. State Legislation Addressing Image-Based Abuse Facilitated by Deepfake Technology

The use of deepfake technology for facilitating domestic violence is a relatively new phenomenon. Despite its newer occurrence, states such as Texas and Virginia have begun to enact state legislation addressing the

113. *See Sextortion Laws*, CYBER CIV. RTS. INITIATIVE, https://cybercivilrights.org/sextortion-laws/ [https://perma.cc/2Y54-QNT2] (last visited Nov. 12, 2023).

114. *Id.* § 22-3053(b).

115. *See* TEX. PENAL CODE ANN. § 21.16(b) (West 2019); *see also* TEX. PENAL CODE ANN. § 12.35 (West 2023) (being guilty of a state jail felony can lead to an individual to receive a term of confinement in a state jail for not more than 2 years or less than 180 days).

116. *See* Sextortion Laws, *supra* note 122.

117. *See id.*

118. S.C. CODE ANN. § 16-15-430 (2023).

119. *See id.*

120. *See generally* FLA. STAT. § 836.05 (2023).

121. *Id.* § 836.05(1).

122. *See* Sextortion Laws, *supra* note 122.

growing concerns on image-based abuse created with deepfake technology.[123] The Texas Penal Code has a section covering the "Unlawful Production or Distribution of Certain Sexually Explicit Videos."[124] It states that it is a misdemeanor if a person "knowingly produces or distributes by electronic means a deep fake video that appears to depict the person with the person's intimate parts exposed or engaged in sexual conduct."[125] Virginia has similar legislation which states that it is a misdemeanor if a person who intends "to coerce, harass, or intimidate, maliciously disseminates or sells" a video or image that depicts a person's intimate parts without their consent or authorization.[126] This misdemeanor also covers a perpetrator who has released intimate images of a person "whose image was used in creating, adapting, or modifying a [video or image] with the intent to depict an actual person and who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic;"[127] therefore covering the concern of deepfake technology.

III. ANALYSIS

Who is Congress really punishing? Before 1994, it was clear that women were confronted with violent acts such as domestic violence, sexual assault, and stalking, without any defense.[128] Thirty years later, women are still defenseless against image-based abuse because the structures in place that are supposed to protect women from domestic violence have not sufficiently kept pace with modern technology. Congress may have made two steps forward in including technological abuse as a form of domestic violence, but it has made a step back with the VAWA's failure to address sextortion or image-based abuse created through deepfake technology.[129] States have attempted to fill in these gaps, however, with only some states addressing image-based abuse and their differing laws, there is an overall lack of consistency for victims. Legislators have also attempted to fill in the gaps with the SHIELD and PDII Acts, both which were never passed. Technology will continue to "evolve and permeate our society" and it will not stop.[130] Therefore, Congress must make a change to provide a uniform law that all victims of image-based abuse can turn to.

Part A will discuss the need for the VAWA to evolve with the current age of the Internet and why Congress should seriously consider updating the VAWA to include the appropriate civil and criminal remedies for victims of image-based abuse. Part B will cover why Congress should consider adopting legislation that contains language similar to the SHIELD and PDII Acts. Finally, at the conclusion of this section it will become clear that the language

123. *See* Coyer, *supra* note 48.
124. TEX. PENAL CODE ANN. § 21.165 (West 2023).
125. *Id.* § 21.165(b)-(c).
126. VA. CODE ANN. § 18.2-386.2 (West 2024).
127. *Id.*
128. *See* U.S. DEP'T JUST., OFF. ON VIOLENCE AGAINST WOMEN, *supra* note 49.
129. *See* 2023 White House VAWA Fact Sheet, *supra* note 63.
130. Morelle, *supra* note 83; *see also* Klobuchar, *supra* note 86.

of current statutory frameworks does not encompass what women are currently experiencing today. Therefore, adopting language and/or provisions from both Acts will complement the VAWA, allowing the statute to meet its goal of protecting woman from violent acts such as domestic violence.

A. Congress Should Reauthorize the VAWA to Include Appropriate Civil and Criminal Remedies to Combat the Growth of Image-Based Abuse

The current statutory framework in place by Congress does not comport with today's reality that image-based abuse is an increasingly prolific way to facilitate domestic violence.[131] The VAWA must be reauthorized to provide adequate protections to victims of image-based abuse. The VAWA was created to combat violent acts against women; and back when it was first enacted, the violent acts toward women were primarily physical and verbal abuse such as sexual assault, domestic abuse, dating violence, and stalking—it is why the VAWA in 1994 focused on those particular acts.[132] Today, the VAWA has acknowledged that domestic violence does include technological abuse, but it is still missing essential provisions to protect women from how technological abuse is being effectuated.[133] There needs to be a criminal remedy for victims of revenge porn and a civil and criminal remedy for victims of sextortion and image-based abuse created with deepfake technology.

Again, the issue of technological abuse has not gone unnoticed. Legislators have attempted to combat this issue in the past with the SHIELD and PDII Acts.[134] Additionally, states have taken steps toward providing victims of image-based abuse with remedies such as section 21.16(b) of the Texas Penal Code, which provides a criminal remedy for victims of revenge porn.[135] Steps are not being made by Congress to include the proper remedies for victims in the VAWA or other Acts. Therefore, the present federal-level framework is not serving its intended purpose of protecting the women of *today*: victims of technology-facilitated domestic violence.

1. What the VAWA is Missing

The 2022 VAWA reauthorization is silent on providing victims of revenge porn with a *criminal* remedy. To combat the harms of image-based abuse and protect women from their abusers, the VAWA acknowledged the reality women face with having their intimate images used against them. The VAWA was changed to provide a *civil* remedy to victims of revenge porn in which they can receive actual or liquidated damages in the amount of

131. *See, e.g.*, JOYFUL HEART FOUND., *supra* note 45.
132. *See* Heger, *supra* note 55.
133. *See* 34 U.S.C. § 12291(a)(40).
134. *See generally* S. 412; *see also* H.R. 3106.
135. *See e.g.*, TEX. PENAL CODE ANN. § 21.16(b) (West 2019); *see also* TEX. PENAL CODE ANN. § 12.35 (West 2023). *See also* Nonconsensual Distribution of Intimate Images, *supra* note 111.

$150,000,[136] as well as a temporary restraining order, a preliminary injunction, or a permanent injunction.[137]

A civil remedy alone is not only inadequate for victims, but a perfunctory attempt to provide victims of image-based abuse with justice.[138] As said by Dr. Mary Anne Franks, President and Legislative & Tech Policy Director of the Cyber Civil Rights Initiative, "[c]ivil remedies should be a complement to criminal prohibition, not a substitute for it."[139] This half-hearted attempt is evident when considered in light of the fact that conduct that affects people generally is criminalized while similar conduct that is traditionally targeted at women is not. For example, the dissemination of intimate images of an individual without their consent is not a federal crime, but credit card fraud is.[140] It is illegal to steal someone's credit card, but it is not illegal to disseminate a person's intimate images without their consent.[141] The attempt or threat to disseminate intimate images of an individual unless they provide more images or actual sexual contact is not a federal crime. But identity theft is.[142] It does not matter that the perpetrator wrongfully compromises a victim's bodily autonomy and exposes them without their consent.[143] Women's rights are consistently infringed upon without any consequences to the perpetrator.

This is not to say that civil remedies are entirely inadequate. However, providing only a civil remedy does not solve the problem. Victims should be afforded the opportunity to condemn their abusers and see them face prosecution for their actions. Providing a criminal remedy would also deter individuals from committing a true violation of an individual's bodily autonomy.[144] There are many forms of conduct that are punished by criminal law such as "theft, drug possession, [and] destruction of property."[145] Compare the harms created by these crimes with the harms created by revenge porn, sextortion, and the overall image-based abuse through deepfake technology. The harms experienced through image-based abuse, as a whole, are "far more severe, lasting, and irremediable."[146]

---

136. *See* Consolidated Appropriations Act, H.R. 2471, 117th Cong. § 1309(b)(3)(A)(i) (2022).

137. *Id.*

138. *See generally* Dr. Mary Anne Franks (@ma_franks), X (Feb. 9, 2022, 8:32 PM), https://x.com/ma_franks/status/1491585879693049862?s=20 [https://perma.cc/6Z4C-C3YG].

139. Dr. Mary Anne Franks (@ma_franks), X (Feb. 9, 2022, 8:43 PM), https://twitter.com/ma_franks/status/1491588667764359170 [https://perma.cc/6WUE-SNQS]; *see also Mary Anne Franks, J.D., D.Phil Bio*, CYBER C.R. INITIATIVE, https://cybercivilrights.org/mary-anne-franks-j-d-d-phil/ [https://perma.cc/G237-JNRV].

140. *See, e.g.*, Dr. Mary Anne Franks (@ma_franks), X (Feb. 10, 2022, 2:43 AM), https://twitter.com/ma_franks/status/1491588667764359170 [https://perma.cc/RKX2-H6SD].

141. *See* 18 U.S.C. § 1029 (criminalizing credit card fraud).

142. *See* 18 U.S.C. § 1028 (criminalizing fraud and related activity in connection with identification documents).

143. *See* Image-based Sexual Abuse, *supra* note 26.

144. *See The 2023 Shield (S. 412) Act: An Explainer*, CYBER C.R. INITIATIVE, https://cybercivilrights.org/wp-content/uploads/2023/06/May-2023-CCRI-SHIELD-Explainer.pdf [https://perma.cc/JSY5-7PBW] (last visited Nov. 11, 2023).

145. *Id.*

146. *Id.*

Again, the civil remedy provided in the VAWA only addresses the *actual* dissemination of images—revenge porn—not the attempt or threat of dissemination—sextortion, which will continue to grow with the prevalence of technology in our society.[147] A victim should not have to wait until their perpetrator actually disseminates the photos to then just be able to bring a civil action. But even just providing a civil remedy for victims of sextortion would be a step in the right direction, but again, not the *only* step that needs to be taken.[148]

The same can be said for image-based abuse victims whose images have been created by deepfake technology. There is no mention of nor remedies for revenge porn and sextortion creating with deepfake technology in federal legislation.[149] Deepfake technology is not an unfamiliar problem that only affects sexual abuse; it has also become a growing concern in the realm of politics.[150] However, image-based sexual abuse has also been exacerbated by deepfake technology.[151] Not acknowledging that these crimes can be done through fake images and videos would place many image-based abuse victims in the dark with no remedies to bring these appalling actions to light.

For now, to help victims of sextortion and image-based abuse made with deepfake technology see perpetrators face consequences for their actions, prosecutors must turn to other federal statutes such as the interstate statute, or statutes covering stalking, hacking, or identity theft.[152] The victims of these crimes should be afforded the opportunity to punish their abusers in the way they deem fit—whether by filing suit or by supporting criminal proceedings initiated by a prosecutor. Victims will continue to be unable to make this choice if Congress persists in making cursory attempts in providing them justice.

2. Congress Should Consider Incorporating Language Exhibited in the SHIELD and PDII Acts to Adequately Address Image-Based Abuse

The women of this country are ill-served by the lack of sufficient remedies for victims of image-based abuse. Congress has made it clear that it

147. *See, e.g.*, FBI, *Sextortion: A Growing Threat Preying Upon Our Nation's Teens*, FBI (Jan. 17, 2024), https://www.fbi.gov/contact-us/field-offices/sacramento/news/sextortion-a-growing-threat-preying-upon-our-nations-teens [https://perma.cc/NH79-GJFJ].

148. *See id.* (discussing how a civil remedy, similar to the one provided for revenge porn, would be an important tool to protect against broader misuse of intimate images).

149. *See generally* Violence Against Women Act Reauthorization Act of 2022, Pub. L. No. 117-103, 136 Stat. 49 (2022).

150. *See* Barney & Wigmore, *supra* note 43; *see also* Collier & Wong, *supra* note 43.

151. *See* Wang, *supra* note 42; *see also* Natasha Singer, *Teen Girls Confront an Epidemic of Deepfake Nudes in Schools*, N.Y. TIMES (Apr. 8, 2024), https://www.nytimes.com/2024/04/08/technology/deepfake-ai-nudes-westfield-high-school.html [https://perma.cc/RB9T-SYUA] ("[u]sing artificial intelligence, middle and high school students have fabricated explicit images of female classmates and shared the doctored pictures.").

152. Wittes et al., *supra* note 76.

has a goal in protecting women from violent acts.[153] However, domestic violence does not exclusively occur in the same ways as it did back in 1994. Now with the current Internet age, domestic violence can be perpetrated with the use of technology to obtain or create intimate images of a victim without their consent or knowledge. Congress needs to adapt its legislation to adequately protect the women of today. By not having clear and specific federal legislation covering revenge porn, sextortion, and image-based abuse facilitated with deepfake technology, Congress is placing a heavy burden on victims.

Congress has tried to make strides toward a change for women experiencing domestic violence, yet it continues to turn a blind eye when having to care for women who are experiencing technology-facilitated domestic violence. Addressing only a quarter of a problem only helps a quarter of the victims. Women who have their intimate images disseminated without their consent have a federal civil cause of action, but the perpetrator does not face criminal liability. Women who have threats placed above their heads that their intimate images will be disseminated without their consent unless they perform a certain act cannot seek redress in federal criminal or civil court. Women who have sexually explicit images or videos created with depictions of themselves are not victims of a federal crime.

Victims of revenge porn, sextortion, and image-based abuse facilitated with deepfake technology are forced to take alternative avenues if they want the perpetrator to face criminal or civil proceedings at the federal level. Victims hope that the facts of their case, the facts of their traumatic experience, is enough to fit under, for example, a blackmail or general extortion statute.[154] Why is Congress making it harder to prosecute these horrific crimes? Why are victims facing more challenges than the perpetrators of these crimes? As previously mentioned, these crimes are underreported, therefore victims would likely feel more empowered to report their abuse if they knew that a stronger, more concrete framework was in place to help them.

Prior to the VAWA's enaction, domestic violence was not accounted for once a domestic abuser crossed state lines.[155] Now, states are trying their best to lighten the burden on victims through legislation because states properly acknowledge that unlike before, these crimes now go even beyond physical boundaries with the Internet.[156] However, states cannot do all of the work, especially because it leads to inconsistencies in approaching image-based abuse crimes. A victim in one state may face a higher burden of proof, whereas a victim in another state will not.[157] The potential for victims to be

153. *See* About the Office on Violence Against Women, *supra* note 49.

154. *See* David Russcol, *In Latest Violence Against Women Act Reauthorization, Congress Created a Remedy for Victims of Revenge Porn*, BOS. LAW. BLOG (Aug. 11, 2023), https://www.bostonlawyerblog.com/in-latest-violence-against-women-act-reauthorization-congress-created-a-remedy-for-victims-of-revenge-porn/ [https://perma.cc/A79N-WHVY].

155. *See, e.g.*, Wittes et al., *supra* note 76.

156. *See* Cyber Civil Rights FAQ, *supra* note 40.

157. *Compare* D.C. Code § 22-3053(a)(1) (2024), *with* TEX. PENAL CODE ANN. § 21.16(b) (West 2019).

treated differently because of where they live further proves why there needs to be a clear federal law that addresses and provides civil and criminal remedies for image-based abuse.

In light of this, Congress should seriously consider adopting legislation that has elements of both the SHIELD Act and the PDII Act. We need federal legislation to make these abhorrent behaviors actionable in a federal court of law. An ideal piece of legislation that would adequately cover revenge porn, sextortion, and image-based abuse facilitated with deepfake technology, would include language similar to what is used in both Acts.

The SHIELD Act, as a model, provides not only a criminal remedy for victims of revenge porn—something the VAWA lacks—but also a civil *and* criminal remedy for victims of sextortion.[158] Using language such as: "Any person who threatens to or does knowingly mail or distribute an intimate visual depiction of an individual would face a fine, imprisonment of no more than 5 years, or both,"[159] would address both revenge porn and sextortion, thereby filling in the gaps in the VAWA. Additionally, by including and recognizing sextortion as a crime and providing victims with a civil and criminal remedy under the VAWA, states will have an incentive to adopt laws like South Carolina's.[160] A reauthorization to the VAWA should additionally include a criminal remedy for victims of revenge porn. A civil remedy alone is a subpar response to the growing prevalence of image-based abuse.

Additionally, Congress should consider adopting language that has been used in the PDII Act. In its next reauthorization, the VAWA can either include an entirely separate section, like the PDII Act does, or add onto Section 1309 of the Act to include language covering image-based abuse by deepfake technology.[161] The statute can state that to qualify as a "depicted individual," the individual's intimate images could be from the result of having been taken—either knowingly or unknowingly—or the images can be "a result of digitization or by means of digital manipulation."[162] This language would address the developing issue of deepfake technology as a method of producing sexual content without a victim's knowledge and/or consent.[163]

158. *See* S. 412.

159. *See id.* (providing an example on language that could be used in future legislation to address revenge porn and sextortion).

160. *See* S.C. CODE ANN. § 16-15-430 (2023).

161. *See* H.R. 3106 § 1309A.

162. *Id.* § 1309A(a)(2).

163. Although a constitutional analysis of a proposed law of this type is outside the scope of this Note, it must be noted that this law would likely not implicate First Amendment concerns. This type of law should not be viewed as an infringement on a person's First Amendment right, but rather a way to further a person's right to privacy. *See* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 349 (2014). Governments have a compelling interest in protecting the privacy of victims of image-based abuse. *See* John A. Humbach, *The Constitution and Revenge Porn*, 35 PACE L. REV. 215, 240 (2014). A law that would include revenge porn, sextortion, and image-based abuse facilitated with deepfake technology as federal crimes would deter individuals from committing these crimes, should pass constitutional muster, and most importantly, provide justice to victims who have been experienced a tremendous violation of their privacy.

IV. CONCLUSION

For the above reasons, Congress must make sufficient strides in providing victims of image-based abuse with adequate remedies. Many legislators and states have taken steps to further the goal of protecting women from domestic violence. Domestic violence no longer exclusively entails physical, mental, or emotional abuse. With the pervasiveness of technology and the Internet, domestic violence can now take the form of image-based abuse. Modern-day victims of domestic violence are faced with perpetrators who will disseminate intimate images or depicted intimate images of them without their consent and/or knowledge. These perpetrators have a reckless disregard for a victim's bodily autonomy and right to privacy. Prosecutors must turn to other avenues and other federal laws to bring justice to victims who have experienced irreparable harm.

This Note has attempted to uncover the concerns of the VAWA's halfhearted and incomplete attempt to address the issue of technological abuse. In not keeping pace with today's technology, its failure to criminalize revenge porn, sextortion, and image-based abuse with deepfake technology, and its lack of civil remedies for the latter two, Congress is not adequately meeting its goal of protecting women from violent acts. Many states have stepped up to the plate in allowing for criminal proceedings against perpetrators of these crimes. However, states alone cannot provide women with justice, especially when these crimes frequently cross state lines and go beyond physical boundaries with the Internet. If Congress wants to protect women from violent acts, then it needs to seriously consider adopting language that would cover the crimes discussed in this Note. If not, we must wonder: Who is Congress really punishing—the perpetrators of these crimes or their victims?

Watching and Waiting: Modern Social Media Surveillance of Immigrants and Fourth Amendment Implications

Vaishali Nambiar*

TABLE OF CONTENTS

I. INTRODUCTION 200

II. BACKGROUND 201

A. The State of Immigrant Surveillance in the United States 201

1. The U.S. Immigration System & Historical Approaches to Surveillance 202
2. The Rise of Social Media Surveillance 204
3. Categories of Social Media Surveillance 206

B. Fourth Amendment Framework 208

1. Reasonable Expectation of Privacy Test 208
2. The Third-Party Doctrine 209
3. The Border-Search Exception 211
4. Recent Trends & the Evolution of Privacy Norms Online 212

III. ANALYSIS 215

A. Why All Social Media Data Should Not be Considered Wholly "Public" 215

B. Extensive Data Collection Post-Carpenter 218

C. Is Modern Social Media Surveillance Effective? 221

IV. RECOMMENDATIONS 222

V. CONCLUSION 223

* J.D., May 2025, The George Washington University Law School; B.A. 2021 Community and Global Public Health, University of Michigan. I am deeply grateful to the late Professor Ethan Lucarelli, whose thoughtful guidance was instrumental in the development of this Note. I also extend my sincere thanks to the FCLJ Editorial Board for their dedication throughout this process. A special acknowledgment goes to Professor Daniel Solove for sparking my passion for privacy law and for his invaluable mentorship. Finally, to my parents—there are no words that could ever fully convey my appreciation for your unconditional love and support.

I. INTRODUCTION

The Internet is ubiquitous—permeating our commerce, culture, and daily life.[1] Over the last decade, technological developments have created an online world that feels like a natural extension of the physical world. Social media platforms are a major force in the online world. These platforms create an environment for online users to interact with each other, typically by way of engaging with user-generated content or private messaging features.[2] Today, there are approximately 4.9 billion social media users worldwide, and the average user now spreads their digital footprint across six to seven different platforms.[3] Essentially, social media platforms have become hubs for the massive accumulation of valuable personal data. One consequence of this is that the government often engages in surveilling social media users and collecting and analyzing their personal data; and immigrants are among the communities most significantly impacted by this issue because they tend to face increased scrutiny by law enforcement.[4]

There are various approaches to social media surveillance, and there is evidence that the government is increasingly moving towards utilizing machine learning technology and automated tools to collect and analyze social media data.[5] These tools are powerful because they make many aspects of surveillance much more efficient, allowing for quick data aggregation and analysis.[6] For example, in 2018, law enforcement was able to locate and arrest an immigrant using the pseudonym "Sid," solely by way of photos and status updates he posted on Facebook.[7] This tracking was conducted by data mining firms U.S. Immigration and Customs Enforcement ("ICE") contracted with at the time, and ultimately, Sid was "only one of thousands of individuals" ICE was tracking at that point.[8]

This Note will argue that courts are currently not reading the Fourth Amendment broadly enough to afford adequate privacy protections to immigrants against social media surveillance carried out by law enforcement.

---

1. *See* Jacob Poushter, *Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies*, PEW RSCH. CTR. (Feb. 22, 2016), https://www.pewresearch.org/global/2016/02/22/internet-access-growing-worldwide-but-remains-higher-in-advanced-economies/ [https://perma.cc/KUT2-SBHX].

2. *See* Ben Lutkevich, *What is Social Media?*, TECHTARGET, https://www.techtarget.com/whatis/definition/social-media [https://perma.cc/5FWB-6PAB] (last visited Nov. 5, 2024).

3. *See* Belle Wong, *Top Social Media Statistics and Trends of 2024*, FORBES ADVISOR (May 18, 2023, 2:09 PM), https://www.forbes.com/advisor/business/social-media-statistics/ [https://perma.cc/R4LY-W3MV].

4. *See* Nicol Turner Lee & Caitlin Chin-Rothmann, *Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color*, BROOKINGS (Apr. 12, 2022), https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ [https://perma.cc/5MLB-ENSH].

5. *See* Barton Gellman & Sam Adler-Bell, *The Disparate Impact of Surveillance*, CENTURY FOUND. (Dec. 21, 2017), https://tcf.org/content/report/disparate-impact-surveillance/ [https://perma.cc/MP7L-XW3X].

6. *See* Lee & Chin-Rothmann, *supra* note 4.

7. *See id.*

8. *Id.*

Due to the evolving nature of user expectations of privacy online and the expansive nature of modern surveillance techniques utilized by law enforcement, this Note argues that courts should adopt a more expansive view of the Fourth Amendment's protections to ensure individual privacy is protected in an increasingly digital world. This Note addresses the major contexts in which law enforcement conducts social media surveillance on immigrants: searches at the border and during visa processing.

Section I will discuss how, historically, immigrant surveillance in the United States has consistently iterated and adapted to the latest technologies of the time. This section also details the role political administrations and key federal agencies, like the U.S. Customs and Border Protection ("CBP") and ICE, have played in implementing specific surveillance initiatives over the last decade. Section II will outline major court cases that have shaped how courts understand the Fourth Amendment to protect individual privacy interests relative to governmental interests in surveillance. More specifically, this section will detail the various legal tests and doctrines, such as the reasonable expectation of privacy test and the third-party doctrine, that help courts determine whether an individual has a cognizable privacy interest. Subsequently, the Analysis section will advance the argument that immigrants maintain a reasonable expectation of privacy in their social media data and that courts should read the Fourth Amendment to recognize this privacy interest, particularly after the Supreme Court's decision in *Carpenter*. In the final section, this Note will propose legal and policy recommendations to provide more adequate protection for the privacy interests of immigrant populations.

II. BACKGROUND

A. The State of Immigrant Surveillance in the United States

This part of the Note will provide an overview of the state of immigrant surveillance in the United States. The first section will discuss methods law enforcement has historically utilized for surveillance, as well as detail the role of the Department of Homeland Security in implementing immigrant surveillance programs. Next, this Note will describe the rise of social media platforms over the last decade, and how this trend led to the creation of several surveillance initiatives during former President Trump's presidency that centered on social media data. Finally, the third section will categorize the different approaches that law enforcement agencies have taken with respect to modern social media surveillance.

1. The U.S. Immigration System & Historical Approaches to Surveillance

Immigrant populations in the United States have historically been targets of excessive government surveillance.[9] Modern approaches to the monitoring of immigrant populations can be traced back to the methods adopted by police in the 19th century to target areas of cities where high concentrations of immigrants resided.[10] In the 19th century, law enforcement utilized the new technologies of the time for surveillance, like fingerprinting, and adopted excessive data retention practices, by collecting and storing masses of files containing profiles of immigrants.[11] These surveillance approaches have only grown more powerful with technological advancements in recent years.[12] More specifically, law enforcement today leverages machine learning and AI-powered technology as part of its surveillance agenda to both collect information and enable seamless data retention and information sharing between law enforcement agencies.[13]

Today, several federal agencies handle immigration and immigrant surveillance.[14] The focus of this Note will be on the surveillance practices of the Department of Homeland Security ("DHS") and the State Department. DHS houses 16 different offices, but the two most relevant to immigrant surveillance are CBP and ICE.[15] While CBP is responsible for securing the border, ICE enforces immigration laws in non-border areas and handles detention and deportation.[16] The Department of State houses several smaller bureaus and offices, but the Bureau of Consular Affairs ("BCA") is one of the most dominant agencies in the context of immigrant surveillance, as it is the office primarily responsible for issuing United States visas and adjudicating visa applications of aliens outside the country.[17] Another important element of this structure is the Privacy and Civil Liberties Oversight Board ("PCLOB"). PCLOB is an independent agency that provides oversight to ensure there is a balance between the federal government's anti-terrorism

9. *See* Matthew Guariglia, *How the Surveillance of Immigrants Remade American Policing*, TIME (Nov. 21, 2023, 2:32 PM), https://time.com/6336882/police-surveillance-history/ [https://perma.cc/KE7A-2FRH].

10. *See id.*

11. *See id.*

12. *See generally* Faiza Patel et al., *Social Media Monitoring*, BRENNAN CTR. FOR JUST. (Mar. 11, 2020), https://www.brennancenter.org/our-work/research-reports/social-media-monitoring [https://perma.cc/G763-CJJJ].

13. *See id.*

14. *See generally* Megan Davy et al., *Who Does What in U.S. Immigration*, MIGRATION POL'Y INST. (Dec. 1, 2005), https://www.migrationpolicy.org/article/who-does-what-us-immigration [https://perma.cc/3K4T-T35Z].

15. *See Operational and Support Components*, U.S. DEP'T HOMELAND SEC., https://www.dhs.gov/operational-and-support-components [https://perma.cc/4ZPJ-8EHG] (last visited Jan. 24, 2024).

16. *See* Davy et al., *supra* note 14.

17. *See id.*; *see also Bureaus of Consular Affairs*, U.S. DEP'T OF STATE, https://www.state.gov/bureaus-offices/under-secretary-for-management/bureau-of-consular-affairs/ [https://perma.cc/LUV6-EFHD] (last visited Jan. 24, 2024).

efforts and the interests of privacy and civil liberties.[18] In 2007, Congress passed Section 803 of the Implementing Recommendations of the 9/11 Commission Act, which required eight federal law enforcement agencies—including DHS and the State Department—to issue reports to Congress and PCLOB about their work.[19] The Board regularly publishes publicly available reports detailing their activities and recommendations for various federal government surveillance issues.[20]

Though federal law enforcement agencies are responsible for the implementation of surveillance programs, over the years, political and social factors have also played a dominant role in shaping public sentiment toward immigrants and in influencing attitudes toward the monitoring of immigrant communities.[21] One of the most significant examples is the 2001 USA PATRIOT Act, which was bipartisan legislation passed after the 9/11 terrorist attacks to grant law enforcement agencies greater surveillance powers and to ease the process by which agencies could collect foreign intelligence information.[22] Another major topic defining anti-migrant rhetoric in recent years is the U.S.-Mexico border crisis.[23] The U.S.-Mexico border has been described as one of the "most politicized spaces in the country," likely in part due to invasive surveillance by law enforcement in this area.[24] Surveillance tactics employed in this area over the years include cell phone searches at the border, facial recognition technology, real-time crime analytics, and the use of drones and mobile surveillance vehicles.[25]

---

18. *See History and Mission*, U.S. PRIV. & CIV. LIBERTIES OVERSIGHT BD., https://www.pclob.gov/About/HistoryMission [https://perma.cc/8ZBR-6W4P] (last visited Jan. 24, 2024).

19. *See id.*

20. *See id.*

21. *See* Besheer Mohamed, *Muslims are a Growing Presence in U.S., but Still Face Negative Views From the Public*, PEW RSCH. CTR. (Sept. 1, 2021), https://www.pewresearch.org/short-reads/2021/09/01/muslims-are-a-growing-presence-in-u-s-but-still-face-negative-views-from-the-public/ [https://perma.cc/5V9C-MHQH] (discussing public attention on Muslim Americans after 9/11 and how Americans' view of Muslims has become increasingly polarized along political lines).

22. The key statute regulating foreign intelligence gathering within the United States is the Foreign Intelligence Surveillance Act of 1978. The Act was designed as a permissive law to allow the government to engage in foreign intelligence gathering. Under the 1978 law, law enforcement had to show the "primary purpose" of their investigation was foreign intelligence. However, after the PATRIOT Act was passed, the bar was lowered to be "significant purpose." *See Surveillance Under the USA/Patriot Act*, AM. C.L. UNION (Oct. 23, 2001), https://www.aclu.org/documents/surveillance-under-usapatriot-act [https://perma.cc/7TPC-WUTA]; *see generally EFF Analysis of the Provisions of the Provisions of the USA PATRIOT Act*, ELEC. FRONTIER FOUND. (Oct. 27, 2003), https://www.eff.org/deeplinks/2003/10/eff-analysis-provisions-usa-patriot-act [https://perma.cc/998A-A6ZW].

23. *See* Saira Hussain, *Surveillance and the U.S.-Mexico Border: 2023 Year in Review*, ELEC. FRONTIER FOUND. (Dec. 21, 2023), https://www.eff.org/deeplinks/2023/12/surveillance-and-us-mexico-border-2023-year-review [https://perma.cc/5J9M-FWUS]; *see also* Dana Khabbaz, *How CBP Uses Hacking Technology to Search International Travelers' Phones*, EPIC (Feb. 22, 2022), https://epic.org/how-cbp-uses-hacking-technology-to-search-international-travelers-phones/ [https://perma.cc/DL84-JQQ5].

24. Hussain, *supra* note 23.

25. *See id.*

2. The Rise of Social Media Surveillance

As discussed in the Introduction, there are almost 5 billion social media users worldwide. Social media companies have become a mainstay in people's lives, perhaps because they have continued to expand beyond their original use of giving users a public forum for interaction.[26] For example, platforms like X (formerly Twitter) or Reddit fall under the label of "social media" but are often used by individuals as a means for passive news gathering rather than public interaction.[27] Another example is TikTok, where many individuals create accounts solely as a means for consuming entertaining content that the algorithm feeds them rather than engaging with people they know in their real lives.[28] Ultimately, as social media continues to sustain the attention of individuals, more valuable personal data accumulates on these platforms—evidenced by the rise of targeted advertisers on social media platforms hoping to capitalize.[29]

There have been several efforts over the years to capitalize on the valuable data available on social media and implement social media monitoring programs, particularly during the Trump administration.[30] Former President Donald Trump's presidency was marked by anti-migration policies targeting persons entering through the U.S.-Mexico border and initiatives like "The Muslim Ban" that received widespread criticism from immigrant rights activists.[31] With respect to monitoring specifically, President Trump actively endorsed several new immigrant surveillance efforts by agencies like DHS and the State Department between 2017–2019.[32] For example, as part of the "Muslim Ban" executive orders, the State Department issued an emergency notice in May 2017 to increase screening and information collection by requiring visa applicants to provide a list of social media identifiers they had used within the previous 5 years.[33]

A critical turning point in law enforcement's approach to social media surveillance came in July 2017 when ICE announced it was searching for data-mining firms to implement a monitoring program driven by automated

---

26. Katie Fleeman, *Social Media and Reader Engagement*, KNIGHT SCI. JOURNALISM, https://ksjhandbook.org/social-media-reader-engagement/different-platforms-different-audiences/ [https://perma.cc/9HLE-RUS4] (last visited Mar. 3, 2024).

27. *Id.*

28. *See* Mostafa ElBermawy, *Social Media is Dead: From Connection to Consumption*, NOGOOD (July 27, 2022), https://nogood.io/2022/07/27/social-media-is-dead/ [https://perma.cc/U492-UGQG].

29. *See* Nik Froehlich, *The Truth in User Privacy and Targeted Ads*, FORBES (Feb. 25, 2022, 9:29 AM), https://www.forbes.com/sites/forbestechcouncil/2022/02/24/the-truth-in-user-privacy-and-targeted-ads/?sh=6c40c8bc355e [https://perma.cc/X9VJ-9PCV].

30. *See Social Media Surveillance*, ASIAN AMS. ADVANCING JUST. 1 (Feb. 11, 2020), https://www.advancingjustice-aajc.org/sites/default/files/2020-02/Social%20Media%20Surveillance%20Backgrounder.pdf [https://perma.cc/X827-AWU5].

31. Adam Isacson et al., *Putting the U.S.-Mexico 'Border Crisis' Narrative into Context*, WASH. OFF. ON LAT. AM. (Mar. 17, 2021), https://www.wola.org/analysis/putting-border-crisis-narrative-into-context-2021/ [https://perma.cc/5P53-VV6H].

32. *See Social Media Surveillance*, *supra* note 30.

33. *See id.*

technology. [34] The "Extreme Vetting Initiative Program" proposed to constantly monitor social media posts by U.S. visitors and "streamline the current manual vetting process while simultaneously making determinations via automation if the data retrieved is actionable."[35] However, after receiving strong public pushback, ICE withdrew the proposal and rebranded the program as the "Visa Lifecycle Vetting Initiative" ("VLVI").[36] Through the VLVI, in June 2018, ICE spent $100 million to hire 180 people to continuously monitor 10,000 foreign visitors flagged as high-risk.[37]

Despite the seeming shift back to a human-driven decision-making process, concerns still remain. In February 2018, President Trump announced the establishment of a "National Vetting Enterprise" ("NVE") within the DHS' National Vetting Center ("NVC").[38] NVC's stated mission is to streamline intelligence information sharing between agencies to "ensure that immigration and border security decisions are fully informed and accurately implemented."[39] Some critics note that the establishment of the NVE, taken along with DHS rhetoric and directives, seems to suggest a "persistent interest in incorporating machine learning technology in the future in immigration vetting functions."[40]

This is a troubling issue because several machine learning-driven tools employed by DHS are not capable of accurately analyzing users posts.[41] For example, "algorithmic tone and sentiment" analytics, which try to uncover user sentiments and beliefs from their posts, were only found to make accurate predictions of users' political ideologies on Twitter 27% of the time.[42] The problem only compounds when tools analyze user posts that are in different languages and nonstandard dialects.[43]

A separate issue with these initiatives is that many of them have been rolled out as pilot programs.[44] As a result, there is little publicly released

---

34. *See* Sam Biddle & Spencer Woodman, *These are the Technology Firms Lining Up to Build Trump's "Extreme Vetting" Program*, INTERCEPT (Aug. 7, 2017, 1:45 PM), https://theintercept.com/2017/08/07/these-are-the-technology-firms-lining-up-to-build-trumps-extreme-vetting-program/ [https://perma.cc/T29S-6B4V].

35. *See id.*; *see also* George Joseph & Kenneth Lipp, *How ICE is Using Big Data to Carry Out Trump's Anti-Immigrant Crusade*, SPLINTER NEWS (Aug. 11, 2017, 6:30 PM), https://splinternews.com/how-ice-is-using-big-data-to-carry-out-trumps-anti-immi-1797745578 [https://perma.cc/4GQF-37BC].

36. Patel et al., *supra* note 12.

37. *See id.*

38. Chinmayi Sharma, *The National Vetting Enterprise: Artificial Intelligence and Immigration Enforcement*, LAWFARE (Jan. 8, 2019, 9:00 AM), https://www.lawfaremedia.org/article/national-vetting-enterprise-artificial-intelligence-and-immigration-enforcement [https://perma.cc/E5KB-PTYP].

39. *National Vetting Center FAQs*, U.S. CUSTOMS & BORDER PROT., https://www.cbp.gov/border-security/ports-entry/national-vetting-center [https://perma.cc/JQ9K-UY8M] (last visited Jan. 24, 2024).

40. Sharma, *supra* note 38.

41. *See* Patel et al., *supra* note 12.

42. *Id.*

43. *See id.*

44. Patel et al., *supra* note 12, at 26.

information about program implementation or success.[45] The most recent guidance discussing these measures seems to be a 2016 report from the DHS Office of the Inspector General ("OIG") about ICE's use of social media monitoring during the visa issuance process. In that report, the DHS OIG found that ICE pilot programs, including those involving automated searches, lacked adequate metrics for measuring efficacy.[46] Further, the report recommended that USCIS and ICE create a plan with more "well-defined, clear, and measurable objectives and standards for determining pilot performance."[47] With respect to other surveillance programs, recent documents obtained by the Knight First Amendment Institute from the Office of the Director of National Intelligence ("ODNI"), the head agency overseeing the U.S. intelligence community, reveal ODNI staff acknowledging that the collection of social media identifiers are "useless" to the immigration screening process.[48]

3. Categories of Social Media Surveillance

Aside from pilot programs, there are three common methods of social media monitoring that law enforcement agencies utilize. First, government agencies often purchase data from private surveillance companies.[49] Government agencies like ICE and CBP have a history of contracting with data mining firms for assistance in collecting and analyzing social media data.[50] For example, CBP contracted with data mining firm Palantir to design a framework that identified non-obvious links between individuals based on a variety of information, including social media data.[51] Another example is ICE's partnership with data mining firm, Giant Oak, for support on a surveillance program implementing continuous monitoring for immigrants under the agency's visa applicant screening program.[52] Through the partnership, Giant Oak supplied ICE with the "Giant Oak Search Technology

45. *See id.*

46. *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success*, U.S. DEP'T HOMELAND SEC. (Feb. 27, 2017), https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf [https://perma.cc/MSS3-ZULT] [hereinafter *DHS Social Media Screening*].

47. *Id.*

48. *See State Department Rule Requiring Visa Applicants to Register Their Social Media Handles is Ineffective New Documents Say*, KNIGHT FIRST AMEND. INST. (Oct. 5, 2023), https://knightcolumbia.org/content/state-department-rule-requiring-visa-applicants-to-register-their-social-media-handles-is-ineffective-new-documents-say [https://perma.cc/W7Z5-CUC7] [hereinafter *State Department Rule Ineffective*].

49. *See Social Media Surveillance*, *supra* note 30; *see* Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*, ELEC. FRONTIER FOUND. (Dec. 2, 2019), https://www.eff.org/wp/behind-the-one-way-mirror#Data-brokers [https://perma.cc/4WWG-2TAW] (explaining that "data broker" is a broad term, but it often refers to firms that purchase and assemble data from a variety of smaller companies and streams to eventually sell).

50. *See Social Media Surveillance*, *supra* note 30.

51. *See id.*

52. *See id.*

System" ("GOST").[53] GOST provides "behavioral-based [I]nternet search capabilities," enabling analysts to review an individual's social media profile, provide a social graph of their connections, and assigns them a rating—"thumbs up" or "thumbs down."[54]

Another approach to monitoring is the government's collection of social media data through visa applications, like the DS-160 and DS-260.[55] Before Trump took office in January 2017, DHS had already started implementing a process of requesting foreign travelers arriving through the Visa Waiver Program to voluntarily provide their social media handles.[56] These forms request visa applicants to voluntarily provide their social media usernames for any social media accounts they have owned in the preceding 5 years.[57] The information applicants provide on these applications is compared against other DHS databases, and a copy of their application is stored in CBP's Automated Targeting System ("ATS").[58]

The third category of social media monitoring is through searches occurring at the border. Here, typically, ICE extracts social media data from electronic devices during the course of a border search.[59] Afterward, ICE may use its analytical tool, the FALCON Search & Analysis System ("FALCON-SA"), to analyze the collected social media data and generate reports to inform agency decision-making and strategy.[60] Some of the tool's analytical capabilities include presenting relationships between different entities and people, graphical depictions of the chronology in which events occurred, and geospatial placement of entities or events on a map.[61] Particularly concerning is the fact that once extracted and analyzed, the collected data can also be stored and shared across other law enforcement agencies.[62]

---

53. Joseph Cox, *Inside ICE's Database for Finding "Derogatory" Online Speech*, 404 MEDIA (Oct. 24, 2023, 9:00 AM), https://www.404media.co/inside-ices-database-derogatory-information-giant-oak-gost/ [https://perma.cc/4LQ2-5P6M].

54. *Id.* (quoting a GOST user guide).

55. *See Social Media Surveillance*, *supra* note 30.

56. *See id.* (the Visa Waiver Program is a program allowing "citizens of 38 countries to travel and stay up to 90 days without a visa").

57. *See id.*

58. *See* DHS/U.S. Customs and Border Protection (CBP)–009 Electronic System for Travel Authorization (ESTA) System of Records, 81 Fed. Reg. 39680, 39681 (June 17, 2016); *see also* U.S. DEP'T HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM at 94 (2017) https://www.dhs.gov/sites/default/files/2022-07/privacy-pia-cbp006-ats-july2022_0.pdf [https://perma.cc/VC39-EGPA] ("ATS compares information about individuals entering and exiting the country . . . with other identified patterns requiring additional scrutiny based on CBP Officer experience, trend analysis of suspicious activity, law enforcement cases, and raw intelligence.").

59. *See* Patel et al., *supra* note 12, at 28.

60. *See id.*

61. *See* Jonathan R. Cantor, *Privacy Impact Assessment Update for the FALCON Search and Analysis System*, U.S. DEP'T HOMELAND SEC. (Oct. 11, 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice032b-falconsa-appendixbupdate-march2021.pdf [https://perma.cc/7XDF-AU4B].

62. *See* Patel et al., *supra* note 12, at 28.

B. Fourth Amendment Framework

This section will provide the legal framework for how the Fourth Amendment's protections are interpreted. For the Fourth Amendment to apply, the court must find that a "search" or "seizure" has occurred.[63] Under the Supreme Court's Fourth Amendment jurisprudence, a search exists where an individual has a "reasonable expectation of privacy"—an actual or subjective expectation of privacy that society is prepared to recognize as reasonable.[64] However, the Supreme Court has found an expectation of privacy is not reasonable when individuals voluntarily provide their information to third parties, like businesses and institutions.[65] Additionally, the Supreme Court has found in multiple cases that routine searches and seizures by law enforcement at the border do not offend the Fourth Amendment.[66] Applying this framework to the modern context of digital search has presented challenges, as lower courts have had to grapple with how much they are willing to recognize digital norms and expand collective notions of the "reasonable expectation of privacy."[67]

1. Reasonable Expectation of Privacy Test

The Fourth Amendment protects people from unreasonable searches and seizures by the government.[68] Moreover, any "searches deemed necessary should be as limited as possible."[69]

To determine whether there has been a search or seizure to which the Fourth Amendment applies, courts apply the "reasonable expectation of privacy test," which originates from *Katz v. United States*.[70] In *Katz*, the FBI wiretapped the outer part of a public phone booth to record the defendant's phone conversation and the prosecution attempted to enter these recordings into evidence.[71] In a landmark decision, the Supreme Court reversed the trial and appellate courts' decision to admit the recordings because it found that Katz was justified in believing that his phone conversation would remain private, though it took place in a public phone booth.[72] As noted in Justice Harlan's concurrence in *Katz*, the Court arrived at this conclusion by applying the reasonable expectation of privacy test, which asks whether a person has an actual or subjective expectation of privacy and if this expectation of privacy is one that society is prepared to recognize as reasonable.[73] If the answer to both parts is yes, then the Fourth Amendment applies.[74] Before *Katz*, Courts took a property-based approach (commonly referred to as the

63. U.S. Const. amend. IV (protecting "against unreasonable searches and seizures").
64. *See* discussion *infra* Section I.B.1.
65. *See* discussion *infra* Section I.B.2.
66. *See* discussion *infra* Section I.B.3.
67. *See* discussion *infra* Section I.B.4.
68. *See* U.S. CONST. amend. IV.
69. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).
70. *See* Katz v. United States, 389 U.S. 360, 516 (1967).
71. *See id.* at 348.
72. *See id.* at 352–53.
73. *See id.* at 516 (Harlan, J., concurring).
74. *See id.*

"physical trespass doctrine") that only recognized Fourth Amendment violations where there was a physical intrusion on one's property.[75] However, the *Katz* case marked an expansion in the Court's understanding of Fourth Amendment violations—with the Court famously writing that "the Fourth Amendment protects *people*, not places."[76]

Nonetheless, in *U.S. v. Jones*, the Supreme Court clarified that *Katz* did not replace the physical trespass doctrine with the reasonable expectation of privacy test, but rather it added to it.[77] In *Jones*, the FBI placed a GPS tracker on a defendant-suspect's vehicle to continuously track his movements for a month.[78] The government argued that the defendant could not have a reasonable expectation of privacy in his movements through public streets.[79] However, the Court rejected this argument, noting that *Katz* aside, the placement of the tracker on the vehicle was a *physical trespass* that constituted a search within the scope of the Fourth Amendment under the physical trespass doctrine.[80] The Court further reiterated that under *Katz* individuals may still retain a reasonable expectation of privacy over things that happen in public.[81]

2. The Third-Party Doctrine

In *Smith v. Maryland*, the Supreme Court created the third-party doctrine, which essentially states that people do not have a reasonable expectation of privacy in the things they voluntarily entrust to third parties.[82] In *Smith*, the police requested a telephone company to record the numbers the defendant, Smith, was dialing and used the collected evidence to charge him with a crime.[83] Smith tried to suppress the evidence on the basis of the Fourth Amendment, arguing that he had a reasonable expectation of privacy for conversations in his home and that the police did not obtain a warrant to conduct this search.[84] Ultimately, the Court held that Smith did not have a reasonable expectation of privacy in the numbers he dialed—because he should have known his phone company had a record of this information.[85] The Court justified the third-party doctrine by citing to a string of other cases applying a similar legal framework (now commonly referred to as the "misplaced trust doctrine").[86]The misplaced trust doctrine essentially provides that when someone voluntarily divulges information to another, they

75. *See generally* Olmstead v. United States, 277 U.S. 438 (1928).
76. *See Katz*, 389 U.S. at 351.
77. *See* United States v. Jones, 565 U.S. 400, 409 (2012).
78. *See id.* at 402–03.
79. *See id.* at 406.
80. *See id.* at 404–07.
81. *See id.* at 406–07.
82. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
83. *See id.* at 737.
84. *See id.*
85. *See id.* at 742–43.
86. *Id.* at 743–44.; *see* Allyson W. Haynes, *Virtual Blinds: Finding Online Privacy In Offline Precedents*, 14 VAND. J. ENT. & TECH. L. 603, 623 (2012).

assume the risk of betrayal.[87] This is typically applied in situations where law enforcement goes undercover to deceive someone for the purposes of information gathering.[88] However, as the dissent in *Smith* notes, a crucial distinction between the two doctrines is that in the undercover agent scenario, the defendant typically exercises more voluntary discretion in revealing personal details.[89] In contrast, in situations arising under the third-party doctrine, the defendant must be willing to avoid using technology that has become a "personal or professional necessity" in order to avoid surveillance.[90]

Since *Smith* was decided in 1979, the third-party doctrine has persisted and created a channel for law enforcement to directly compel data from companies without a search warrant.[91] As a result, some social media companies, like Meta, have dedicated sections on their websites with various metrics regarding the number and types of information requests they receive from law enforcement over a specific period.[92] Additionally, the company may detail its policy for handling these requests.[93] For example, Meta's page provides that the volume of requests it receives has increased steadily—from approximately 37,000 in 2015 to 147,000 in 2023.[94] Moreover, between January and June 2023, law enforcement made 13,511 requests by way of a subpoena, implicating a total of 28,700 users/accounts.[95] Meta addressed and produced some data for 83% of these requests.[96]

Nonetheless, the third-party doctrine has faced a great deal of criticism in recent years, particularly in an age where so much personal data exists online in the hands of third parties.[97] In fact, courts have been moving towards narrowing the scope of the third-party doctrine.[98] Most significant in recent years was the Supreme Court's 2018 decision in *Carpenter v. United States*. In this case, the government suspected the defendant of a series of robberies, so they requested the defendant's wireless carriers to provide his cell-site location information ("CSLI") records to verify where he was when the

87. *See* Hoffa v. United States, 385 U.S. 293, 302 (1966).

88. *See generally id.*; On Lee v. United States, 343 U.S. 747 (1952)*;* United States v. White, 401 U.S. 745 (1971).

89. *See Smith*, 442 U.S. at 749–50.

90. *Id.* at 750.

91. *See* Brent Skorup, *Tech Companies' Terms of Service Agreements Could Bring New Vitality to the Fourth Amendment*, HARV. L. REV. (Sept. 9, 2024), https://harvardlawreview.org/blog/2024/09/strongtech-companies-terms-of-service-agreements-could-bring-new-vitality-to-the-fourth-amendment-strong/ [https://perma.cc/YD54-TTXD].

92. *See Government Request for User Data*, META, https://transparency.fb.com/reports/government-data-requests/country/US/ [https://perma.cc/XUF5-8JSZ] (last visited Nov. 7, 2024).

93. *See id.*

94. *See id.*

95. *See id.*

96. *See id.*

97. *See* Harvey Gee, *Last Call for the Third-Party Doctrine in the Digital Age After Carpenter*, 26 B.U. J. SCI. & TECH. L. 286, 297 (2020) (describing the third-party doctrine as "one of the most critiqued aspect(s) of Fourth Amendment jurisprudence").

98. *See* United States v. Warshak, 631 F.3d 266, 284-286 (2010) (holding that the government could not compel a commercial ISP to turn over the content of their subscriber's emails without a warrant, and noting the Fourth Amendment should keep up with modern technology).

robberies occurred.[99] The carriers complied with the request and provided the police with records indicating all of the cell-sites Carpenter's phone used over the course of four months.[100] It may seem third-party doctrine would apply here, but the Supreme Court held that there was a reasonable expectation of privacy in extensive records of historical CSLI held by third parties.[101]

Though the Court did not completely eliminate the third-party doctrine in *Carpenter*, it narrowed it by recognizing the amount of data at issue was so vast and revealing.[102] In his dissenting opinion, Justice Kennedy pointed to six specific factors and considerations that influenced the Supreme Court's decision that the third-party doctrine did not apply to the surveillance of CSLI data. These factors were: (1) how revealing the data was, (2) the amount of data collected, (3) the number of people affected, (4) the inescapable nature of the surveillance, (5) whether the disclosure of data to the third party is automated, and (6) the difficulty of conducting surveillance.[103] Despite these factors being enumerated most clearly in a dissenting opinion, some legal scholars have coined these the "*Carpenter* factors" and used the factors to interpret the decision.[104]

3. The Border-Search Exception

One major exception to the scope of the Fourth Amendment's protections is border searches, which means that law enforcement may conduct routine searches and seizures at the border without probable cause or a warrant.[105] This exception is often justified by a need to balance Fourth Amendment interests and the right to privacy against legitimate governmental interests, like national security.[106]

The border search exception is relevant to social media monitoring because a key method law enforcement uses to collect social media information from immigrants is through searches of smartphones and digital devices at the border. In 2022, CBP conducted approximately 45,499 border searches of electronic devices.[107] While federal courts have consistently applied the exception in circumstances involving a physical search at the border, in recent years, some courts have been more hesitant to apply the exception in cases of searching digital data.[108]

---

99. *See* Carpenter v. United States, 585 U.S. 296, 301–03 (2018).

100. *See id.*

101. *See id.* at 309.

102. *See id.* at 311–12.

103. *See id.* at 339–40.

104. *See, e.g.*, Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of the Fourth Amendment*, 135 HARV. L. REV. 1790, 1800 (2022).

105. *See* United States v. Ramsey, 431 U.S. 606, 616–17 (1972).

106. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).

107. *See* Sophia Cope, *Federal Judge Makes History in Holding that Border Searches of Cell Phones Require a Warrant*, ELEC. FRONTIER FOUND. (May 30, 2023), https://www.eff.org/deeplinks/2023/05/federal-judge-makes-history-holding-border-searches-cell-phones-require-warrant [https://perma.cc/TZ2B-QAMT].

108. *See id.*

One reason for this trend is likely the Supreme Court's 2014 decision in *Riley v. California*. In *Riley*, the police searched the defendant during an arrest and seized his cell phone.[109] After conducting a search of the phone, the police subsequently introduced items found during the search into evidence during trial.[110] Upon review, the Supreme Court held that the warrantless search and seizure of the digital contents of a cell phone is unconstitutional under the Fourth Amendment.[111] The Court found that traditional justifications for a search, harm to officers, and destruction of evidence did not exist with searches of digital data.[112] Moreover, the Court emphasized that cell phones contained "vast quantities of personal information" that could not be compared to a brief physical search.[113] Though the *Riley* case was about a non-border search, it did deal with another Fourth Amendment exception—search incident to arrest.[114] Moreover, the case illuminates the fact that the Supreme Court gives greater deference to privacy interests where digital data is involved.[115] Since the decision, other courts have applied *Riley* in the context of border searches.[116] In *United States v. Smith*, the Southern District of New York drew upon the logic in *Riley* and held that the border search exception does not apply to digital information on a traveler's cell phone because "the magnitude of the privacy invasion caused . . . would allow the government to extend its border search authority well beyond the border itself."[117]

4. Recent Trends & the Evolution of Privacy Norms Online

The Supreme Court's decision in *Carpenter* illustrates that the Court is willing to endorse a more expansive understanding of the reasonable expectations of privacy amidst new technologies being leveraged for invasive purposes.[118]

Another force driving the widened understanding of what constitutes a "search" is the "mosaic theory" of the Fourth Amendment, which was first introduced in *United States v. Maynard*. [119] The mosaic theory essentially

109. *See* Riley v. California, 573 U.S. 373, 378–79 (2014).

110. *See id.* at 379–80.

111. *See id.* at 401.

112. *See id.* at 386.

113. *Id.* at 386.

114. *See id.* at 392 (stating that "the fact that an arrestee has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely . . . ").

115. Riley v. California, 573 U.S. 373, 392 (2014) (quoting Maryland v. King 569 U.S. 435, 463 (2013)) (stating that " . . . when privacy-related concerns are weighty enough . . . a search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee").

116. *See* United States v. Smith, 673 F. Supp. 3d 381, 394 (S.D.N.Y. 2023).

117. *Id.*

118. *See, e.g.*, *Carpenter*, 585 U.S. at 313; *see generally Jones*, 565 U.S. 400.

119. Matthew B. Kugler & Lior J. Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205, 206 (2015) (explaining that the mosaic theory was first articulated by Justice Douglas Ginsburg of the D.C. Circuit and served as a stark contrast to prior Fourth Amendment thinking until the Supreme Court embraced it in United States v. Jones).

conducts a Fourth Amendment analysis that assesses a search by observing a series of police surveillance attempts over time rather than examining each discrete police action for whether it in itself qualifies as a search.[120] Taken together, each bit of information aggregated from each surveillance attempt creates a "collective mosaic" that can be quite revealing.[121] So, even if individual steps do not constitute a search, taken together as a mosaic, they may collectively count as a search.[122] Since *Maynard*, in *U.S. v. Jones*, Justice Alito and Justice Sotomayor's concurrences appeared to also endorse the mosaic theory by acknowledging privacy concerns arising from data aggregation.[123] This continues to be a relevant issue today, with machine learning and automated technology tools that can render data analysis and aggregation a quick task.[124]

With respect to privacy on online platforms, some scholars frame privacy settings as "offers" by the website to protect certain pieces of information in a way that induces reliance upon users.[125] Privacy scholar Woodrow Hartzog has argued that privacy features should be construed as enforceable promises and courts should recognize their impact on a user's privacy expectations.[126] While this Note is not specifically focused on the application of contract law principles to the privacy context, the abundance of scholarship supporting the notion that user behavior is influenced by the constraints companies set qualitatively figures into this Note's argument that users may retain privacy expectations while participating on social media platforms.[127]

In fact, lower courts seem increasingly willing to recognize additional factors in the digital realm that inform a user's privacy expectations—like the presence of modifiable privacy settings on social media platforms.[128] However, there is no clear consensus on how much and in what ways users may secure their privacy settings to retain a reasonable expectation of privacy. Some courts have held that a defendant must be able to show that their social media account applied privacy settings that prevented *anyone* from accessing their account information to prove they held a reasonable expectation of privacy and receive Fourth Amendment protections.[129] The court's justification for imposing this high bar is largely because of their adherence

120. *See* Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313–14 (2012).

121. *Id.*

122. *See id.*

123. *See Jones*, 565 U.S. at 415-16, 427-30.

124. *See* Daniel J. Solove, *The Limitation of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 991 (2023).

125. Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1652 (2011).

126. *See id.*

127. *See generally* Matthew Tokson & Ari Ezra Waldman, *Social Norms in Fourth Amendment Law*, 120 MICH. L. REV. 265, 300 (2021); *see also* Hartzog, *supra* note 125.

128. *See* United States v. Westley, No. 3:17-CR-171 (MPS), 2018 WL 3448161, at *6 (D. Conn. July 17, 2018); *see* United States v. Adkinson, No. 4:15-cr-00025-TWP-VTW, 2017 WL 1318420, at *5 (S.D. Ind. Apr. 7, 2017); *see* United States v. Meregildo, 883 F.Supp.2d 523, 525 (S.D.N.Y. Aug. 10, 2012).

129. *See* United States v. Devers, 2012 WL 12540235, at *2 (N.D. Okla. Dec. 28, 2012).

to the misplaced trust and third-party doctrines. For example, in *U.S. v. Meregildo*, the defendant, a Facebook user, argued that they had a reasonable expectation of privacy over their social media data because they tailored their privacy settings to only allow "friends" to view their posts.[130] Though the court agreed a defendant could potentially retain a reasonable expectation of privacy on social media by way of privacy settings, the court declined to find this privacy interest here because the defendant had "no justifiable expectation his friends would keep his profile private . . . because those friends were free to use the information however they wanted—including sharing it with the government."[131]However, other courts have taken the opposite view—finding that individuals who modify their social media privacy settings to share only with "friends" do in fact maintain a reasonable expectation of privacy.[132] For example, in *United States v. Chavez*, law enforcement officers searched a defendant's Facebook account for evidence of a fraudulent telemarketing scheme. In this case, the defendant allowed public access to some content on his social media page (e.g., his name), but he limited access to other content to just himself or his Facebook friends because there were some things "he did not want 'a member' of the general public . . . who was not a 'Facebook Friend'" to see.[133] The court found that the defendant's action to exclude the public from certain content demonstrated that "he maintained a subjective expectation of privacy in that content."[134] The Government attempted to argue, drawing from the misplaced trust doctrine, that the defendant had no reasonable expectation of privacy because the content restricted to friends was shared with hundreds of people, "many of whom . . . he barely had a relationship with."[135] The court rejected this argument outright, warning that dangerous implications could result from courts being the arbiters of whether interpersonal relationships are "sufficiently meaningful."[136] Moreover, the court noted that accepting the Government's argument would be "contrary to the Framers' intention to secure the privacies of life against arbitrary power."[137]

Other courts have also drawn attention to the Fourth Amendment's particularity requirement that any necessary searches should be as limited as possible when constructing a social media user's expectation of privacy.[138] In *United States v. Blake*, a defendant asserted that the FBI's warrant to search their Facebook account was overbroad and violated the Fourth Amendment's particularity requirement because, as the court observed, it "required disclosure to the government of virtually every kind of data that could be found in a social media account."[139] The court agreed with the defendant, finding that the warrants could have been limited to specific messages and

130. *See* United States v. Meregildo, 883 F.Supp.2d 523, 525 (S.D.N.Y. Aug. 10, 2012).
131. *Id.*
132. *See* United States v. Chavez, 423 F.Supp.3d 194, 205 (W.D.N.C. 2019).
133. *Id.* at 202.
134. *Id.*
135. *Id.* at 204.
136. *Id.*
137. *Id.*
138. *See* United States v. Blake, 868 F.3d 960, 973–74 (11th Cir. 2017).
139. *Id.*

periods of time where the defendant was suspected of committing the crime at issue.[140] Moreover, the court noted that such a broad search would be the Internet-era version of a "general warrant," the "abhorred" colonial-era instrument allowing for excessive rummaging of people's belongings.[141]

III. ANALYSIS

The first part of this Note has provided an overview of the key federal agencies involved in implementing different social media surveillance initiatives on immigrants today. It has also outlined the relevant Fourth Amendment jurisprudence illustrating how courts have interpreted individual privacy protections amidst technological advancements that have enabled easier surveillance. The latter half of this Note will apply the Fourth Amendment framework to the social media surveillance landscape. With a focus on the Supreme Court's decision in *Carpenter*, this Note will advance the argument that courts should adopt a more expansive view of the Fourth Amendment to uphold privacy protections when social media surveillance tactics are most aggressive. Moreover, this section will shed light on the low efficacy of modern social media surveillance programs to further support the assertion that adopting a more privacy-protective view in this context would not inappropriately impose upon the interests of law enforcement.

A. Why All Social Media Data Should Not be Considered Wholly "Public"

As outlined in the previous section, many factors may play a role in a court's decision of whether a search or seizure offends an individual's privacy rights under the Fourth Amendment. However, determining whether the information gathered is "public" or "private" in nature typically plays a leading role in the analysis of whether an individual has a reasonable expectation of privacy.[142]

This section will argue that individuals' social media data can be understood as private information deserving of adequate privacy protections for two reasons. First, "social media data" is a broad term encompassing a wide range of information we ordinarily recognize as "personal." Second, the design of social media platforms and modifiable privacy settings encourage users to expect that their data is private and not accessible to law enforcement.

In *Katz*, the 1967 case that created the "reasonable expectation of privacy test," the Court explicitly stated that what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[143] Therefore, counterarguments that suggest individuals do not have a privacy interest because social media platforms are inherently "public" do not adequately capture the issue at hand. Not *all* user behavior on social

140. *See id.*
141. *Id.* at 973.
142. *Katz*, 389 U.S. at 351–52.
143. *Id.*

media is public and broadcast to all users in the digital world to take note of. The reality is that an individual's "social media data" consists of more than just the text and images they voluntarily share on a public profile.[144] In fact, mining social media data enables the collection of user information like personal identifiers and demographics (e.g., age, gender), location data (e.g., current address, places visited), user engagement on the platform (e.g., likes, comments, reposts), and personal associations (e.g., "friends," people and pages a user "follows").[145] As discussed earlier, it is important to note that social media platforms have expanded to use cases that do not involve socializing and interacting with others. Therefore, to adequately understand privacy interests on social media platforms, user behavior and expectations must be central to the inquiry.

Oftentimes, a user's behavior online can explicitly or implicitly indicate their manifested intention to remain "private." The most obvious example is when individuals create a social media profile that is intended to be private from the start—opting for a de-identified username and/or making the conscious choice to avoid posting any content of their own, particularly anything that may reveal personal identifying information. Even when a user's profile is public, this may not automatically mean that the user has chosen to make *all* their activity on the platform public. Most social media platforms offer a range of privacy settings that may inform users' expectations of their privacy rights.[146] These privacy settings are typically separate from the platform's privacy policies and allow users to customize who can access specific content they post, view their activity, and more.[147] By taking active steps to customize their privacy settings, users are arguably exhibiting a desire to maintain their privacy online.

As illustrated by *Meregildo* and *Chavez*, lower courts that have had the opportunity to address Fourth Amendment protections with respect to social media searches and are willing to recognize that privacy settings can impact social media users' expectations of privacy.[148] While the *Meregildo* and *Chavez* courts diverged about whether a user modifying privacy settings to "friends only" meant an individual "lost" their reasonable expectation of privacy, these cases are still consistent. Both courts examined the role privacy settings played when conducting their Fourth Amendment analysis and in

144. *See* Alexandra Mateescu et.al, *Social Media Surveillance and Law Enforcement*, DATA C.R. 1, 2–4 (Oct. 27, 2015), https://datacivilrights.org/pubs/2015-1027/Social_Media_Surveillance_and_Law_Enforcement.pdf [https://perma.cc/Y55L-BKWC]; *see* Adrian Shahbaz & Allie Funk, *Social Media Surveillance*, FREEDOM HOUSE, https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance [https://perma.cc/36UY-RNQT] (last visited Jan. 27, 2024)**;** *see Social Media Data Mining: Understanding What It Is and How Businesses Can Use It*, U. SAN DIEGO (Apr. 3, 2020), https://www.sandiego.edu/blogs/business/detail.php?_focus=76022 [https://perma.cc/MVD3-VNBC].

145. *See generally* Mateescu et.al, *supra* note 144; Shahbaz & Funk, *supra* note 144.; *Social Media Data Mining*, *supra* note 144.

146. *See* Thorin Klosowski, *Simple Online Security for Social Media Accounts*, N.Y. TIMES (Apr. 22, 2022), https://www.nytimes.com/wirecutter/guides/online-security-social-media-privacy/ [https://perma.cc/9VQA-9H8F].

147. Hartzog, *supra* note 125.

148. *See, e.g.*, *Meregildo*, 883 F.Supp.2d at 525; *see Blake*, 868 F.3d at 973–74; *see also Westley*, 2018 WL 3448161, at *6; *see also Adkinson*, 2017 WL 1318420, at *5.

formulating whether the defendant retained a reasonable expectation of privacy.[149]

When the concept of a "reasonable expectation of privacy" was created, it was intended to be informed by social norms.[150] However, as Justice Alito contemplated in his concurrence in *Jones*, the reasonable expectation of privacy test is prone to circular reasoning, and judges may be confusing their own expectations of privacy instead of the hypothetical reasonable person.[151] Alternatively, as legal and privacy scholars Matthew Tokson and Ari Waldman posit, individual actors do not create norms, but rather, norms are shaped by companies and the product design they promote.[152] Consequently, social media users can only exert their privacy interests within the constraints that platforms *allow* them to. The reasonable expectation of privacy test rests on the assumption that privacy expectations are stable, but technology can change those expectations.[153] For the ordinary social media user, the only way to exercise control over their privacy after signing up for an account is by utilizing the platform's customizable privacy settings. Courts have already been affirmatively expressing support for the evolving nature of the Fourth Amendment for years.[154] Therefore, it is within the courts' power to understand and apply the Fourth Amendment in the context of subjective user privacy expectations informed by the reality of social media platforms.

Many credit the "beginning of social media" to 2004 when MySpace reached one million active monthly users.[155] Since then, social media has become a dominant force in the digital world.[156] The rapid growth of social media platforms has been likened to other recognized communication-enabling technologies like computers, smartphones, and the Internet.[157] Today, the most popular social media platforms, like Facebook, YouTube, and WhatsApp, each host over one billion users and have sustained themselves for over ten years.[158] Because the Fourth Amendment protects people, not places, its protections must extend to the number of individuals active on social media platforms every day.[159]

Given the fact that social media platforms hold such a crucial position in modern-day communication, and there are both privacy and free speech interests at stake here, the third-party doctrine should not be applied without recognition of the reality of what it means to be an online user in today's

149. *See Meregildo*, 883 F.Supp.2d at 525–26; *see Chavez*, 423 F.Supp.3d at 201–02.

150. *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (noting that an expectation of privacy must be "one that society is prepared to recognize as 'reasonable'").

151. *See Jones*, 565 U.S. at 427.

152. *See* Tokson & Waldman, *supra* note 127, at 300.

153. *See Jones*, 565 U.S. at 427 (Alito, J., concurring).

154. *See, e.g.*, Warshak v. United States, 631 F.3d 266, 286 (6th Cir. 2014) (noting that "as some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise").

155. Esteban Ortiz-Ospina, *The Rise of Social Media*, U. OXFORD (Sept. 18, 2019), https://ourworldindata.org/rise-of-social-media [https://perma.cc/66X7-AVEU].

156. *Id.*

157. *See id.*

158. *See id.*

159. *See Katz*, 389 U.S. at 351.

digital world. Even in 1979, when *Smith v. Maryland* was decided, Justice Marshall noted in his dissent that "privacy is not a discrete commodity, possessed absolutely or not at all."[160] Moreover, in recent years, the Supreme Court seems more receptive to criticisms of the third-party doctrine applied online. For example, in her concurrence in *U.S. v. Jones*, Justice Sotomayor noted that the doctrine needed to be reconsidered because people are presently forced to provide information about themselves to third parties for even the most mundane tasks.[161]

B. Extensive Data Collection Post-Carpenter

This section will describe how the Supreme Court's decision in *Carpenter v. United States* signals a shift away from a rigid application of the third-party doctrine and argue that *Carpenter* should have a cognizable impact on how courts understand individual privacy interests on social media. First, this section will examine the Supreme Court's holding in *Carpenter* and the boundaries the Court set in determining the scope of its decision. Next, it will illustrate how law enforcement's aggressive social media surveillance tactics satisfy several of these factors such that the third-party doctrine should not bar the Fourth Amendment's application in this context.

Though *Carpenter* expanded the Fourth Amendment's protections, the Court specifically emphasized that the decision was limited to CSLI data, did not eliminate the third-party doctrine, and should not be interpreted to question traditional surveillance tools, like security cameras.[162] Despite the Court's efforts to define the scope of its decision, it did not specifically provide a test for future courts to apply in deciding what qualifies as comprehensive data collection. Therefore, the decision ultimately still raises considerations for similar kinds of data collection that could also be found too extensive to fall within the bounds of the third-party doctrine.

As noted earlier, the six factors gleaned from *Carpenter* to determine whether surveillance is exempt from the third-party doctrine are: how revealing the data is, the amount of data collected, the number of people affected, the inescapable nature of the surveillance, whether the disclosure of data to the third party is automated, and the difficulty of conducting surveillance.[163] The social media surveillance techniques law enforcement have employed on immigrants arguably qualify as extensive based upon four factors—revealing nature of data, amount of data collected, number of people affected, and difficulty of conducting surveillance.

First, social media data is "revealing" in a manner acknowledged by the *Carpenter* court. In *Carpenter*, the Court found location information to be particularly sensitive because it also revealed "familial, political, professional, religious, and sexual associations" that ultimately represented "privacies of life."[164] Similarly, social media data contains extensive personal

160. *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).
161. *Jones*, 565 U.S. at 417 (Sotomayor, J. concurring).
162. *See Carpenter*, 585 U.S. at 298.
163. *See id.* at 339-40.
164. *See id.* at 311.

information—from basic identifiers (e.g., name, age, and address) to location data (e.g., current location, businesses frequented), and information about an individual's relationship status, political affiliations, and religious beliefs that may be directly or indirectly gleaned from their activity on the platform.[165] Additionally, even DHS has categorized social media handles as sensitive personally identifiable information.[166]

Data aggregation is a recognized privacy concept that illustrates why social media surveillance can be so revealing and invasive. This concept describes the phenomenon where individual data points seem trivial but actually become more powerful and invasive of privacy when linked together to form a bigger picture.[167] Data aggregation is the basis for the mosaic theory of Fourth Amendment analysis that has become increasingly recognized after *Jones* and *Carpenter*.[168] In the context of social media monitoring, data aggregation explains why machine learning and analytical tools used by law enforcement can be so invasive. For example, during border searches, after extracting social media data from cell phones, ICE runs collected information through an analytical tool, FALCON-SA, that is capable of conducting a "social network analysis."[169] The produced analysis highlights trends and draws connections between different people, businesses, and ICE investigations based upon a combination of collected social media data and other information from separate ICE and CBP databases.[170] Moreover, the agency is authorized to not only access data, but also store and share it with other law enforcement agencies.[171]

Personal data is interrelated to begin with because "life involves relationships and transactions between people."[172] AI and machine learning tools only further facilitate our ability to interrelate people.[173] ICE's social network analysis tool, which is capable of drawing connections between people, is an illustrative example.[174] This also highlights the fact that the value of social media monitoring is not gathering information about a singular person, but rather gathering information about *many* people the analytical tool deems to be closely affiliated with an individual. Consequently, though law enforcement may be targeting recent immigrants, long-time American citizens are effectively being surveilled too because their information is

165. *See generally* Samuel Wamba et al., *The Primer of Social Media Analytics*, 28 J. ORGANIZATIONAL & END USER COMPUTING 1 (2016).

166. *See* Rachel Levinson-Waldman et al., *Social Media Surveillance by the U.S. Government*, BRENNAN CTR. JUST. (Jan. 7, 2022), https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government [https://perma.cc/KH96-3G4W].

167. *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1889–90 (2013).

168. *See* Kugler & Strahilevitz, *supra* note 119, at 205–08.

169. Patel et al., *supra* note 12, at 15.

170. *See id.* at 16.

171. *See id.* at 27.

172. Solove, *supra* note 124, at 990.

173. *See id.* at 991.

174. *See* Patel et al., *supra* note 12, at 15–16.

indirectly analyzed and stored in law enforcement databases.[175] In *Carpenter*, the Court left open the question of whether "collection techniques involving foreign affairs or national security" fell within the scope of its holding. However, given that the scope of surveillance may be so wide, sometimes bleeding into the lives of average American citizens, arguably comprehensive monitoring cannot always be appropriately categorized under the umbrella of foreign affairs.

The scope of surveillance also further relates to the next *Carpenter* factor regarding the amount of data collection at issue. Social media monitoring may result in a large amount of data collection from a significant number of people, depending on the circumstances. Surveillance tactics that rely on "continuous" monitoring have the capacity to amass a significant amount of data.[176] One example is ICE's contract with Giant Oak, a data mining firm, to implement a surveillance program that continuously monitors visa applicants from the time of submission.[177] Visa applicants' social media data was then aggregated and analyzed to evaluate behavioral patterns and ultimately aid in enforcing its Overstay Lifecycle program.[178] A similar technique is used during the course of a border search. When ICE accesses a digital device during a border search, it can currently extract information from the device if the data is "pertinent" to an investigation or enforcement activity.[179] As previously discussed, once social media data is extracted from the device, it is processed through FALCON-SA for analysis and ultimately generates an in-depth report on findings.[180] It is also worth noting that in circumstances where ICE relies on human-driven monitoring, instead of machine learning and AI, the surveillance is arguably still extensive. For example, in 2018, ICE spent $100 million to hire 180 people to monitor 10,000 "high-risk" foreign visitors continuously throughout their stay in the United States, only ceasing efforts if the visitor is granted legal residency.[181]

The existence and use of machine learning surveillance programs are also responsive to the *Carpenter* factor regarding the difficulty of conducting surveillance. This factor essentially provides that where the time and effort required for surveillance is low, the more likely it is to be considered a search because it is more prone to abuse, overuse, and less administrative or political scrutiny.[182] Additionally, many privacy scholars discussing mass surveillance initiatives point to the "quantitative privacy" concerns these programs

175. *See id.* at 29.

176. Patel et al., *supra* note 12, at 7–8; *see* Shaiba Rather & Layla Al, *Is The Government Tracking Your Social Media Activity?*, ACLU (Apr. 24, 2023), https://www.aclu.org/news/national-security/is-the-government-tracking-your-social-media-activity [https://perma.cc/3RPF-4WWY] (discussing a DHS program that monitored non-citizens from the time they apply for an immigration benefit to when they become a naturalized citizen).

177. *See* Cox, *supra* note 53.

178. *See id.* (explaining how ICE has expanded its use of AI-powered tools to more generally surveil social media for posts containing derogatory comments).

179. *See* Patel et al., *supra* note 12, at 27.

180. *See id.* at 28.

181. *See id.* at 26.

182. *See* Tokson, *supra* note 104, at 1804.

raise.[183] Privacy law scholars David Gray and Danielle Citron assert that what matters most for Fourth Amendment analysis is the *means* of surveillance.[184] Therefore, privacy interests are implicated where surveillance is "broad and indiscriminate" because these conditions enable a surveillance state.[185] In the social media context, the machine learning tools ICE utilizes allow for bulk screening programs that operate with high efficiency, analyzing data from a mass amount of people and providing synthesized reports for law enforcement.[186]

C. Is Modern Social Media Surveillance Effective?

A common theme underlying Fourth Amendment cases is the tension between privacy interests and the interests of law enforcement and national security. However, both privacy and national security are important values for the greater public welfare, and the Supreme Court has recognized that each represents strong values that should not be compromised.[187] However, law enforcement's proposed and implemented social media surveillance tactics thus far are aggressive and largely extinguish the privacy interests of immigrants altogether. Despite the extensive nature of surveillance, it is questionable, at least to this author, just how beneficial this surveillance really is for national security purposes.

First, there is an abundance of research finding that there is no single indicator or profile that can affirmatively predict if someone is a terrorist.[188] Therefore, law enforcement's practice of monitoring social media for "hints" of the risk someone poses to the nation seems questionable. Moreover, law enforcement officials themselves seem to be skeptical of how useful social media surveillance actually is.[189] An email chain between staff at the Office of the Director of National Intelligence indicated that staff members believed collecting social media identifiers was useless and added no value to the immigration screening process.[190] Additionally, the 2016 report from the DHS

183. Danielle Citron & David Gray, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 73–75 (2013).

184. *See id.* at 71–72.

185. *Id.*

186. *See* Patel et al., *supra* note 12, at 25–28.

187. *See* United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div., 407 U.S. 297, 321 (1972) (stating that national security interests do not categorically trump individual privacy and free expression).

188. *See, e.g.*, Faiza Patel, *Rethinking Radicalization*, BRENNAN CTR. JUST. 8–10 (Mar. 8, 2011), https://www.brennancenter.org/our-work/research-reports/rethinking-radicalization [https://perma.cc/HG8K-J9VT]; *see* Levinson-Waldman et al., *supra* note 160 (noting that social media conversations are difficult to interpret and "[g]overnment officials and assessments have repeatedly recognized that this dynamic makes it difficult to distinguish a sliver of genuine threats from the millions of everyday communications that do not warrant law enforcement attention"); *see generally* Timme Bisgaard Munk, *100,000 False Positives for Every Real Terrorist: Why Anti-Terror Algorithms Don't Work*, FIRST MONDAY (Sept. 2017), https://firstmonday.org/ojs/index.php/fm/article/view/7126/6522 [https://perma.cc/TJV5-TPB7].

189. *See State Department Rule Ineffective*, *supra* note 48.

190. *See id.*

Office of the Inspector General explicitly stated that ICE's pilot programs lacked adequate metrics and recommended that USCIS and ICE focus more efforts on evaluating initiatives.[191]

IV. RECOMMENDATIONS

Technology has enabled law enforcement to monitor immigrants and impinge upon their privacy without any real consequence or mechanism for accountability. Despite little evidence supporting the notion that social media surveillance is effective, law enforcement continues to engage in social media surveillance in various ways.[192] As previous sections have described, some examples include requesting social media handles on visa applications, extracting digital data at the border, and working with private entities to utilize advanced data analytics tools powered by mass data aggregation and automated monitoring.[193] There are serious privacy concerns at stake and revamping this system requires interventions at both the legal and policy level. Therefore, this section will (1) argue that law enforcement should be required to obtain a warrant before engaging in specific forms of social media surveillance, and (2) advocate for a process requiring more transparency from law enforcement agencies engaging in social media surveillance.

First, this Note argues that after the Supreme Court's decision in *Carpenter*, there are specific forms of social media surveillance that should require law enforcement to obtain a warrant prior to use. As discussed, the *Carpenter* factors highlight various elements that can make surveillance particularly aggressive and thereby exempt from the third-party doctrine.[194] The revealing nature of data, the volume of data collected, the large number of individuals affected, and the relative ease of conducting surveillance are all implicated in the social media surveillance context. For example, surveillance techniques relying on machine learning and automated monitoring often enable law enforcement to engage in continuous monitoring over a period of time.[195] Moreover, the sophisticated nature of this technology likely allows law enforcement to screen vast quantities of data at a rate exceeding manual screening.

Even under *Carpenter*, many invasive social media surveillance practices would not be deemed aggressive enough to require law enforcement to obtain a warrant. Examples might include where law enforcement looks up an individual's public social media page or where a law enforcement agent goes undercover to befriend an individual on social media for information-gathering purposes. These are ultimately human-driven processes that do not respond to the concerns raised by *Carpenter* about technology being leveraged to make surveillance broad, cheap, and quick.[196]

---

191. *See DHS Social Media Screening*, *supra* note 46 ("The OIG's draft report states that the 'pilots did not have metrics to measure success' and 'did not establish […] benchmarks.'").

192. *See* discussion *supra* Section III.C.

193. *See* discussion *supra* Sections II.A.2–3.

194. *See Carpenter*, 585 U.S. at 339-40.

195. *See generally* Patel et al., *supra* note 12, at 8.

196. *See Carpenter*, 585 U.S. at 311-12.

Ultimately, it is important to highlight that requiring law enforcement to obtain a warrant prior to conducting certain kinds of social media surveillance does not automatically resolve privacy concerns on its own. As noted earlier, many of the most aggressive social media surveillance initiatives were pitched as pilot programs, which are not often rigorously evaluated for program efficacy and implementation.[197] This gives way to another problem: a dearth of reporting and publicly available information that brings transparency to the process, goals, and success of these surveillance initiatives. It is difficult to assess the interests at stake and how people's rights are being infringed upon without more transparency.

Therefore, this Note also proposes a policy recommendation aimed at improving transparency from law enforcement agencies about social media surveillance practices. One way this could be achieved is through the PCLOB.[198] As previously noted, federal law enforcement agencies issue reports to PCLOB about their work, and PCLOB regularly publishes its own reports detailing recommendations on various surveillance issues.[199] For example, there could be a mandatory reporting obligation imposed on law enforcement agencies to provide information about new pilot programs, particularly those employing machine learning and automated decision-making tools. This information would ideally provide insight concerning program implementation, data retention practices, and any metrics evaluating program efficacy. Moreover, the PCLOB could advise agencies on how to design programs to be more privacy-conscious and publish reports on an agency's compliance with privacy principles for public transparency.

Another policy recommendation is for Congress to impose more transparency obligations for social media platforms in responding to law enforcement's requests for user data. While some social media companies, like Meta, already voluntarily publish a range of metrics related to law enforcement's requests for information, it is unclear whether all platforms are required to do so by law.[200] Setting a standardized list of metrics that platforms are required to provide would also help policymakers have a better grasp of surveillance trends and make it easier for users to understand their privacy risks across platforms. Additionally, platforms could be required to provide more insight into their internal processes for determining whether an information request from law enforcement is adequate. Finally, social media companies could be required to provide some level of notification to users if their data is requested where not otherwise legally prohibited.

V. CONCLUSION

Social media surveillance is a civil liberties issue that significantly impacts the privacy rights of both recent immigrants and Americans. This

197. *See* Patel et al., *supra* note 12, at 26.; *see DHS Social Media Screening*, *supra* note 46.

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

199. *See id.*

200. *See, e.g.*, *Government Request for User Data*, *supra* note 86.

issue is only becoming more pressing with the rise of automated tools that make it easier and cheaper for law enforcement to extract an abundance of information about an individual that goes far beyond the traditional notion of a Fourth Amendment search. Over the years, courts have consistently recognized the need for the Fourth Amendment to keep up with the latest technology and surveillance tools. Due to aggressive, warrantless surveillance, there needs to be judicial recognition that immigrants using social media have justifiable expectations of privacy on platforms. As the number of participants on social media platforms grows, it is important to prioritize individual privacy rights in Fourth Amendment interpretation to keep up with an expanding cyberspace.